IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013), PP 66-72
www.iosrjournals.org

A survey on Pharming attack Detection and prevention methodology

Jayshree Patel[1], Prof. S.D. Panchal[2]
[1]*IT Systems and network Security, Gujarat Technological University, India*
[2]*CE Department, VGEC, Chandkheda, India*

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. It is a classy edition of phishing attacks – endeavor to take users' identification like username and password by redirecting them to a fake website using DNS-based techniques.*

Pharming attacks can be performed at the client-side or into the Internet. This attack will be affecting large group of computers within single instance. As compare to phishing attack, In pharming attack , attacker need not targeting individual user. If pharming is performed by modifying the DNS entries, than it will be affecting to all the users who is accessing the web page through that DNS. Pharming attack may not be identified just by observing the URL, as URL will be the legitimate, not the site.

Keywords - *Pharming, advance phishing, prevention against Pharming attack, detecting Pharming attack*

I. INTRODUCTION

Pharming an advance phishing attack. Both Pharming and phishing is used to online identity theft. 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. Like phishing, pharming coerces victims into visiting a fake website and supplying information. However, instead of tricking recipients into clicking on an email link, pharming can secretly redirect victims to a fraudulent website directly from their web browser. Pharming effectively eliminates the need for "bait" emails and is therefore potentially more dangerous than "normal" phishing scams and can cast a wider "net" in which to snare victims. Even phishing-savvy web users could fall victim to a Pharming scam without realizing it.[1]

In order to make pharming work, attackers may compromise a victim's system directly by secretly installing malicious software on his or her computer or modifying the host file. Alternatively, the scammers may use "DNS cache poisoning" to effectively compromise the DNS server. What this means in plain English is that, even if you manually enter the web-address of your bank or financial institution directly into your browser, or click on a saved bookmark, it is possible that a pharming attack could cause your browser to unobtrusively redirect to a fraud site. If the scam site is made to resemble the legitimate website of the targeted institution, a victim could enter account numbers, passwords and other sensitive information before he or she realized what was happening. [2,3]

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, which I will be discussing in detail in later section.

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 performs 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. 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. [4]

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. [5]

Section II contains various attack scenarios to Perform Pharming attack; subsequent section III contains related work which describes the existing solutions and some of the prevention techniques for Pharming attack. Last section concludes the work.

II. ATTACK SCENARIOS

For the last ten years, the proliferation of fake websites lead researchers to propose many approaches for counteracting identity theft based attacks. Most of these approaches focused either on phishing attacks - by providing multiple detection techniques such as blacklists, heuristics, authentication schemes, etc. - or on DNS-based attacks performed in the ISP network or at the server-side. In this section, we discuss pharming attacks performed at the client-side as well internet side in detail.

pharming attack can be done on

- Client side
- Internet

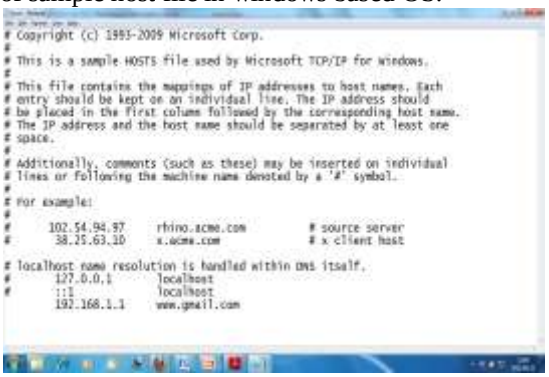
A. Pharming Attack at Client Side

Local host attack

Local host attack statically modifies the victim's operating system host files to redirect the user's traffic to a domain under the attacker's control. Whenever client browser request for the web page, first it is going to check the host entry in hosts file. So in this case, attacker will statically modify host file entry, so the user will unknowingly redirect to the fake page. Same method can be used to block the site at local level. [6, 8]

For windows based Operating System, hosts files are located under *"C:\Windows\System32\drivers\etc\hosts"*.For Linux based system, location of host file would be *"/etc/hosts"*.

Following is the snapshot of sample host file in windows based OS.



Windows local host file

If you observe the figure1 closely, then last made is, 192.168.1.1 and host name is *www.gmail.com* , So when user's browser try to locate URL same as mentioned, then it will be redirected to the 192.168.1.1, which is definitely not the IP address of legitimate gmail's server.

Browser Proxy Configuration Attack

Browser proxy configuration attack overrides the victims' web browser proxy configuration options, using DNS spoofing or poisoning techniques, to redirect all the web traffic to a fraudulent proxy server that is under the attacker's control. Another type of browser attack - DNS rebinding attack - tends to convert the user's web browser into an open network proxy[3] , e.g. the client's browser can visit a malicious website that embeds a Flash movie which opens a socket to an arbitrary port number rebounded by the attacker. As a result, the attacker is enabled to read arbitrary documents, compromise internal machines, hijack some IP addresses, etc. [6,7]

Rogue DHCP

In this attack scenario, Attacker installed fake DHCP server in to client's network scenario. To understand this attack scenario, it is essential to understand how DHCP works.

Let us assume that there are two DHCP servers available in network. One is legitimate and another is rogue. Scenario will works like following.

- DHCP client broadcasts a DHCPDISCOVER packet
- DHCP servers broadcast a DHCPOFFER packet. In this case both legitimate and fake will broadcast DHCPOFFER packet, and freeze the IP address to assign it to the client
- After getting DHCPOFFER packet, DHCP client unicast a DHCPREQUEST packet. Here client will send DHCP request to the server from whom it is getting first DHCPOFFER packet. So if it is getting request from fake one before legitimate, then fake server will assign IP address pool, which contains IP, Subnet mask, default gateway, and DNS server's IP, by broadcasting DHCPACK packet.

So if rogue DHCP server provides wrong IP pool, which contains the DNS server IP, which would be attacker's DNS server, then all DNS query will redirected to the fake DNS server. [6, 7]

Home or border router attack

In this, attacker uses the vulnerabilities of router or gateway in order to exploit it. Once it get access to the router, he will modify the DNS entries in to the router, so the entire network behind that router will affected by pharming attack. So compromised route will leads to the pharming attack. [8]

B. Phamring attack at Internet

Another approach of pharming attack is it can be done on Internet, or ISP side. In this section I am going to explain various attack scenarios for Internet.

Domain Hijack

In order to access website through internet, we need to register domain name to the naming authority in order to avoid name conflict. Domain name is having limited lifetime, that is depend on the package you are choosing from the hosting provide sites. Through this technique, a domain that has just expired is purchased someone else with malicious purposes. [8, 9]

Similar Domain Name

The attacker can register multiple spelling permutations of the targeted domain name in order to lure users, for instance, an attacker can register a domain name that adds an extra words to the legitimate domain name, e.g. *www.bank.au.com* can be used to fake the bank's site *www.bank.com*. [8,9]

Transparent Proxy

It is a proxy server, which lies between end user and internet. User is not aware about existence of it. Basic usages of such proxies are to increase the speed of internet access.

Squid-imposter is an example of that which is squid based proxy, which can add html page for offline storage, it inject URL contents to your browser, that is the feature of HTML5 offline cache feature.Even though client is not connected to proxy after that, that offline content will remain there for long time. So, transparent proxy can be installed in the Internet to force the client's outgoing traffic to be redirected through the attacker's server [8,9]

DNS cache Poisoning

In DNS cashing, client will first send the query to the local DNS server, if entry not found then local DNS will forward the query to public DNS like the same way that I explained in iterative query. Once Local DNS get the authoritative response (refer figure 2.2(b)), local DNS will store the result in local cache for faster access for next time. It will maintain entry in tabular format which contains hostname, IP address, and TTL value. So the query for same host name will further resolved from local DNS cache only. [8,9]

So in this scenario, attacker will takes the advantage of DNS server's caching vulnerability. Attacker would add multiple fake resolution entries to host, so that a DNS query for a particular domain name resolves into the attacker's IP address. [8,9]

DNS spoofing attack

In this scenario, attacker will add its own DNS server into network, and pretend like the legitimate server. It can be achieved via various ways.

One can achieve this attack by sending the crafted packet to the client, which appears as packets are coming from legitimate DNS server. In that attacker has to take care that crafted packet should contains source IP as legitimate DNS IP, source port should be legitimate DNS port, i.e. 53, destination ip and port would be clients IP, Port, and most important this is UDP checksum. So it is really difficult to achieve. [8]

Another way to achieve this is to perform MITM attack, and capture all traffic of client and DNS. One attacker is able to capture traffic, between client and DNS, attacker will launch DoS attack on legitimate DNS server and make it unavailable. [10]

III. RELATED WORK

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

PROTECTION AGAINST PHARMING ATTACK

There are some precautionary measures that one should take in order to protect against pharming attack. That I am going to explain in detail in this section.

i. Secure HTTP [13,14,15]

To cope with the HTTP problems above, servers usually start the Secure Socket Layer (SSL) protocol (or its standardized version, Transport Layer Security (TLS) protocol; the HTTP with the SSL protocol is called HTTPS. The SSL supports server authentication and optional user authentication. However, the server usually authenticates the user by the username-password pair since otherwise the users have to register themselves to Certificate Authorities (CAs). On the other hand, the server authentication is not so convenient to use because of complex manipulations on the records in CAs; in establishing a secure channel of the SSL, the browser confirms the server's domain-name certificate signed by the CA, next chooses a random key shared with the server and used to protect the confidentiality and integrity of requests and responses. Thus HTTPS can prevent against phishing and pharming attacks.

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

However, the SSL has not been so widely deployed due to the complexity of cryptographic techniques in establishing the secure channel; a one-processor server with HTTPS is about 5 to 7 times slower than that with HTTP.

ii. 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.

It is suggested that router should be reset its all configuration before changing password. This step ensures that if users are already victims of a drive-by pharming attack, they can start with a clean slate at the router level.

iii. Authentication mechanism

- There are some simple solutions that now a day's banking site using. Instead of asking username and password at single instance, site should prompt password page , once user enters valid name. By implementing this mechanism, we can protect ourselves from pharming and phishing attack.
- Another approach that helps for protecting against phishing and pharming is two factor authentications. 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 one should try is, instead of using correct username and password, 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.

iv. Other protecting measures [14]

- Use legitimated and trusted internet service provider
- Check the browsers URL, to make sure spelling is correct for protecting against similar domain name attack.
- Verify the certificate of the site, whether it is legitimate or not.
- Download and install latest security updates for your web browser, Operating system, antivirus and firewall to avoid client side attack. As implementing security at multiple level is known as Defence in depth.

DETECTION AGAINST PHARMING ATTCK

Detection methodology will be used when user is accessing the webpage. It is going to prompt the user, if the site is suspicious or not.

i. Dual Approach

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 send 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. [8]

When installing the anti-pharming solution, the user is asked to choose the third-party DNS server among a pre-defined list of DNS servers (e.g. OpenDNS, Google DNS, etc.). We recommend the user to choose a third-party DNS server different from his IS. [8]

Issues:

- 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.

ii. Webpage Signature matching

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. [9, 10, 11]

Issues:

- 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.
- So, analyzing a webpage based on its structure and type of links can give high false positives rates

iii. Webpage content comparison [13]

This approach is successor of Dual mode approach (B-i) 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. [12]

Issues:

- 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.

iv. Visual similarity based detection [13]

In this approach, URL and Image of the website which is stored in predefined database will be compared. Fig 2. is explains this approach via Flow chart. Fist it will take snapshot of the visited site, and compare it with image database ,if it compare the image then it will check domain name, if it is correspond, then that will be legitimate page. If image is not matched, then output will be stored in unknown. And if Image match and URL don't match then that will be the phishing site.

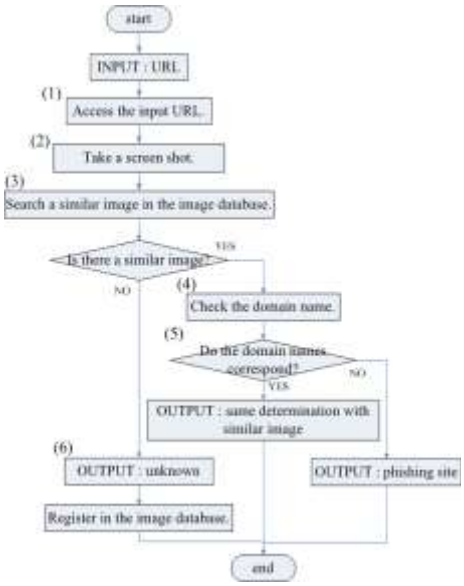


Fig 2. Visually similarity based approach

Issues:

- Would spend more time and consume more processing power in comparing images
- As per study, this is not full proof method, statistics shows that out of 1,868 sites 18.0 % sites has given false positive, as now a day images may change dynamically.

IV. CONCLUSION

Pharming is a very serious attack, and ISPs are implementing security in order to protect agaist pharming attack. To protect against pharming attack, user needs to understand basics of attacks and some basic steps though which user would protect his or her identity or credentials. All the detection techniques described in report are effective, but none of them is providing high accuracy. All of these approaches are suffering from high rate of false positive. Similarity assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. But sometime, security is more important than the speed, especially in case of E-transaction. So to provide maximum security against attacks one should integrate multiple solutions, which would reduce the false positive rate and increase browsing speed.

Acknowledgements

We take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this survey paper. We wish to express our sincere gratitude to Prof. S.D. Panchal, HOD IT, VGEC, Chandkheda, Ahmedabad, Gujarat. We can't say thank you enough for his tremendous support, motivation and help. We would also like to express our gratitude to Mr. Naresh Kumar Gardas, course coordinator, C-DAC and Ms. Kiran Bhagiya, Coordinator, GTU for having permitted us to carry out this work and for all valuable assistance.

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, 2007, p. 495*-506.
[2] G.Ollman,Jul.2005,The Pharming Guide[online]; Avalibale: http:// www. Ngssoftware. com / papers/ ThePharmingGuide.pdf.
[3] Microsoft Corporation, 2013, 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.*2009.
[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] Gastellier-Prevost, S.; Laurent, M., Defeating pharming attacks at client side, IEEE, 2011, p. 33-40.
[13] M. Hara, A. Yamada, et Y. Miyake, Visual similarity-based phishing detection without victim site information,"Nashville, Tennessee, USA: IEEE, 2009, p. 30-36.
[14] Marasu T., "An HTTP Extension for Secure Transfer of Confidential Data", IEEE International conference on networking, Architecture and Storage, 2009, p. 12-20
[15] Netscape, "SSL3.0Specification" 1996, [Online], Available: wp.netscape.com/ eng/ ssl3/ draft302.txt.