Table of Contents

Introduction-Understanding Phishing and Pharming 3

What Are Phishing and Pharming?  4

Figure #1 – Unique Phishing Attack Trend 2003-2004 4

Early Attempts 4

Systematic Attacks 5

Figure #2 - Active Phishing Sites 2004-2005 5

Getting Smarter, 5

Financial Impact, Pharming – A New Threat is Born 6

Phishing & Pharming Mitigations with McAfee 7

Anti-Spam Filtering – Phishing Protection 7

McAfee Anti-Virus summary, What about desktop protection? 7

Host & Network Intrusion Protection 7

The phishing – Evolution, conclusion 8
Introduction

Understanding Phishing and Pharming

To properly protect your critical business assets from today’s “Phishing” attacks you must first understand the history of Phishing, the types of Phishing techniques that are used in today’s security underworld, and ways that McAfee can help you trap and defend against these attacks. Also, what is the newest trend in security attacks known as “Pharming”, the current evolution of “Phishing,” how it is different, what can be done to defend against and, what are the best remediation techniques for both of these types of attacks.

With insight into the threats of Phishing, and Pharming (See definitions) this paper is intended to help identify what a Phishing attack is, what it looks like in a network, and how it can be mitigated. Also, what Pharming attacks may look like based in different attack scenarios and how to alleviate it’s affect on your business assets. We will also outline how historically, these two types of attacks have developed into today’s sophisticated deadly-duo aimed business, consumer, and government entities.
What Are Phishing and Pharming?

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, Phishers often convince recipients to respond. Technical subterfuge schemes plant crime ware onto PCs to steal credentials directly, often using Trojan key logger Spyware. Pharming crime ware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

Early Attempts

The early phish for credit card details etc, were less sophisticated. The email would contain a link to a website that looked like a legitimate website (but in fact of course wasn’t). Very often the web site address was not a domain, but simply an IP Address such as 162.122.19.2 and the emails were often very poorly written, with bad grammar and spelling and with a little attention to detail would be made for what they were, and cheap scam.

As with anything new Phishing attacks evolved quickly become harder to recognize, with more sophistication, better written and better spelling, more convincing emails. Phishers quickly became more proficient often using HTML containing images and graphics from the legitimate banks or financial organization with the links represented in these email
as if they were the targeted institutions sites making them seem as being sent from the real corporation.

This is very simple to do because in HTML that link that appears can be given any name or description and the true destination hidden.

**Systematic Attacks**

Then toward the end of 2003, Phishing took a more sinister look and feel: when people started getting ‘phished’ for Bank credentials and credit card details that were subsequently used to obtain money or merchandise.

Over the past year, the number of phishing attacks has increased at an alarming rate, as shown in Fig 2.

The bait for these phishing attacks is usually through email. An email message is ‘spammed’ out to a large number of people and contains a link to a website. The email is usually asking for the user to update their information normally under the guise of ‘improving security systems’ or because of a potential breach of information has occurred. A wide variety of social engineering techniques are used.

When the user clicks on the link, they are sent to a web page that very closely resembles that of the legitimate institution, but is actually a fake. When the user enters their personal details they are stored allowing the hacker to recover later at their leisure.

![Active Reported Phishing Sites by Week November 2004 - February 2005](image)

**Fig 2 – Number of active reported phishing sites Nov 2004 – Feb 2005 (data from Anti-Phishing Working Group)**

**Getting Smarter**

To the trained eye it was still relatively straightforward to identify the phishing websites. Consumers were told to ensure that the site they were visiting contained the correct URL and included the yellow padlock to ensure the site was secure.

The Phishers were again, one step ahead. An exploit in Microsoft’s Internet Explorer technology allowed scripts to cover the URL bar so they were able to hide the URL of the site with the real banks address. The same technique allowed them to display a false padlock in the status bar.

Consumer awareness continues to grow so once again the Phishers have responded. Instead of sending emails persuading consumers to visit websites, “key logging” Trojans have started being deployed. As soon as the user visits their bank website, all the typed keys are logged and sent back providing the hacker with the account number, passwords and other critical data.
Banks and financial institutions tried to counter the threat by only asking for partial passwords, but over time persistent Phishers can still obtain the full password.

The battle continues, with banks now introducing drop down lists to select passwords, and virtual keyboards, and the Phishers responding with ‘mouse loggers’ and screen grabbers to obtain the information. More and more sophisticated techniques are being deployed by both Phishers and companies because there is so much at stake.

The Financial Impact

The estimates for how much money is lost through phishing attacks vary widely. The Australian bankers association reported A$10 million loss due to online fraud last year. It has been estimated that phishing cost US banks and credit card issuers $1.2 Billion in damages in 2003 (InternetNews.com) and the Association of Payment Clearing Services in the UK reported that direct fraud losses from online phishing scams cost £12M in 2004.

Regardless of the actual figure, the Phishers make significant money and are believed to be run by organized crime groups and even terrorists. Complex networks of bank accounts and money mules (people recruited to process the money for a small cut, often unwittingly) make it increasingly difficult for law enforcement to track them down.

More recently, Phishing attacks were responsible for the compromise of tens of thousands of consumer banking and credit cards records from firms that are paid to provide this information to legitimate entities. Phishing attacks by organized criminals has increased from 6597 in October 2004 to 14411 in April 2005 roughly a 45% rise over the past 7 months.

Pharming a new Threat is Born

A new twist in the online identity fraud battle is a technique known as ‘Pharming’. There are two techniques used, the first involves the use of a virus or Trojan to modify the user’s ‘Hosts’ file. This file is left over from the early days of the internet, and is used to relate a web address (URL) to a specific machine address (IP address) and is a simple text file. The Pharming technique, modifies this file to include the web address of well known banks and financial institutions with the IP address of the phishing site. So when the user opens the browser and enters the address of their bank, they get sent to the phishing site instead. No clicking on links in emails etc.

This second technique is equally sinister and again relies on an obsolete piece of functionality, this time implemented in DNS. DNS replaced the local hosts file as the mechanism for resolving a web address to a specific IP address. When the user enters an address it is looked up in the DNS server, if that DNS server doesn’t know the IP address it asks other DNS servers for the address and then gets the result. The problem is that part of the protocol allows extra information to be passed back as well. So the Phisher, sends an email that contains a link to a website, when the DNS lookup for that address is done, this extra information is included with the URL of the bank, but directed at a phishing site. This is best described as an example:

1. The Phisher sends out a spam for ‘www.phishsite.com’
2. A DNS query is made for ‘www.phishsite.com’
3. The ‘www.phishsite.com’ DNS server also returns data for ‘www.thebank.com’ which gets stored in DNS.
4. When anyone using the same ISP tries to visit ‘www.thebank.com’ they get redirected to the phish site.

This type of attack can be easily prevented by configuring the DNS server not to accept these extra records, but vulnerabilities are high because this is a fairly new and unique attack and the majority of IT managers are not aware of it.
Phishing & Pharming Mitigations with McAfee

Anti-Spam Filtering – Phishing protection

The McAfee SpamKiller product family includes specific rules and filters for detecting phishing attacks. Using a variety of heuristic techniques to identify the common characteristics of phishing emails they can be detected and blocked even if that specific attack has not been initiated before (“day-zero”). Independent tests against data submitted to the Anti-Phishing Working Group (APWG) and data gathered by McAfee spam traps show consistent detection rates of >97% for known and unknown phishing emails.

McAfee SpamKiller can be installed in a variety of ways depending on your specific requirements and applications. As an appliance-based solution, a solution to be installed directly onto your email servers either Microsoft Exchange and Lotus Domino, a solution to be installed onto your firewall (Microsoft ISA Server), and finally as a managed service hosted by McAfee for those customers who desire an outsource services solution.

McAfee Anti Virus Scanning Technology

The McAfee Anti-Virus scanning engine also offers detection for the most common targets of phishing for all McAfee email products by detection specific characteristics and classifying them as Phish-bankfraud.eml.

In addition many phishing websites use known exploits in Internet Explorer (as described above) to try and obscure the true location, and often use Trojans, Backdoor’s and Keyloggers. McAfee has extensive blocks already in place for these types of attacks.

What about Desktop Protection?

McAfee VirusScan Enterprise 8.0i with its integrated intrusion protection and firewall technology provides an effective mechanism for protecting against the constantly changing Phish threat. With the addition of a simple rule, attempts to hijack the users local host file can be prevented. The firewall technology prevents any Trojans or backdoors from sending harvested data to the Phisher as well as preventing the machine being recruited into a ‘bot-net’ to send out phishing spam. All of this is in addition to the world class detection provided by the AV scanning engine and McAfee’s AVERT research organization.

Host and Network Intrusion Protection

Phishers often target poorly protected machines as either a host for their Phishing site, by the compromise of legitimate web server or by using insecure machines to initiate “Phish spam” at a later date harvesting the collected data for exploitation.

McAfee’s Entercept, Desktop Firewall and IntruShield solutions help protect enterprise resources from unwittingly being used for criminal purposes aimed outside but also protecting their own users and customers from Phishing attacks.

The Phishing - Evolution

‘Phishing’ is the practice of trying to obtain confidential information such as credit card, bank details, account details or the like, from unsuspecting users and was originally started as a means of obtaining AOL login credentials. The hacker would simply send an email pretending to be from AOL asking for login name and password of a user, usually under the pretence of some security breach. Unsuspecting users would respond with the requested data, thereby giving the Phisher the necessary personal information they need to obtain access to your sensitive account information.
Conclusions

Phishing and Pharming along with their associated identity thefts have continued to grow at an alarming rate and are wreaking major havoc on the world's economy, as well as individual financial standings. Because these scams are difficult to detect, and the money that is being made by criminal organizations through these activities is huge; the complexity and frequency of attacks will continue to grow as large sums of money are to be made.

McAfee's proven protection for systems helps them from being hijacked by Phishers stops the sending of spam, to blocking spam, detecting Trojans and Keyloggers, protecting against Pharming techniques and blocking the phishing websites, McAfee's range of proven, proactive security products provide multiple levels of protection against this growing threat.