Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Phishing Attack Techniques

Soumya. T
ME CSE, Assistant Professor CSE, Sasurie Academy of Engineering

Abstract: *Now in a day's phishing is a special type of network attack where the attacker creates a replica of an existing web page to fool users in to submitting personal, financial, transaction orpassword data to what they think is their service provider'swebsite. Phishing has two techniques, deceptive phishing and malware – based phishing. Here we focus on deceptive phishing using social engineering schemes. To protect users against phishing, various anti-phishing techniques have been proposed. In this paper we have reviewed various phishing and anti-phishing methods for detecting and preventing phishing attack.*

I.INTRODUCTION

The word 'Phishing' initially emerged in 1990s. The early hackers often use 'ph' to replace 'f' to generate new words in the hacker's community, since they usually hack by phones. Phishing is a new word produced from 'fishing', it refers to the act that the attacker appeal users to visit a faked Web site by sending them faked e-mails (or instant messages), and silently get victim's personal information such as user name, password, national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). One of the primary aims of phishing is to dishonestly carry out fraudulent financial transactions on behalf of users using a forged email that contains a URL pointing to a fake web site masquerading as an online bank or a government entity. A phisher may Tempt a victim into giving his/her Social Security Number, full name, & address, which can then be used to apply for a credit card on the victim's behalf. The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into conceding personal information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to renew personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, on the other hand, is bogus and set up only to steal the user's information

Types of phishing attack- Phishing is a particular type of spam that employs two techniques:

1. Deceptive phishing
2. Malware-based phishing

The first technique is associated to social engineering schemes, which depend on forged email claims that emerge to originate from a legitimate company or bank. Subsequently, through an embedded link within the email, the phisher attempts to redirect users to fake Websites. These fake Web sites are designed to fraudulently achieve financial data (usernames, passwords, credit) from victims.

The second technique involves technical subterfuge schemes that rely on malicious code or malware after users click on a link rooted in the email, or by detecting and using security holes in the user's computer to achieve the victim's online account information directly. Sometimes, phisher attempts to misdirect the user to a fake Web site or to a legitimate one monitored by proxies.

II.LITERATURE REVIEW

In [1] they present an allegation of the various techniques currently used to detect phishing email, at the different stages of attack, mostly focusing on machine- learning techniques. A comparative study and evaluation of filtering methods is carried out. This provides an understanding of the problem, its recent solution space, and the future research directions anticipated. Classifiers used to identify phishing email are based on: supervised learning, i.e. they must learn before they can be used to detect a new attack; unsupervised learning, which is faster, but has a low level of accuracy; or a hybrid (supervised and unsupervised) learning, which is time consuming and costly.

In [2] they explain various approaches to detection for replication of web site layout and structure through source code (and optionally image) fingerprinting. This Anti phishing technique based on URL and Domain Identity, and Image Based Webpage Matching .It first identifies the related authorized URL in which approximate string matching algorithm is used. The image based matching mechanism uses key point's detection and feature extraction methods.

In [3] they present a novel technique to visually compare an alleged phishing page with the legitimate one. The target is to determine whether the two pages are warily similar. Signature based algorithm is used, the proposed approach is inspired by two previous open source anti-phishing solutions: the Anti Phish browser plug in and its DOM Anti Phish extension. This results in impressive speed-ups. A negative comparison between two pages is produced in a few milliseconds.

In [4] they present that participant using the high exactness anti-phishing tool considerably outperformed those using the less accurate tool in their ability to: (1) differentiate legitimate websites from phish; (2) avoid visiting phishing websites; and (3) avoid transacting with phishing websites. URL and DNS Based spoofing technique are used. The results indicate that using more accurate anti-phishing tools can significantly improve users' ability to identify phishing websites and to better avoid visiting and transacting with phish. It is also imperative to improve methods for conveying tool warnings.

In [5] they implement a model i.e. – IPDCM, can handle about 50 pages per second, which make it feasible for real internet security production applications. This intelligent model for detecting phishing websites, extract 10 different types of features such as title, keyword and link text information to represent the website. Heterogeneous classifiers are then built based on these different features Hierarchical clustering technique has been employed for automatic phishing categorization. And also SVM is used in this technique.

In [6] this technique is purely based on image comparison using discriminative key point features in WebPages. They used an invariant content descriptor, the Contrast Context Histogram (CCH), to compute the similarity degree between suspicious pages and authentic pages. This anti phishing tool is highly efficient and error free. It can be used in online banking, online shopping and to maintain the mail accounts.

III. PROPOSED SYSTEM

Here we will use Ant colony algorithm to detection of phishing attack, while processing of algorithm it generates multiple rules for the phishing data and suspicious links within short of time. This policy will help to protect client and server side attacks. URL and Domain Identity mechanism is used in this technique. ACO algorithm is used to illustrate and recognize all the factors and rules in order to classify the phishing website and the relationship that correlate them with each other. This algorithm is implemented in PHP and advanced java.

IV. CONCLUSION

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing isbeing combated through user education, legislation, and integrated anti-phishing measures in modern Web browsers. We focus on deceptive phishing using social engineering schemes. To protect users against phishing, various anti- phishing techniques have been proposed. To detect phishing web site mostly filtering methods, classifiers based on machine learning algorithm i.e. supervised and unsupervised learning and Visual Similarity Assessment based technique is to be applied.

V. REFERENCES

[1] Ammar Almomani, B. B. Gupta, Samer Atawneh, Meulenberg, Eman Almomani,"A Survey of Phishing Email Filtering Techniques", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, 2013.

[2] T.Balamuralikrishna, N.raghavendrasai, M.Satya Sukumar, "Mitigating Online Fraud by Ant phishing Model with URL & Image based Webpage Matching", International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, March -2012.

[3] A.V.R.Mayuri,"Phishing Detection based on VisualSimilarity", International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, March -2012.

[4] Ahmed Abbasi, Fatemeh "Mariam" Zahedi, Yan Chen "Impact of Anti-Phishing Tool Performance on Attack Success Rates".

[5] Weiwei Zhuang, Qingshan Jiang, Tengke Xiong,"An Intelligent Anti-phishing Strategy Model for Phishing Website Detection".

[6] Mallikka Rajalingam, Saleh Ali Alomari, Putra Sumari "Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages", International Journal of Computer Science and Security (IJCSS), Vol. 6, 2012.

[7] Shivender Singh, Anil K. Sarje, Manoj Misra,"Client- Side Counter Phishing Application using Adaptive Neuro-Fuzzy