NOVEL APPROACH TO DETECT AND PROTECT AGAINST PHARMING ATTACK

[1]Jayshree Upadhyay, Assistant Professor, Aditya Silver Oak Institute of Technology, Ahmedabad, [2]Sagar Patel, Assistant Professor, Aditya Silver Oak Institute of Technology, Ahmedabad, [3]Manish Singh, Assistant Professor, Aditya Silver Oak Institute of Technology, Ahmedabad

***Abstract*— Pharming is an advance phishing attack. It is also known as “phishing without a lure”. A hacker's attempt to change/exploit the DNS settings of a server so that when you enter the address of a legitimate website, it redirects you to a fake/copy of the original site hosted somewhere else. There are multiple ways to redirect user to the attacker’s site. This thesis report covers attack classification which may leads the user to the fake site under the control of attacker. Literature survey explains the existing solution for detecting and protecting against Pharming attack with its consequences. This paper proposes innovative lightweight method for detecting and resolving pharming attack. Paper also consist implementation of proposed solution and result analysis and comparison of results with existing approach.

***Index Terms*— Pharming, Phishing, Advance Phishing Attack**

I. INTRODUCTION

In a simple language, advance level of phishing attack is known as pharming attack. Both Pharming and phishing are well-known to steal the identity of user. Pharming can also refer as “Phishing without lure”. Phishing uses fraudulent e-mail messages to lure you to fake Web sites and try to get you to supply personal information like account passwords, pharming attacks redirect you to a hacker's site even when you type the address of a real site into your browser. Generally, to make phrming attack successful, attacker needs to either modify local host entry, or IP configuration of client system, or needs to exploit the vulnerabilities of DNS server. Pharming attack can also be achieved in internet scenario [1]

Pharming attacks are much more difficult to detect as compare to phishing attack. Because both the visited URL and the website are similar to the legitimate site. Pharming attacks aim to corrupt DNS information to redirect users to a fake website under the control of the attacker. To perform phishing, attacker has to send some sort of mail which contains link, which make user click on that, so phishers has to approach target one by one. In pharming attack, if Attacker compromise DNS server, then all the client who so ever are referring that DNS server will be redirected to the attacker’s site which may looks like the legitimate site. So we can say that Phishers have to approach their targets one by one, where as Pharmer’s can scoop up many victims in a single pass. [1, 2]

With phishing attack, it is very easy to recognize attack by just observing URL, whereas in Pharming URL observation will not help, as attacker is going to modify DNS entry. So even though user is typing correct URL, it would be redirected to fraudulent web page. So here URL observation will not help. [1, 2]. Currently, pharming does not appear to be as common as phishing. However, many computer security experts are predicting that pharming attacks will continue to increase as more criminals embrace these techniques.

RELATED WORK

To make the pharming attack most successful, one needs to exploit vulnerable DNS server. Most of the attack scenarios of pharming attacks are based on DNS. Attacker may manipulate the DNS entries to redirect the users to fake website. Some well-known attacks are Localhost attack, DNS cash poisoning and DNS spoofing attack. Attacker may implement rouge DHCP server to assign IP address of fake DNS server as a primary DNS IP in order to achieve the pharming attack. In order to detect the pharming against such mentioned DNS attacks, various solutions are provided. In this section we would understands such approaches.

Dual Approach [8]

In this approach, browser plug-in has been developed. So when ever user is requesting to the website, first it will check the IP address resolve by the local DNS. And another query will be sent to the public DNS, which would be legitimate. Then it compares the IP address which it got from both DNS servers. If IP address differs than it will prompt that this page is suspicious. If it matches the IP address, then it will be consider as genuine page. There are various issues associated with this approach.

Issues with this approach

- It will slow down the browsing speed, as for each and every site it is sending request to two different DNS server.

- The third-party DNS or Open DNS server responses can greatly vary according to the location from which the DNS query was launched. For example, if we are referring open DNS server of google from India, and if we are trying to access some site which is local to India, than DNS entry of local and open DNS will be differ, even though both are contains legitimate entry.

Web Page Signature matching [9, 10, 11]

In this approach, signature from the webpage will be extracted, and will compare it with available database. So here database server will be maintained. If it matches the signature, then not an issue. If it does not match the signature than page might be under Pharming attack.

Issues with this approach

- Web pages content is more and more dynamic, by integrating ads, RSS feeds, etc.
- Phishing and legitimate sites use both absolute and relative paths for images, links, etc.
- Attackers create phishing/pharming site very similar to the legitimate one, by using mirroring tools and keeping links to the legitimate site as much as possible. They
- Modify minimal part of the legitimate site to lure as many users as possible
- Additional script can be added to the HTML content depending on the web browser of the user (Internet Explorer, Firefox, Opera, …)
- HTML structure of the same webpage can be very different in terms of organization, links, depending on the location where the webpage is downloaded.
- It is difficult to detect Pharming attack for new site, as signature of new site might not be available into the database.

Visually Similarity based approach [12]

In this approach, author has suggested to take the snapshot of entered URL. After getting an snapshot, image will be compared to the database, which is already available for various and well-known sites. Database also contains images of the websites. It is going to compare recently taken image with database image, if it matches, then check the domain name for correspondence image. If domain name also matches then there is no issue, and if it does not match then site might under Pharming attack

Issues with this approach

- It require more processing power to perform image processing.
- It is going to decrease browsing speed
- Image of the web page may change dynamically over period of time.

Webpage content comparison [13]

This approach is successor of Dual mode approach (A) for Pharming detection. In this approach, an agent which is installed as browser plug-in will first compare the local DNS response with public DNS response. If it differs, then it will compare the html code of the both pages which are responded by local DNS as well as from public DNS. On the base of threshold value it will prompt the user about the Pharming attack.

Issues with this approach:

- It will slow down the browsing speed, as for each and every site it is sending request to two different DNS server.
- DNS response may differ if we are using public DNS of some different region, and after that, content of the webpage also differs according to geographical location (google.co.in for India, google.co.au for Australia).
- Comparing the content of entire webpage will require more processing power and it will reduce the browsing speed.

After analyzing related approaches and solutions, it is clear that none of the reviewed solutions provide efficient method to ensure the security against Pharming attack.

PROPOSED SOLUTION

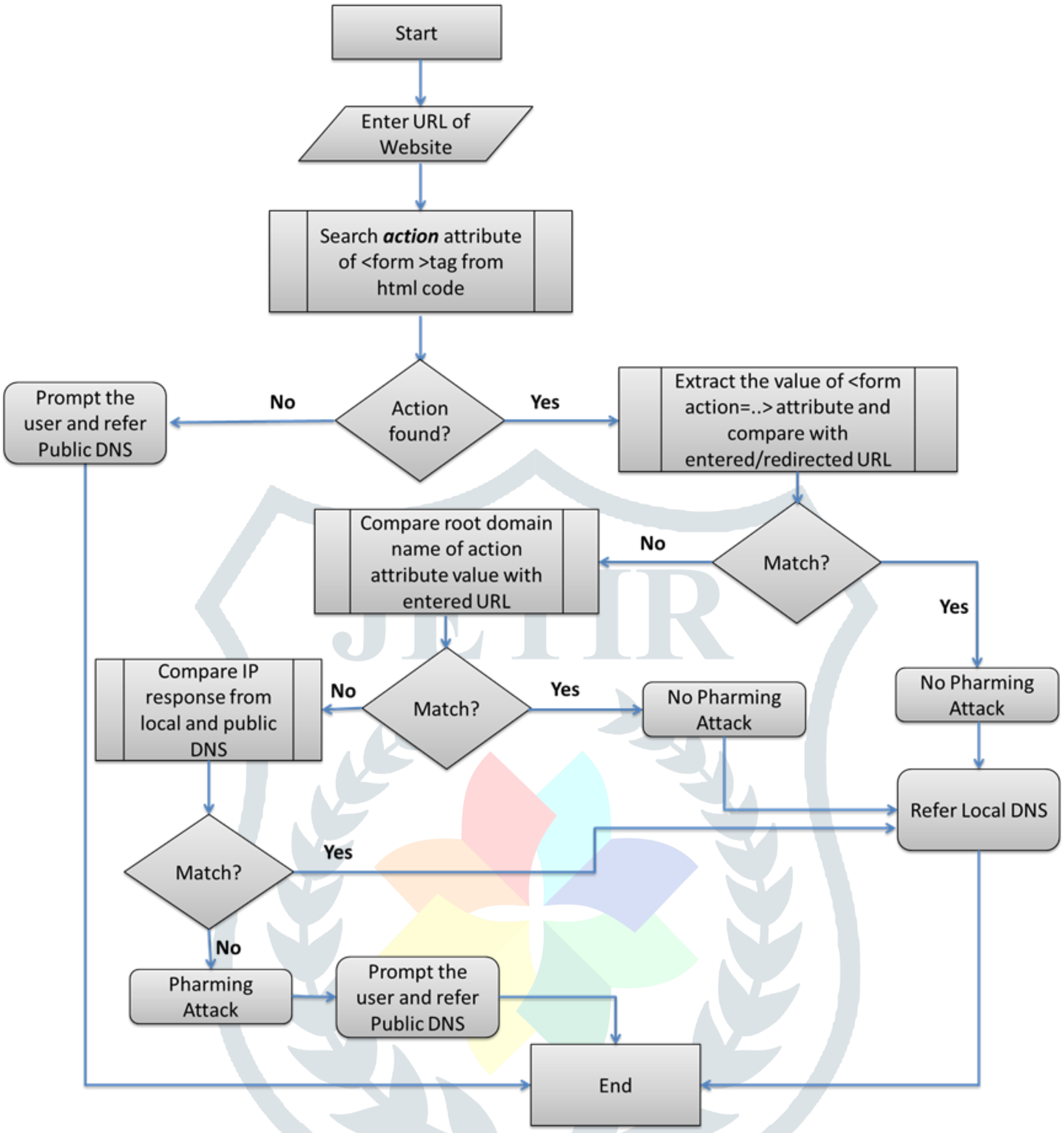

Start
Enter URL of Website
Search action attribute of <form >tag from html code
Action found?
No
Yes
Prompt the user and refer Public DNS
Extract the value of <form action=..> attribute and compare with entered/redirected URL
Match?
No
Yes
Compare root domain name of action attribute value with entered URL
No Pharming Attack
Compare IP response from local and public DNS
No
Match?
Yes
No Pharming Attack
Refer Local DNS
Match?
Yes
No
Pharming Attack
Prompt the user and refer Public DNS
End

Figure 3.1: Proposed architecture

IMPLEMENTATION

In order to implement the scenario, python programing language has been chosen. Customize browser has been developed with proposed idea implemented within that to prove the concept. As far as length of code is concerned python is most efficient language [17, 18, 19]. As a part of implementation, following attack scenario has been generated.

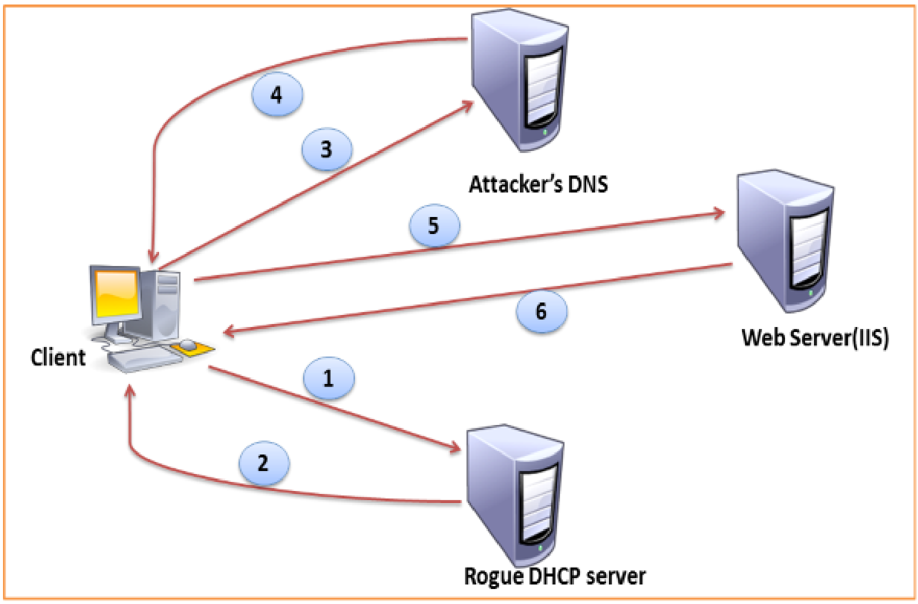
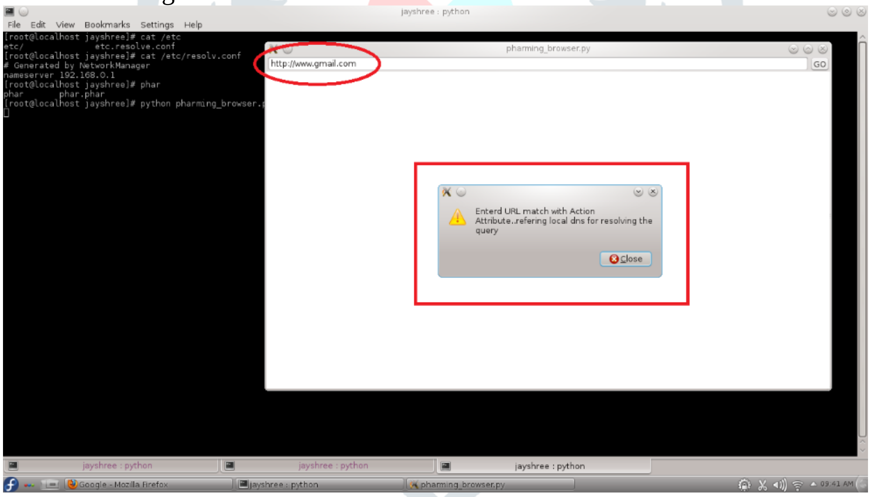


Figure 4.1: Implementation Scenario

At the client end, customized browser which contains proposed idea implemented, has been used to test the scenario. This browser contains limited functionality like surfing the web pages. Along with limited functionality code has been implanted to detect and resolve the Pharming attack. Following is the supporting snapshot for demonstrating browser's surfing capability. Methods to detect and resolve Pharming attack has been integrated with the browser code. Following are the supporting snaps for fully functional browser for Pharming attack detection and resolution. In order to demonstrate successful functionality of code, prompt window contains various messages for various situations.



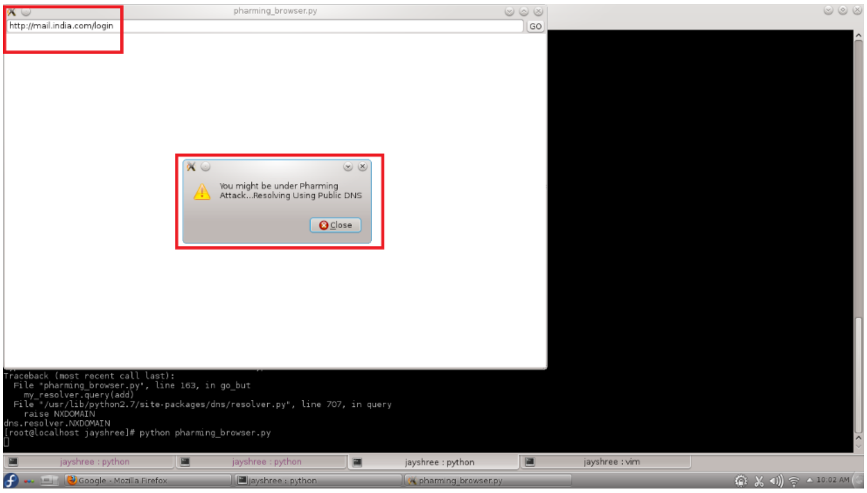
```
[root@localhost jayshree]# cat /etc
etc/                etc.resolve.conf
[root@localhost jayshree]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.0.1
[root@localhost jayshree]# phar
phar        phar.phar
[root@localhost jayshree]# python pharming_browser.p
```

http://www.gmail.com

Enterd URL match with Action Attribute..refering local dns for resolving the query

Figure 4.2: Accessing genuine gmail's page

To test the case of sites which might be under Pharming attack, we hosted various sites on local web server, with changed action attribute value. In that case browser would prompt warning of phaming attack, after that would resolve the query using public DNS.



You might be under Pharming Attack...Resolving Using Public DNS

```
Traceback (most recent call last):
  File "pharming_browser.py", line 163, in go_but
    my_resolver.query(add)
  File "/usr/lib/python2.7/site-packages/dns/resolver.py", line 707, in query
    raise NXDOMAIN
dns.resolver.NXDOMAIN
[root@localhost jayshree]# python pharming_browser.py
```

Figure 4.2: Suspicious Page

Result has been generated for 880 total site against the existing approach. False positive rate for the existing approach has been calculated on the bases of threshold value, which is as follows:

Threshold	Total Sites (Genuine + Fake)	FP Rate
100	880	31.57%
99.5		46.49%
98		53.35%

Table 4.1: False positive rate of existing approach [13]

Total Sites (Genuine + Fake)	FP Rate
880	8.88%

Table 4.1: False positive rate of proposed approach

As per Table 4.1 and 4.2, clear difference evident in improved manner. Even though previous approach considers 100% threshold value to compare web page, it is having higher false positive rate as compared to proposed scheme. Due to dynamic nature of web sites it is not feasible solution to compare the content of web pages returned from different DNS to 100%. But problem with previous approach is that if it reduces the threshold; false positive rate dramatically increase.

So it is unambiguous to say that proposed approach is consuming less processing time and decrease the false positive rate as compare to the approach [13] mentioned in section 2.4.4.

CONCLUSION

Main motive behind launching Pharming attack is to steal personal information like banking or credit cards details and credentials associated with personal. To achieve it, attacker needs to design fake page which appears identical to the legitimate one. This proposed method would work on both client and server side attack scenarios. It would first detect the Pharming attack and if attack is detected, refers public DNS settings for further browsing.

Result evaluation and analysis section of thesis report proves that proposed scheme consume less processing time as compared to existing approach. It results in increase browsing speed. It is also unambiguous to say that proposed approach reduces the false positive rate.

However implementing such mechanism in browser will take more execution time as compared to normal web page execution. But, security is more important than the speed, especially in case of E-transaction. Therefore to provide maximum security against Pharming attack one should integrate multiple solutions, which would reduce the false positive rate and increase browsing speed.

References:

[1] S. Stamm, Z. Ramzan, et Jakobsson Markus, “Drive-By Pharming,” Proceedings of the 9th international conference on Information and communications security, Zhengzhou, China: ACM, 2017, p. 495-506.

[2] G.Ollman,Jul.2017,“The Pharming Guide[online]”; Avalibale: http:// www. Ngssoftware. com / papers/ ThePharmingGuide.pdf.

[3] Microsoft Corporation, 2017, “ Domain Name System [online] ”; Available :

http://technet.microsoft.com/en-us/network/bb629410.aspx

[4] C. Jackson, A. Barth, A. Botz, W. Shao, et D. Boneh, “Protecting browsers from DNS rebinding attacks,” ACM, vol. 3, Issue 1, Jan.2014.

[5] C. Karlof, U. Shankar, J. Tygar, et D. Wagner, “Dynamic pharming attacks and locked same-origin policies for web browsers,” Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Viriginia, USA: ACM, 2007, p. 58-71.

[6] Y. Cao, W. Han, et Y. Le, “Anti-phishing Based on Automated Individual White-List,” Proceedings of the 4th ACM workshop on Digital identity management, Alexandria, Viriginia, USA: ACM, 2008, p. 51-60.

[7]A.P.E. Rosiello, E. Kirda, C. Kruegel, et F. Ferrandi, “A layoutsimilarity- based approach for detecting phishing pages,” Nice, France: IEEE, 2007, p. 454-463.

[8] Gastellier-Prevost, S.; Granadillo, G.G.; Laurent, M.,” A dual approach to detect pharming attacks at the client-side”, IEEE 2011, p.1-5.

[9] Chih Sheng Chen, Shr-An-Su,Yi-Chan Hung,Jun. 7,2011, “Protecting computer users from online fraud”, US patent number US7,85,555 B1

[10] Chao-Yu Chen,Tse-Min Chen,Aug.14,2012,”Autonomous system based Phishing and Pharming Detection”,US patent number US 8,245,304 B1

[11] Jung Min KANG,Do Hoon LEE,Eng Ki PARK,Choon Sik PARK,FEB. 26,2009”Method and apparatus for providing phishing and pharming Allerts”,US patent number US 2009/0055928 A1

[12] M. Hara, A. Yamada, et Y. Miyake, “Visual similarity-based phishing detection without victim site information,” Nashville, Tennessee, USA: IEEE, 2015, p. 30-36.

[13] Gastellier-Prevost, S.; Laurent, M.,” Defeating pharming attacks at client side”, IEEE, 2016, p. 33-40.

[14] Marasu T., “An HTTP Extension for Secure Transfer of Confidential Data”, IEEE International conference on networking, Architecture and Storage, 2016, p. 12-20

[15] Netscape, “SSL3.0Specification” 1996, [Online], Available: wp.netscape.com/ eng/ ssl3/ draft302.txt.

[16]Github,” Benchmarking of programming language[Online]”, Available: attractivechaos. github. com / plb/

[17] “Statement Ratio [Onine]”, Available: http://www.codinghorror.com/blog/2005/08/are-all-programming-languages-the-same.html

[18] Li Jun; Li Ling, “Comparative research on Python speed optimization strategies”, ICISS, 2010, p. 57-59

[19] Guan, Bei; Wu, Yanjun; Wang, YongJi, “A Novel Security Scheme for Online Banking Based on Virtual Machine”, IEEE sixth international conference on software security, 2012, p. 12-17