Pharming

“When the phish aren't biting, it's time to go into pharming”

03/01/2014

Osvaldo Concepcion

Dairon Perez

Gersain Mesa

Roberto Dominguez

Mawi Perez

Table of Contents

Introduction

Pharming is defined as an attack in which a hacker installs malicious code on a personal computer or server, and redirects users from legitimate websites to fraudulent ones without their consent. It can also be called as "Phishing without a Lure." Furthermore, it is among the most common computer security threats and even though it is a variant of phishing, it uses different techniques to achieve this.

The first use of the word Phishing was in 1987 in a paper and presentation brought to the International HP users group. However, it didn't really come out to the public until the American Online (AOL) accounts were stolen in 1996 by email. Since then, attempts have been made to target customers of banks and online payment services, making Social Networking sites the primary use for these attacks. On the other hand, Pharming was the evolution of phishing when it started to have low effects on users because the scams were easily identified and avoided. Panix was the first investigated case of this attack and in 2005 someone changed the DNS address, email direction, and ownership information of panix.com

Pharming techniques are mainly based on deceiving not only the user but the computer as well, in order to change the real URLs to different IP numbers and consequently take the users to unwanted destinations. Moreover, pharming seeks to obtain personal or private information through domain spoofing. In other words, it poisons a DNS server by infusing false information into the DNS server, resulting in the redirection of the users request. However, your browser will still indicate that you are in a legitimate website making pharming more difficult to detect.

This project has a focus on finding protocols used for this threat, explain how they work and make a demonstration showing the procedure and tools used to preform these attack; thus finding efficient ways to counteract and/or prevent them.

HISTORY

An earlier form of pharming, called phishing, has been around since 1996. By 2003, phishing attacks became really popular for cybercriminals. The problem with phishing attacks was that it was email-based and the victim would have to be convinced to click a link to a fake website to enter their information. With its popularity, phishing attacks became more preventable, so cybercriminals came up with a new form of phishing, called pharming. Unlike phishing, pharming is invisible to the victim. So as users became aware of how to prevent phishing attacks, pharming made that irrelevant.

The first known pharming attack occurred in September 2004 by a teenager who gained control of the ebay.de domain in Germany. A few months later on January 2005, the site for a New York ISP (Panix.com) was hijacked through a pharming attack. Another notable attack came in February of 2007, which infected customers of over 50 different financial institutions worldwide. To be able to pull this off, the group of crackers created a look-alike website for each of the financial institutions to be able to extract information from the infected user. In the same month, researchers at Symantec and the University of Indiana warned the public of a new form of "drive-by" pharming attacks, which would infect home routers with DNS poisoning.

The number of reported pharming cases has increased dramatically in the past few years. Moreover, there were 398 reports in 2010, 511 in 2011, and within just the first half of last year, there were over 1,000 reports of pharming. Accordingly, a large number of recent reports of fraud and identity theft have been caused by pharming attacks over the years.

PHARMING vs. PHISHING

Pharming is the act of redirecting a website's traffic to another. It can be done either by changing the hosts file of a victim's computer or by manipulating the vulnerabilities in DNS server software. The function of the DNS is to translate the name of the sites into the real addresses, because what really directs you to a page is its IP, but most people remember words better than numbers.

On the other hand, Phishing is the action of accessing confidential information by deceiving the user using ads, email, letters, and others. It is a form of social engineering attacks that manipulates a human flaw using technology as a mean of communication. When phishing is performed via email, the criminal sends out a large number of messages to make them look like they come from a legitimate source such as a financial institution and business. Furthermore, the email attempts to lure the reader into clicking a link that appears to go to a licit website, but the actual link redirects to a fraudulent, look a like web address, that is intended to trick the user into supplying confidential information.

These two terms might often be confused due to the fact that they are related to ambiguous online practices, either to sale goods or services online or to gain access to private information. As mentioned before, phishing attacks use some sort of social engineering to compromise personal information, where the cracker creates authentic looking websites and emails. Nonetheless, pharming attacks use a type of social engineering technique known as DNS poisoning. In a pharming attack, your ISP may be compromised making your connection to the internet susceptible.

How it Works

Pharming is the redirection of a Web site's actual or intended traffic to a malicious site. Redirection is often accomplished in one of two ways: modification of host files or by taking advantage of weaknesses in DNS services.

Modification of host files

The Hosts file is an old method of resolving domain names to IP addresses when DNS services are either not available or when slight adjustments to resolved addresses are required. The Hosts file, residing by default on every Microsoft Windows system, contains domain/IP address information, which overrides DNS name resolution. So all an attacker has to do is drop a small script on a desktop, modify the Hosts file, and abracadabra, the user is thenceforth directed to one or more sites of the attacker's choice. Let's step through an example on a Windows XP SP2 system.

The hosts file is located in the same place on all current versions of Windows, shown in Figure 1. Hosts is a text file WITHOUT an extension. Adding an extension causes Windows to ignore the file on bootup.

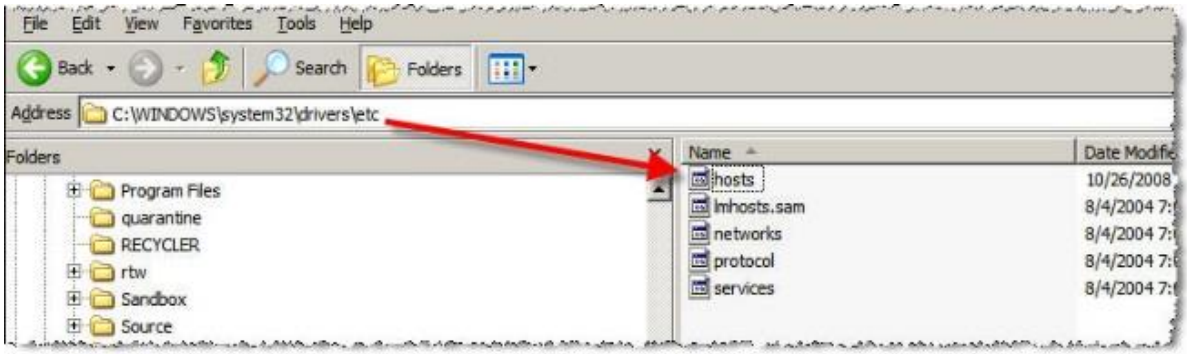

Figure 1

Hosts ships with content designed to assist administrators, as shown in Figure 2. Note the entries are similar to host address resource records in DNS.

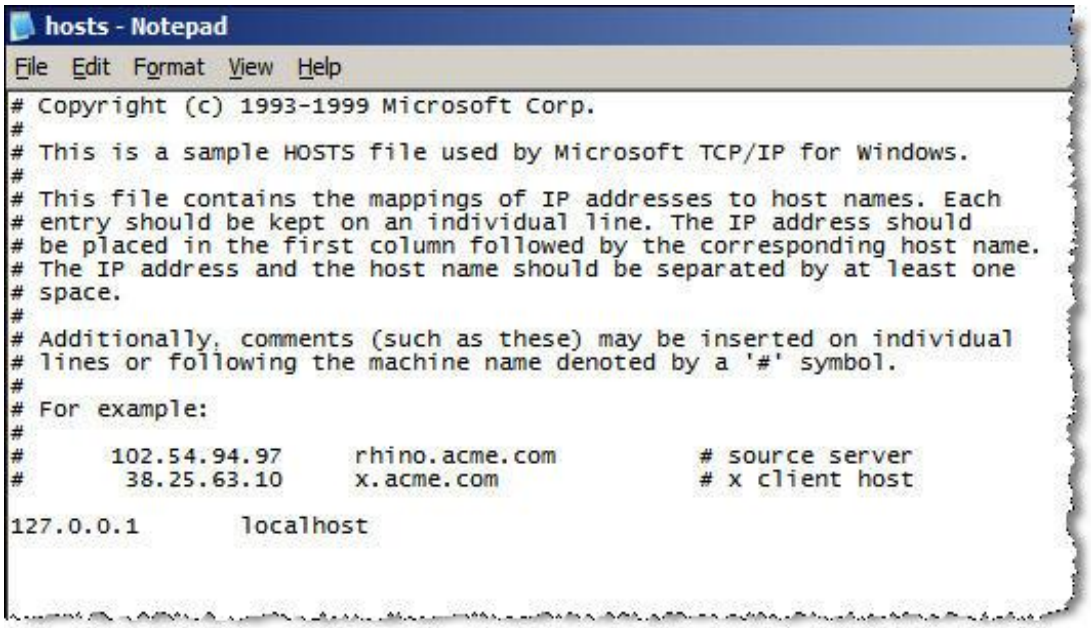

Figure 2

To demonstrate how this works, we chose to redirect google.com to fiu.edu. We started by pinging fiu.edu and entering the IP address returned into the hosts file along with the www.fiu.edu, as shown in Figure 3.

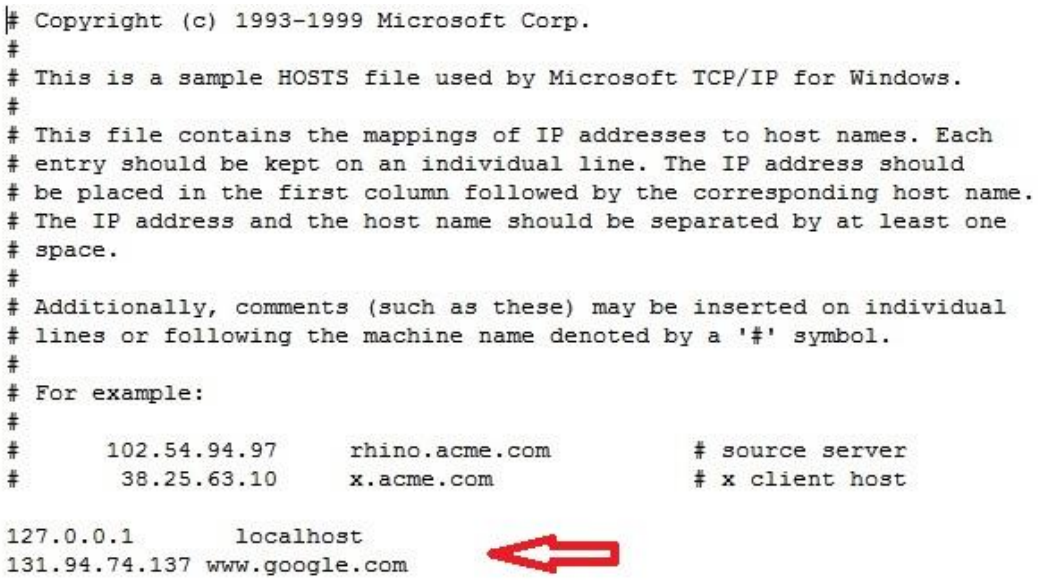

Figure 3

After we saved the file (with no extension), we flushed the resolver cache by entering ipconfig /flushdns at a command prompt. This performed two tasks. First, it removed all cached name resolution records from the test machine. Second, it loaded the contents of the hosts file into the resolver cache. Since the resolver cache is checked before a Windows system sends a DNS query, www.google.com will always resolve to the FIU IP address.

To test, we closed and reloaded Microsoft IE7 and entered www.google.com in the address space. As it can be seen in Figure 4, we were directed to fiu.edu instead of google.com. If an attacker placed this entry, he or she would likely redirect me to a page, which looked exactly like the actual site. Applications at the substitute site could then perform various tasks, including enlisting the redirected system into a botnet.

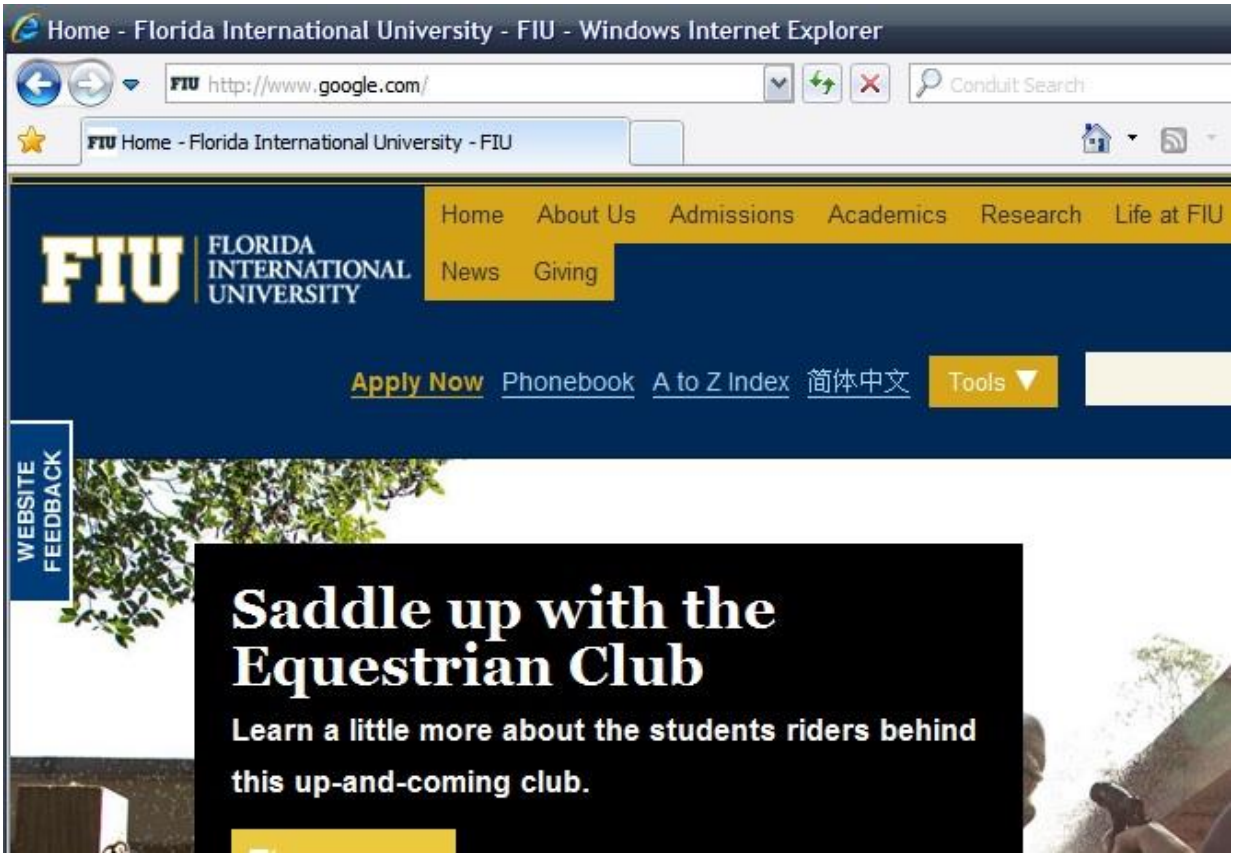

Figure 4

Default access to the Hosts file is read/execute for all users except local admin. As long as your users are not logging in and browsing the Web as local administrators, this type of attack will be troublesome for black hat hackers. But there is another way.

Black hats do not have to gain access to the local Hosts file to redirect users to malicious sites. Recent discoveries about DNS vulnerabilities make resolver cache poisoning at the server level a real possibility, especially if DNS service providers have not patched or properly configured their servers. Poisoned cache entries can potentially redirect all systems requesting name resolution to malicious servers.

DNS poisoning.

DNS cache poisoning consists of changing or adding records in the resolver caches, either on the client or the server, so that a DNS query for a domain returns an IP address for an attacker's domain instead of the intended domain. To demonstrate how this might work, let's step through Figure 5.

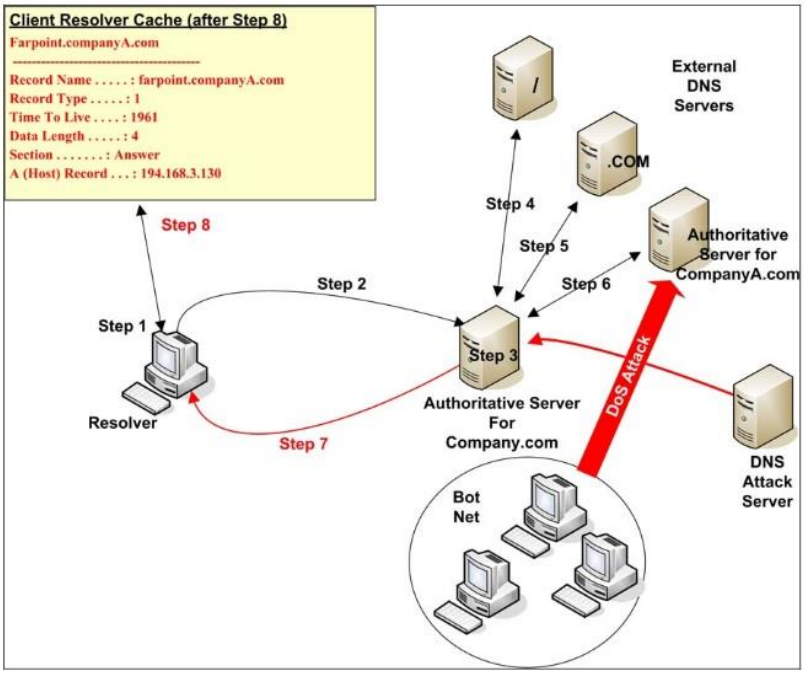

Figure 5

Step 1: The resolver checks the resolver cache in the workstation's memory to see if it contains an entry for Farpoint.companyA.com.

Step 2: Having found no entry in the resolver cache, the resolver sends a resolution request to the internal DNS server.

Step 3: When the DNS server receives the request, it first checks to see if it's authoritative. In this case, it isn't authoritative for companyA.com. The next action it takes is to check its local cache to see if an entry for Farpoint.companyA.com exists. It doesn't. So in Step 4 the internal DNS server begins the process of iteratively querying external DNS servers until it either resolves the domain name or it reaches a point at which it's clear that the domain name entry doesn't exist.

Step 4: A request is sent to one of the Internet root servers. The root server returns the address of a server authoritative for the .COM Internet space.

Step 5: A request is sent to the authoritative server for .COM. The address of a DNS server authoritative for the companyA.com domain is returned.

Step 6: A request is sent to the authoritative server for companyA.com. This is identical to the standard process for an iterative query – with one exception. A cracker has decided to poison the internal DNS server's cache. In order to intercept a query and return malicious information, the cracker must know the transaction ID. Once the transaction ID is known, the attacker's DNS server can respond as the authoritative server for companyA.com. Although this would be a simple matter with older DNS software (e.g. BIND 4 and earlier), newer DNS systems have build-in safeguards. In our example, the transaction ID used to identify each query instance is randomized.

But figuring out the transaction ID is not impossible. All that's required is time.

To slow the response of the real authoritative server, our cracker uses a botnet to initiate a Denial of Service (DoS) attack. While the authoritative server struggles to deal with the attack, the attacker's DNS server has time to determine the transaction ID.

Once the ID is determined, a query response is sent to the internal DNS server. But the IP address for Farpoint.companyA.com in the response is actually the IP address of the attacker's site. The response is placed into the server's cache.

Step 7: The rogue IP address for Farpoint is returned to the client resolver.

Step 8: An entry is made in the resolver cache, and a session is initiated with the attacker's site. At this point, both the workstation's cache and the internal DNS server's cache are poisoned. Any workstation on the internal network requesting resolution of Farpoint.companyA.com will receive the rogue address listed in the internal DNS server's cache. This continues until the entry is deleted. Another method used to poison a DNS cache is the use of a recursive query sent by the attacker. The query can force the target server to connect to the authoritative source of the domain in the query. Once connected, rogue information about one or more domains might be sent to the querying server and posted to the server's cache.

Anti-Pharming

It is referred to the techniques used to prevent or counter-attack pharming. Some of the things used include the use of specialized software, protection of the DNS and the utilization of add-ons in the web explorers like for example toolbars.

The specialized software is often used in large company servers to protect its users and employs from potential pharming and phishing attacks, while the use of add-ons in the web explorers allow the domestic users protect themselves from this technique.

A DNS protection safeguard DNS servers from being compromised by pharming attacks, on the other hand the anti-spam filters not often protects the user from this attack.

Even though we have several tools to prevent pharming, precaution and responsible use of the internet are always the best way to avoid being a victim of pharming, making sure that we are in a safe page with the right credentials, also if you are in a page that requires personal information look if http changes to https. Https means your information will be encrypted, if it doesn't changes do not enter any information since it is possible that anybody can access your information. Another thing you need to pay attention to is the web address because sometimes the crackers use very similar names for their fake web pages, for instance if the page you intend to visit is www.chase.com, they could use www.chasse.com something that you can overlook if you are in a rush, so always try to be alert and make sure you are where you're supposed to be.

Conclusion

In conclusion, Pharming is a cyber attack projected to redirect a website's traffic to another bogus website and we can say that we have deeply explored the phenomenon of it in networking. Consequently, we have expanded our knowledge not only by understanding how it works, but also by investigating through its history and definition, the relationship between Phishing and Pharming.

Additionally, we have made a descriptive analysis about the two different types of pharming that exist: modification of the host file in the user's computer, and via DNS poisoning. We have backed up our analysis with a practical example of how to modify the host files, in order to reach FIU's website intending to access google.com. Although this example has only educational purposes, we also investigated how malicious hackers can take advantage of these attacks. Finally, we scrutinized the different ways to protect computers from Pharming cyber attacks and our objective is to increase awareness about security in networking environments.

References

Aslam, B.; Lei Wu; Zou, C.C., "PwdIP-Hash: A Lightweight Solution to Phishing and Pharming Attacks," Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on , vol., no., pp.198,203, 15-17 July 2010

Gastellier-Prevost, S.; Granadillo, G.G.; Laurent, M., "A Dual Approach to Detect Pharming Attacks at the Client-Side," New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on , vol., no., pp.1,5, 7-10 Feb. 2011

Gastellier-Prevost, S.; Laurent, M., "Defeating pharming attacks at the client-side," Network and System Security (NSS), 2011 5th International Conference on , vol., no., pp.33,40, 6-8 Sept. 2011

Schipke, Rae Carrington, "The Language of Phishing, Pharming, and Other Internet Fraud-Metaphorically Speaking," Technology and Society, 2006. ISTAS 2006. IEEE International Symposium on , vol., no., pp.1,6, 8-10 June 2006

Sun Bin; Wen Qiaoyan; Liang Xiaoying, "A DNS Based Anti-phishing Approach," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.2, no., pp.262,265, 24-25 April 2010

Sun Bin; Wen Qiaoyan; Liang Xiaoying, "A DNS Based Anti-phishing Approach," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.2, no., pp.262,265, 24-25 April 2010

San Martino, A.; Perramon, X., "A Model for Securing E-Banking Authentication Process: Antiphishing Approach," Services - Part I, 2008. IEEE Congress on , vol., no., pp.251,254, 6-11 July 2008

Symantec Corporation. “The 11 most common computer security threats… And what you can do to protect yourself from them.” *Symantec-Norton*. n.p., n.d. Web. 15 Feb. 2014. <http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx>.

Bullguard. “What is pharming?” *Bullguard*. n.p., n.d. Web. 15 Feb. 2014. <http://www.bullguard.com/bullguard-security-center/internet-security/internet-threats/what-is-pharming.aspx>.

Norton. “Online Fraud: Pharming.” *Norton*. n.p., n.d. Web. 15 Feb. 2014. <http://us.norton.com/cybercrime-pharming>.

Catbird vSecurity. “Pharming Shield.” *Pharming Shield*. n.p., n.d. Web. 15 Feb. 2014. <http://www.pharmingshield.com/pharmingshield/pharming-shield.php>.

Christensen, Brett. “Pharming – Information about Pharming Scams.” *Hoax-Slayer*. n.p., n.d. Web. 15 Feb. 2014. <http://www.hoax-slayer.com/pharming.html>.

Ollmann, Gunter. “The Pharming Guide (part 1).” *Technical Info*. n.p., n.d. Web. 15 Feb. 2014. <http://www.technicalinfo.net/papers/Pharming.html>.