ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Lightweight Framework for Detection and Resolution for Phishing, Pharming and Email Spoofing

Pooja Modi[1], Hardik Upadhyay[2], Ketan Modi[3], Krunal Suthar[4]

ME Student, Department of Computer Engineering, M.E.C, Basna, India[1]

Assistant Professor, Department of Computer Engineering, GPERI, Mehsana India[2]

Associate Professor, Department of Computer Engineering, M.E.C, Basna, India[3]

Assistant Professor, Department of Computer Engineering, SPCE, Visnagar, India[4]

ABSTRACT: Email Change the way of communication in today's world. Nowadays email based attacks are growing up. Some of attacks are performed in email like Email Spoofing, Phishing and Pharming attack. Pharming is an advanced version of phishing attack. Main Aim of phishing attack is forgery send a fake email to user and obtained/Retrieved the credential user's information like username, password or banking account data. Pharming attack is un-authorized party change/exploit DNS setting of server so that when you enter the legitimate/Original Website address, it redirecting them to a fraudulent/lure website which are same as realistic. Phishing is a method of retrieve someone personal information, while spoofing is a means of delivery. Email Spoofing is stealing of someone's identity to sending emails containing viruses. It is a trick to hide legitimate user identity and blame to somebody else. In this research we are proposing an approach to decrease a highly false positive ratio detecting of Pharming and phishing attack. Our proposed approach achieves an accuracy level comparable to the best results obtained through related techniques and also using this combine approach to detecting and protecting Pharming, Phishing and email spoofing.

KEYWORDS: Pharming, advance phishing, prevention against Phishing and Pharming attack, detecting Phishing and Pharming attack

I. INTRODUCTION

Throughout the world, online identity theft has been highly increasing. To gaining access to someone's personal or credential data and impersonating them. In today's 21st Century world, electronic identity theft has been easier.

A Word Phishing comes from the "Fishing". Phishers attempt to steal personal information. Phishing attack is an attack to hide fake user identity for doing unlawfully Crime. It is combining Social Engineering and forgery technique. Phishing attack is done in various categories like as Email phishing, SMSishing and vishing for phishing over VOIP. Phishing attacks are makes internet user to reveal their personal credential Information to malicious Party. Phishing attack are starting when some unauthorized party continuously send bulk of forgery mail to user to asking them to click to URL for update their account Information. When user click on that link to included in the e-mail to redirect on fake Website which are same appear to come from legitimate websites such as yahoo update password, credit card number, PayPal, or other banking Sites. User submits their personal credential information like username, password, social security number, phone number, address, and on lure website. The phisher may be able to gain access to more information by just logging in to account. [8]

To Detecting phishing attack, there are mainly two approaches to identify a phishing attack. The first one is based on blacklist and another one is to detect new launched fraudulent website. First approach is blacklists which are checked requested URL Compared with a blacklist URL. If URL is matched with many of blacklists URL then it cannot be redirect to user browser. But all blacklists website cannot be cover all phishing website. Another approach, when new fraudulent website launched that time URL compared with legitimate website content, links, domains for identify the fraudulent website. If any end user was carefully watching visited URL, most of phishing attacks are easily detected because of its URL different from legitimate website. In Phishing, Pharming attack doesn't required any victim click on a link in a fake mail.[8] Phishing attack are done using different Communication channels such as email, instant messaging services, IRC and web-pages are popular.

Pharming attack is advanced version of phishing attack done by DNS vulnerability. Pharming is a web based fraud which causes intended to redirect a website's traffic to another fraudulent site; main aim of attacker has stealing personal data and passwords for unlawfully Crime. [10] Pharming can be done either by changing hosts file on victim's computer or by exploitation of DNS vulnerability. Pharming attack is un-authorized party to change the DNS setting of server so that user entered a legitimate website address its redirect to fraudulent/fake website which are same look like original. [7]

Pharming attacks are more difficult to detect as phishing attack. Because in Pharming attack, attacker attacks on DNS Server and corrupt DNS Information, so it redirect user to a fake/fraudulent website. But in phishing attack, attacker/malicious party has send forgery email to user which contains link that mail is also same appear to come from legitimate websites so that user can easily convince to that mail. [5] When user click on that mail for submits their personal credential information. In phishing attack, it is easy to identify fake website to observing URL but in Pharming attack, it cannot be identify fake website because of attack changes DNS setting. So even that user type a correct URL yet to be a redirected to fraudulent web page. [5][7]

DNS is a hierarchical naming system for computer and provides services on the Internet. Domain Name Services translate a human readable domain name into some corresponding IP address. When user type domain name into a browser, computer send request to a name server (NS) which are maintained by Internet Service Provider (ISP). If Name server found requested URL on cache, then the address is returned into the browser. If the requested URL is not in cached then Name Server will send request further DNS hierarchy of Name Server. But attacker using some trick into adding or modifying retrieved DNS data to send user browser. A user can visit site that is fraudulent site and user submit their account credential data. This attack is also called Pharming attack and also called DNS hijacking. [1]

Email spoofing may be effectively done by phishing attack on receiver side. The term Spoofing usually refers to a category of scam in which the sender poses as somebody else. Any malicious party send mail with origin details have been altered so as make it to appear to origin from the different source. Email Spoofing is stealing of someone's identity to sending emails containing viruses. It is a trick to hide legitimate user identity and blame to somebody else. Most of email spoofing is possible of SMTP vulnerability. SMTP protocol is used for sending mail but does not provide any authentication mechanism. [2]

The end users may also implement verification for originator of email to prevent from falling into the attacks of spoofed email. Email spoofing is easy to spoof because of SMTP Protocol. It does not provide any authentication. Another way to spoofing email is using of address spoofing. In address spoofing, Attacker send forged mail to legitimate recipient, that message stored on top of the recipient mailbox. The address spoofing may contain an email address which is different from the legitimate address. [2] In previous paper, we introduced a combine approach to provide anti-Pharming and Phishing protection integrated into client browser. Using combine approaches we improve false positive ratio and also substantial result that demonstrate its effectiveness and accuracy result to detecting phishing and Pharming attack.

II. PHISHING ATTACK VECTOR

A. Social Engineering Factors

Most of Phishing attacks have been done by Email. Attacker impersonates the send mail to source email address and also attaching appropriate company logo for attempting to legitimate site.

For example, the victim receives an email from a fake email address like support@mybankinfo.com with the subject of the 'security update', requesting them to follow the URL www.mybank-update.info, which is not actual legitimate domain name that belongs to the attacker – not the bank) and provide their banking PIN number. The attacker would ask for the legitimate user to type-in their confidential details like as address, credit card number and security code, and also capturing enough information to complete a real transaction.

B. Phishing Message Delivery

Phishing message delivery can be done as follow:

a) Email and Spam

Attackers send continuously forgery mail to legitimate live email address within a few hours. Most of email addresses used for deliver to legitimate live addresses is purchased from some conventional spam. Attacker sends a fake mail to using of 'Mail From' header with subject of update information for grabbing credential information.

b) Web-based Delivery [9]

A Web-based delivery of phishing attacks is through malicious web-site content. This content may be included HTML code, Logo, images, font, web bugs, Embedding malicious content by the Phisher, or a third-party site hosting some embedded content. Banner advertising is a very simple method for attacking by attacker may use to redirect an organizations customer to a fake web-site and capture confidential information.

c) Instant Messaging

Phishing attack done in instant messaging is very easily because of instant messaging allows HTML dynamic content like graphics, URL's, multimedia etc.

C. Phishing Attack Vectors

a) Man-in-the-middle Attacks

One of the most important attacks is man in the middle attack which is successfully done for gaining control of legitimate user credential information and other resources. In this attack, attacker situates themselves between the legitimate user and web based application. Attacker must be redirect to legitimate user to another server instead of real server.

b) URL Obfuscation

Using this technique, attacker is attacking on server for redirecting legitimate user to another server instead of real server. For example, the legitimate user writes some URL on the web browser like http://www.mybank.com/ that time legitimate user may follow a link to http://www.mybank.com.ch/ instead of http://www.mybank.com/

c) Cross-site Scripting Attacks

Cross-site Scripting Attacks are also known as CSS or XSS. Cross-site Scripting Attacks make use of custom URL or code injection into a valid web based application URL or imbedded data field.

III. PHARMING ATTACK VECTOR

There is several Pharming attack Vector as follow:

1. Home Factors
2. Local Host and Local Network attack
    - Traffic observation and modification
    - Change Lookup process
    - Man-In-The-Middle attack
3. Domain Registration Attack [7][5]
    - Domain Hijacking Attack
    - Similar domain name registration
4. Domain Configuration Attack
    - DNS Wildcards
    - Poorly managed DNS Server
5. DNS Spoofing [1][7]
    - DNS Cache poisoning
    - DNS Id Spoofing with sniffing
    - DNS ID spoofing without sniffing

IV. RELATED WORK

This section describes the solutions, i.e. detection of phishing and Pharming attack and steps one should take for protecting Phishing and Pharming attack. This section will also describe the issues related to the corresponding solution.

A. Survey on Phishing and Pharming attack

a) Detect Pharming attack using Dual Approach [5]

In this dual approach to detect Pharming attack are authenticate each website. In this approach, a framework analyzes both website content of HTML font, Images and logo. Also check the IP address using of multiple DNS server to detect the lure site. In this approach is also developed a browser plug-in.

When user is sending request on browser. First it will check the IP address on local DNS server. DNS server send requested queries into two different servers. One is default and second is third party server. If default DNS server responds from the IP address then responding queries redirect on browser. Another third party are including with default IP so it is a legitimate site. Analysis of IP address, it will be a check the HTML code of visited webpage. When installing the Anti-Pharming solution, user is asked to choose the third party DNS Server among to pre-defined list of DNS server.

Issue with Dual Approach

1. Each and every time requested queries sending into two different DNS server.
2. It reduced a browsing speed.

b) A Layout-Similarity-Based Approach [6]

In this layout similarity based approach is stored sensitive information of each website. In this approach detect the phishing site using of DOMAntiPhish plug-in. When user enters any sensitive value on webpage of any domain. AntiPhish to store that information with the domain. Each time AntiPhish needs to check that sensitive information which are stored in particular domain. But it is not so much trusted.

Issue with a Layout-Similarity-Based Approach

1. Attacker had made any combination of images to creating spoofed web page that look like legitimate web page.
2. Attacker takes conservative approach to reducing the phishing threshold alert.

c) Visual Similarity based Approach [8]

In visual similarity based approach is determined that user need to take snapshot of the any web page which are store in the database. If user wants accessing any webpage it required entered snapshot into URL, which is already available into the database. Database contains multiple images of legitimate website. If the images is matches with the database than it redirect to user browser, and if it does not match then it will be a fake site.

Issues with this approach

1. It reduced a browsing speed.
2. Images stored in database so it needs to maintain backup.
3. It requires more processing power.

d) Content based Approach [9]

In this approach, Main aim is to detecting fraudulent website with help of Html Content. Fraudulent website found will be found during the analysis process. It can be displaying active and passive warning alert on browser. Active alert is a pop-up alert message on browser. In this approach, both IP address and webpage content to be analyzed during the whole process. Browser will be comparing the local DNS also with public DNS server. If IP address is differs then it is open prompt box with message of page is not legitimate site. If IP address is matched then it considered as genuine page.

Issues with this approach

1. Each and every time requested queries sending into two different DNS server.
2. It reduced a browsing speed.

V. COMPARATIVE STUDY

Criteria Group →	Security oriented measures					Others						
Individual Criteria → Providers ↓	SSL Check ?	Encryption used?	Hashing mechanism	Browser Protection?	Email Security ?	DNS Used	IP check and content analysis	Client or Server side ?	Algorithm used ?	Implementation result shown ?	Any Antiphishing method ?	Overhead
[3]	√	√	x	x	√	√	x	C	√	√	x	↑
[7]	x	x	x	x	x	√	√	C	x	√	x	↑
[9]	√	x	x	√	x	x	√	C	x	√	x	↑
[10]	x	√	x	√	x	√	x	C	√	√	x	↓
[11]	√	x	√	x	x	x	x	C	√	x	x	↓

Table IV (e). Comparative study

The table shows above gives detailed comparison about the various schemes proposed by a researcher. The table gives the description about the basic technique used with the benefits that researcher gets as well as the limitations found in schemes.

B. Protection against Phishing and Pharming attack

There are many protection approaches against Phishing and Pharming attack as discussed below:

a) Server side filters and classifier

Server side filtering is based on content-based filtering approach. Server side filter are considered as the best option to fight zero day attack.

b) Securing Router

Home user or an organization should not use default password of router. Password should not be dictionary word in order to prevent it from dictionary attack. Users should change the default password settings on the broadband router or wireless AP. Choosing a more complicated password will provide an added layer of security.

c) Authentication mechanism

There are some simple solutions that now a day's banking site using. Instead of asking username and pass
Gmail has implemented this feature, which will send SMS to the user once it enters valid username and password. User would able to access account only when randomly sends code would be entered by user.

Another non technical approach is that user should enter wrong username and password to the banking or E-commerce sites, If it shows error message, then it is legitimate one, and if it redirects you to same page, or not prompt error message even after entering invalid username and password, then consider it as a fake page.

d) Secure HTTP

HTTPS is the most efficient way to prevent against Pharming attack. An expire certificate or certificate from an unfamiliar organization should not be accepted.

VI. CONCLUSION

In this paper, we studied various research proposals on Phishing, Pharming and spoofing attacks, using DNS (Domain name system) to increase the accuracy level of email spoofing over network. We also made a comparative table which can be used by layman to have handy information about the proposals. Some of the proposals are based on IP checking, web content analysis and SSL checking and so on. We believe that Phishing and Pharming attacks are an area packed of challenges and of vital significance, and many research problems are yet to be identified.

REFERRENCES

1. Network Working Group, "Domain Name- Concepts and Facilities [online]" ; Available: https://www.ietf.org/rfc/rfc1034.txt
2. A.S. Zadgaonkar, Suresh Kashyap and M. Chandra Patel "Developing a model to detect email address spoofing using biometrics technique", *IJISMR* 2013, p.63-65.
3. D. Mooloo; T.P. Fowdur, "An SSL-Based Client-Oriented Anti-Spoofing Email Application", IEEE 2013, p. 1-5.
4. Ivana C.; Andre A. and Sebastien M., "Biometrics Evalution under Spoofing Attacks", *IEEE 2013*, p. 1-13.
5. Gastellier-Prevost, S.; Granadillo, G.G.; Laurent, M.," A dual approach to detect Pharming attacks at the client-side", *IEEE 2011*, p.1-5.
6. Angelo P.E. Rosiello, Engin Kirda, Fabrizio Ferrandi, "A layout-Similarity-Based Approach for Detecting Phishing Pages", IEEE 2011, p. 1-10.
7. Sophic Gastellier-Prevost and Maryline Laurent "Defeating Pharming attacks at client side", IEEE, 2011, p. 33-40.
8. M. Hara, A. Yamada, and Y. Miyake, "Visual similarity-based phishing detection without victim site information", Nashville, Tennessee, USA: IEEE, 2009, p. 30-36.
9. Omer Mahmood, "Three phase Checking against Phishing and Pharming attacks", *Proc. 11th Annual Conf. on Asia Pacific Decision Sciences Institute*, Hong Kong, June 14-18, pp. 399-402.
10. S. Stamm, Z. Ramzan, et Jakobsson Markus, Drive-By Pharming, Proceedings of the 9th international conference on Information and communications security, Zhengzhou, China: ACM, 2007, p. 495-506.
11. Baber Aslam, Lei Wu and cliff C. Zou, "PwdIP-Hash: A lightweight solution to Phishing and Pharming Attacks" *School of Electrical Engineering and computer science, University of central Florida*, Orlando, FL,USA.2012.