Client – Side Pharming Attacks Detection using Authoritative Domain Name Servers

Ibrahim S. Alfayoumi
Faculty of Information Technology
The Islamic University of Gaza
Gaza, Palestine

Tawfiq S. Barhoom
Faculty of Information Technology
The Islamic University of Gaza
Gaza, Palestine

ABSTRACT
Pharming attacks can be performed at the client-side or into the internet. In pharming attack, attackers need not targeting individual user. If pharming is performed by modifying the DNS entries, than it will be affecting to all users who is accessing the web page through that DNS. We propose an approach to protect user at client-side from pharming attacks by comparing IP addresses, using information provided by local DNS server and a list of IP's provided by the domain's Authenticated Name Servers which are the most trusted DNS servers for a domain.

General Terms
DNS security, DNS queries, DNS Poisoning, Pharming attacks

Keywords
DNS, Pharming, Client-Side, Authoritative Name Server, Detecting pharming attack

1. INTRODUCTION
Pharming is an internet scamming practice in which malicious code is installed on a person computer or server misdirecting users to fraudulent website without knowledge or consent. Pharming has been called "phishing without a lure". For example, imagine that whenever a user want to go to his bank, he pick up a phone directory and lookup for his bank's address, once user have his bank's address he go directly to his bank account. In pharming, attackers replace the phone book with a fake one they created.

Now when user pick up that raw from the phone book he will actually get the wrong address, at this wrong address the attackers will have setup a fake bank account page similar to user's real one, when user do business with the fake page he will give all his sensitive information for the attacker including his name, credit card number and password. However user will never realize that he were in a fake bank since he trusted the address that had been given to him. Large number of users can be victimized because attacker does not need to target users one by one, one successful attempting poisoning the DNS server can be potentially used to trick all users of that DNS server. Since pharming does not rely on the victim taking an action that leads to information theft, it is much more difficult to identify and thus far more effective.

DNS vulnerabilities can be exploited at the client-side by corrupting the user/company computer or the border router, but also in the ISP network or at the server-side by intercepting, modifying or spoofing DNS exchanges as well as using content injection code techniques. Most of the papers that proposed third party DNS server detection hade the same problem which is the third-party DNS server responses can greatly vary according to the location from which the DNS query was included - geographic location -.

An Authoritative name server is a name server that gives answers in response to questions asked about names in a zone. An authoritative-only name server returns answers only to queries about domain names that have been specifically configured by the administrator. Name servers can also be configured to give authoritative answers to queries in some zones, while acting as a caching name server for all other zones. [1]

This paper presents our idea of detecting pharming attacks at the client-side by comparing the IP address resolved by local DNS. And another query sends to the domain's Authoritative Name Server as the most trusted and legitimate server, which will resolve all IP addresses of the domain.

These IP addresses will be compared with the result of the local address, if this compare doesn't match with any of the listed IP addresses, then a Pharming attack will be detected.

This paper is organized ass follow: Section 2 introduces all types of pharming attacks. Section 3 describes detection methodologies against pharming attack. Section 4 details our idea and gives first experimentations of how to detect all IP addresses from Authoritative Name Server. Section 5 shows the result on real environment using our implementation. Section 6 discuses ISP DNS environment and Section 7 is Conclusion.

2. PHARMING ATTACK DESCRIPTION
In this section, we'll describe Client – Side pharming attacks types. [2, 3] A number of pharming attacks are performed at the client-side by modifying the local lookup attacks at the user's environment such as:

Local host attack: by modifying the victim's operating system host files to redirect traffic to an attacker's controlled page which has an image of the website so the attacker can fully control the victim traffic.

Browser proxy configuration attack: attacker overrides the victim's web browser proxy configuration options using poisoning techniques so attacker can then redirect traffic to a fraudulent proxy server that is under control of the attacker and Steals all victims' identity. [4]

Rogue DHCP: attacker uses malicious code to install a rogue DHCP on the user's network and control the DHCP local options to redirect all traffic.

Home or Border router attack: by accessing the home router and compromise it to modify the DNS entries to success with fully controls the victim traffic. [5]

3. PHARMING ATTACK DETECTIONS
Dual Approach [3]: In this approach, a browser plug-in has been developed or software has been installed, so whenever user is requesting to the website, the software will check the IP address resolve by the local DNS server. And another

query will be send to a public DNS as a third-party 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. [6] When installing the software, the software could have its own third-party DNS server or the user will be asked to choose it (e.g. OpenDNS, Google DNS, etc.). Its recommend the user to choose a third-party DNS server different from his IS. [6]

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 responses can greatly vary according to the geographical location from which the DNS query was launched.

Webpage Signature matching [3]: In this approach, software with an available database that has a local signature from a number of websites will be installed, when a user checks for a website; a signature from the webpage will be extracted and compared with the available database. If it matches the signature, then it's not an issue. If not, the signature than page might be under Pharming attack. Consider that the database should always be maintained and modified [7, 8, and 9]

Issues:

- Web pages content is dynamic, by integrating ads, RSS feeds, etc.
- Phishing and legitimate sites use both absolute and relative paths for images, links, etc.
- Attackers create poisoned site similar to the legitimate one, and keeping links to the legitimate site lure as many users as possible.
- Depending on the web browser of the user, additional script can be added to the HTML content (Internet Explorer, Firefox, Opera …)
- HTML structure of the same webpage can be very different depending on the geographical 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.

Webpage content comparison [3, 10]: This approach is used to support Dual mode approach for Pharming detection. In this approach, and after the Dual approach detects a differ, the html code of both pages responded by local DNS as well as from public DNS will be compared On the base of threshold value it will prompt the user about the Pharming attack. [11]

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 when using public DNS of some different region.
- Content of the webpage differs according to geographical location (google.ps for Palestine, google.co.au for Australia).
- Comparing the content of webpages will require more processing power and reduce the browsing speed

Visual similarity based detection [10, 12]: In this approach, URL and Image of the website which is stored in predefined database will be compared. Fist it will take snapshot of the visited site, and compare it with image database, if it compares the image then it will check domain name, if it is correspond, then that will be legitimate page. If image do 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.

Issues:

- Comparing images would spend more time and consume more processing power.
- 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.[12]

Some research brought two ways or more together to detect pharming.

4. OUR PROPOSAL

The core idea of our proposal is to focus on solving the problem in the first detection methodology of dual approach [10] that the third-party DNS responses can greatly vary according to the location from which the DNS query was launched.

We suggest using the Authoritative Name server for a domain to detect all IP addresses for a website and check it – one after the other – with the IP address response from the local DNS server, if it matches any of it, the webpage will be considered legitimate. If not, the IP address located from the local DNS will be checked with a reverse lookup to chick its real Authoritative DNS and compare it with the trusted Authoritative Name Servers we gather before, so if it match, the webpage will be considered legitimate. If not, the page is suspicious and the process is considered as a pharming attack.

For this idea, we implemented a PHP code to collect the required information by using DIG command (domain information groper) to query name servers for a domain then fetch IP addresses for the website.

The code will trace all DNS information for a webpage through a ROOT DNS servers and Authoritative Name Servers of user's domain's TLD, reaching user domain's Authoritative Name Servers, then finally which will be used to query all the IP addresses for the wanted website listed at the domain's ZONE file. These addresses will be stored temporarily to check it with the local DNS query and decide whether the webpage is legitimated or suspicious.

With this process the third-party DNS server is the domain's Authoritative Name Servers which has all trusted information.

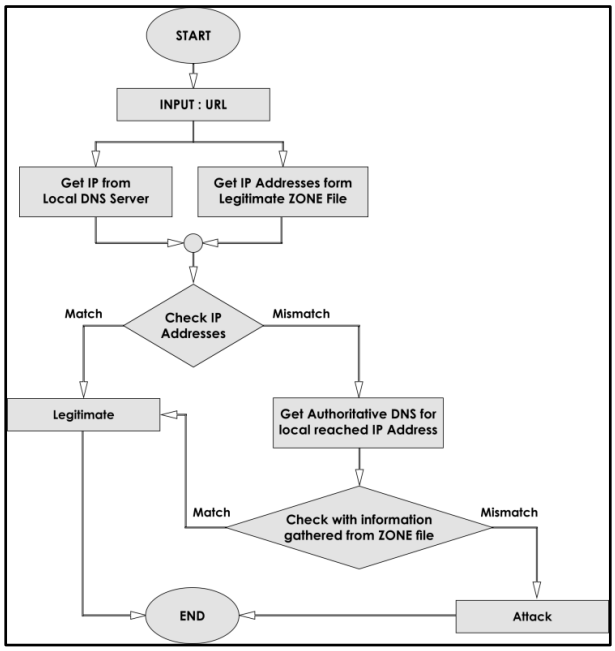

Fig 1: explains this approach via Flow chart

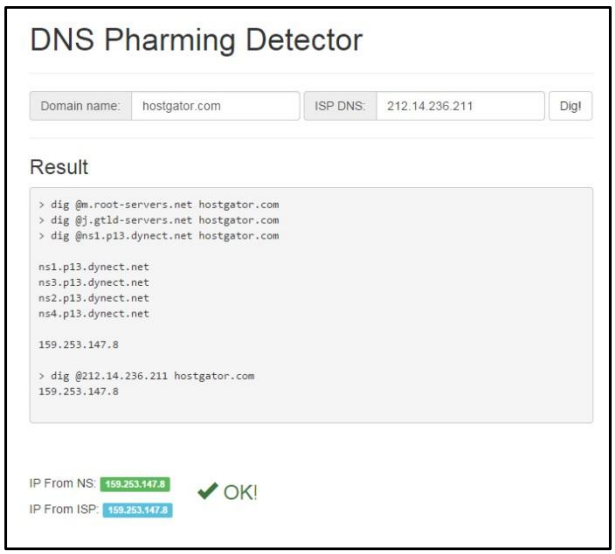

Fig 2: shows the approach interface

5. EXPERIMENT ENVIRONMENT

DIG is a command-line utility used for making DNS queries and displaying their results. It is a much better tool than nslookup. DIG runs on Linux and Windows equally well, and is probably available for most other operating systems too. In Linux, DIG is probably already installed. Installing DIG on Windows is simple; we just downloaded the source file of BIND name server which dig is part of it and give the full location of the file to the PHP code we wrote. For more information about DIG command, see dig command manual page [14].

We examine our approach by two ISPs as real environment using up to 300 famous and most popular websites in a number of areas such as online banks, search engines, mail bulk services, hosting and E-Commerce Companies with different languages and TLD's in the domain name [15].

Table 1: Shows the match result between the IP addresses resolved from the Authoritative Name server and the IP addresses resolved from ISP DNS.

	ANS | IPs	ISP | IPs	
amazon.com	176.32.98.166 205.251.242.54 72.21.215.232	176.32.98.166 205.251.242.54 72.21.215.232	match
yahoo.com	98.139.183.24 98.138.253.109 206.190.36.45	206.190.36.45 98.138.253.109 98.139.183.24	match
facebook.com	173.252.120.6	173.252.120.6	match
hotmail.com	65.55.85.12 157.56.172.28 157.55.152.112 65.55.77.28	157.55.152.112 157.56.172.28 65.55.77.28 65.55.85.12	match
arabbank.ps	37.75.144.176	37.75.144.176	match
bop.ps	213.244.121.5	213.244.121.5	match
wikipedia.org	91.198.174.192	91.198.174.192	match
w3.org	128.30.52.45	128.30.52.45	match
wordpress.org	66.155.40.249 66.155.40.250	66.155.40.249 66.155.40.250	match
icio.us	184.72.49.25	184.72.49.25	match
yandex.ru	93.158.134.11 213.180.204.11 213.180.193.11	93.158.134.11 213.180.193.11 213.180.204.11	match
free.fr	212.27.48.10	212.27.48.10	match
joomla.org	72.29.124.146	72.29.124.146	match
Nih.gov	137.187.25.43	137.187.25.43	match
51.la	117.21.226.199	117.21.226.199	match
Ameblo.jp	180.233.142.129	180.233.142.129	match
Slideshare.net	108.174.2.100	108.174.2.100	match

At the table above – Table 1 – for the first step, when asking for DNS information of the domain facebook.com through ROOT servers using Authoritative Name Servers of the top level domain .com then going to a second level for facebook.com Authoritative Servers we can gain all information we need including website IP address, for the second step using the ISP DNS to resolve facebook.com IP address, from the table we can see that both IP addresses are match and the issue will considered as legitimate website.

If resolving returns number of IP addresses just likes Yahoo.com, it should be all compared and discard the mismatch because it will considered as suspicious.

Table 2: Shows how our approach solves the problem of geographic location using a reverse look-up to check the match of Authoritative Name Servers for both groups of IP addresses.

Google.com			
ANS | IPs	**ISP | IPs**	**Reverse look-up**	
213.244.66.34	173.194.112.66	ns1.google.com	
213.244.66.19	173.194.112.67	ns2.google.com	
213.244.66.59	173.194.112.68	ns3.google.com	
213.244.66.44	173.194.112.69	ns4.google.com	
213.244.66.45	173.194.112.70		
213.244.66.49	173.194.112.71		
213.244.66.38	173.194.112.72		
213.244.66.42	173.194.112.73		match
213.244.66.15	173.194.112.78		
213.244.66.29	173.194.112.64		
213.244.66.27	173.194.112.65		
213.244.66.30			
213.244.66.53			
213.244.66.57			
213.244.66.23			
Twitter.com			
ANS | IPs	**ISP | IPs**	**Reverse look-up**	
199.59.148.10	199.16.156.230	ns1.p34.dynect.net	
199.59.150.39	199.59.149.230	ns2.p34.dynect.net	match
199.59.148.82	199.16.156.198	ns3.p34.dynect.net	
199.59.149.230	199.59.149.198	ns4.p34.dynect.net	
Blogspot.com			
ANS | IPs	**ISP | IPs**	**Reverse look-up**	
216.58.209.105	216.58.211.9	ns1.google.com ns2.google.com ns3.google.com ns4.google.com	match
Sogou.com			
ANS | IPs	**ISP | IPs**	**Reverse look-up**	
106.120.151.63	106.120.151.61	ns1.sogou.com	
180.149.156.69	106.120.151.62	ns2.sogou.com	
180.149.156.70	220.181.124.5		
180.149.156.71	220.181.124.6		
180.149.156.72			match
180.149.156.73			
220.181.124.2			
220.181.124.3			
220.181.124.4			

Google.com at Table2 above mismatch all IP addresses, so a third step will be checked as a reverse look-up for each IP addresses resolved from ISP to assure that it has the same Authoritative Name Servers that we used to resolve in the first step, the third check gives a match of Authoritative Name Servers and the issue will considered as legitimate website.

Table 3: Shows the match result using a second ISP DNS.

	ANS | IPs	**ISP | IPs**	
Google.com No Need of Reverse Look-up	213.244.66.34	213.244.66.53	match
	213.244.66.19	213.244.66.59	
	213.244.66.59	213.244.66.44	
	213.244.66.44	213.244.66.45	
	213.244.66.45	213.244.66.29	
	213.244.66.49	213.244.66.15	
	213.244.66.38	213.244.66.38	
	213.244.66.42	213.244.66.27	
	213.244.66.15	213.244.66.57	

	213.244.66.29 213.244.66.27 213.244.66.30 213.244.66.53 213.244.66.57 213.244.66.23	213.244.66.23 213.244.66.30 213.244.66.19 213.244.66.49 213.244.66.42 213.244.66.34	
yahoo.com	98.139.183.24 98.138.253.109 206.190.36.45	98.138.253.109 206.190.36.45 98.139.183.24	match
arabbank.ps	37.75.144.176	37.75.144.176	match
bop.ps	213.244.121.5	213.244.121.5	match
wikipedia.org	91.198.174.192	91.198.174.192	match
Ameblo.jp	180.233.142.129	180.233.142.129	match
Slideshare.net	108.174.2.100	108.174.2.100	match
Twitter.com No Need of Reverse Look-up	199.59.150.7 199.59.148.82 199.16.156.230 199.16.156.70 199.59.148.10 199.16.156.198 199.16.156.102 199.16.156.6 199.59.149.230 199.16.156.38 199.59.150.39 199.59.149.198	199.59.150.7 199.59.148.10 199.16.156.38 199.59.150.39 199.16.156.70 199.16.156.102 199.59.148.82 199.16.156.230 199.59.149.230 199.16.156.198 199.59.149.198 199.16.156.6	match
Blogspot.com	216.58.211.41	216.58.211.41	match
Sogou.com No Need of Reverse Look-up	106.120.151.63 180.149.156.69 180.149.156.70 180.149.156.71	106.120.151.61 106.120.151.62 106.120.151.63 180.149.156.69	match
	180.149.156.72 180.149.156.73 220.181.124.2 220.181.124.3 220.181.124.4 220.181.124.5 220.181.124.6 106.120.151.61 106.120.151.62	180.149.156.70 180.149.156.71 180.149.156.72 180.149.156.73 220.181.124.2 220.181.124.3 220.181.124.4 220.181.124.5 220.181.124.6	

Table 4: Shows the reverse look-up match for Twitter.com with geographic location issues using the second ISP DNS.

Twitter.com			
ANS | IPs	**ISP | IPs**	**Reverse look-up**	
199.59.148.10 199.59.150.39 199.59.148.82 199.59.149.230	199.59.150.7 199.59.148.10 199.16.156.38 199.59.150.39 199.16.156.70 199.16.156.102 199.59.148.82 199.16.156.230 199.59.149.230 199.16.156.198 199.59.149.198 199.16.156.6	ns1.p34.dynect.net ns2.p34.dynect.net ns3.p34.dynect.net ns4.p34.dynect.net	match

As we can see, with this ISP twitter.com acts with two forms of the solution. The first form - Table3 – ISP resolve the same IP addresses of the Authoritative Name server and need not to move to the second stage while the second one – Table4 – we forced to make a reverse look-up to check the mismatch IP addresses and make sure that its resolved from the trusted Authoritative Name Servers.

Sometimes the Authoritative Name Server for a domain could be unreachable because its down or the DNS service is not running.

Another type of failure is caused by the use of a broken DNS server at ISP side that causes DNS outages [16].

6. ISP DNS ISSUES

ISPs are bad at DNS; they provide pipe services and Internet connectivity. They have set up their business to ensure they can carry packets across their network. That's what they lead with when they are out making a sale. [16, 17]

Managed services like DNS are different from network engineering. While network services require their own expertise with routers and switching, this expertise rarely translates to expertise in services like DNS. DNS as a service is not only focused on the network availability but also server operating systems, software updates, load-balancing, customer interfaces, and physical server limitations. [16]

Network operators work within an entire environment where they control everything on their network. Often times these operators are not familiar with the unique problems associated with DNS and other services.

Online applications like DNS are world-facing by design and both security and denial of service attacks are more pressing concerns. Constant management is critical to their success, and those operating it need to be well versed in the appropriate techniques. Network operators, for example, are not necessarily familiar with critical software patches that must be implemented in a timely manner to ensure attackers can be fended off. [16]

7. CONCLUSION

Pharming is a very serious attack, the challenge of keeping sensitive information like bank accounts and passwords of the users safe from the hand of attackers become more important day after day. ISPs are responsible of implementing security in order to prevent pharming attacks. At client-side, users need to understand basic of attacks and some basic steps to protect his or her identity or credentials.

Our idea provides a high accuracy in protecting. Detecting pharming attacks on the client-side may suffer from time-consuming; it needs too long time to calculate a pair of pages. But sometimes, security is more important than speed, especially in case of E-transaction.

Authoritative queries may vary from ISP to other, for future work we are going to search for this issue and develop our approach to implement a model that could be installed on user device as a software or in the browser itself as a plugin so we can make better analysis tests using several geographical location for more improving our idea.

Authoritative queries must be secured, more for future we have to focus on detection and prevention at server-side

8. REFERENCES

[1] Name server, Wikipedia the free encyclopedia, Dec. 2014, [online]; available: http://en.wikipedia.org/wiki/Name_server

[2] G. Ollman,"The Pharming Guide," Oct. 2014, [online]; available: http://www.technicalinfo.net/papers/Pharming.html

[3] Jayshree Patel, Prof. S.D. Panchal, A survey on Pharming attack Detection and prevention methodology, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN:2278-8727Volume 9, Issue 1 (Jan.-Feb. 2013), PP66-72

[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] S. Stamm, Z. Ramzan, et Jakobsson Markus,"Drive-By Pharming", Proceedings of the 9th international conference onInformation and communications security, Zhengzhou, China: ACM, 2007, p. 495-506.

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

[7] 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

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

[9] 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

[10] M. Hara, A. Yamada, et Y. Miyake, Visual similarity-based phishing detection without victim site information,"Nashville, Tennessee, USA: IEEE, 2009, p. 30-36.

[11] Gastellier-Prevost, S.; Laurent, M., Defeating pharming attacks at client side, IEEE, 2011, p. 33-40.

[12] G. Pavithra, D. S. John Deva Prasanna, Countering Phishing Threats using Visual Cryptography, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 3, March 2013

[13] Areej N. El-Buhaisi, Detection Model for Pharming attack based on Ip-Address Check and Website Predictability, Thesis for the degree of master of science in information technology, the Islamic university of Gaza, 2013.

[14] Dig(1) - Linux Manual page, Dec. 2014,[online]; available: http://linux.die.net/man/1/dig

[15] Moz top 500,Dec. 2014, [online]; available: http://moz.com/top500

[16] DYN, The Case Against Free ISP DNS, Feb 2015,[online]; available: http://dyn.com/wp-content/uploads/2013/06/CaseAgainstFreeISPDNS.pdf

[17] Excedo DNS, DYNECT, The Case Against Free ISP DNS, Jan 2015,[online]; available: http://www.excedodns.eu/images/excedodns/files/Case_Against_Free_ISP_DNS-EN-V1.pdf