White Paper | January 2006

McAfee®
Proven Security™

Phishing and Pharming

Understanding phishing and pharming

Table of Contents

Understanding Phishing and Pharming

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, you should know about the newest trend in security attacks, an evolution of phishing known as *pharming*, how it is different, what can be done to defend against it, and the best remediation techniques for both of these types of attacks. With insight into the threats of phishing and pharming, 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, as well as what pharming attacks may look like based on different attack scenarios and how to alleviate their effect on your business assets. We will also outline how, historically, these two types of attacks have developed into today's sophisticated, deadly duo aimed at 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 Web sites that are 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 crimeware onto PCs in order to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

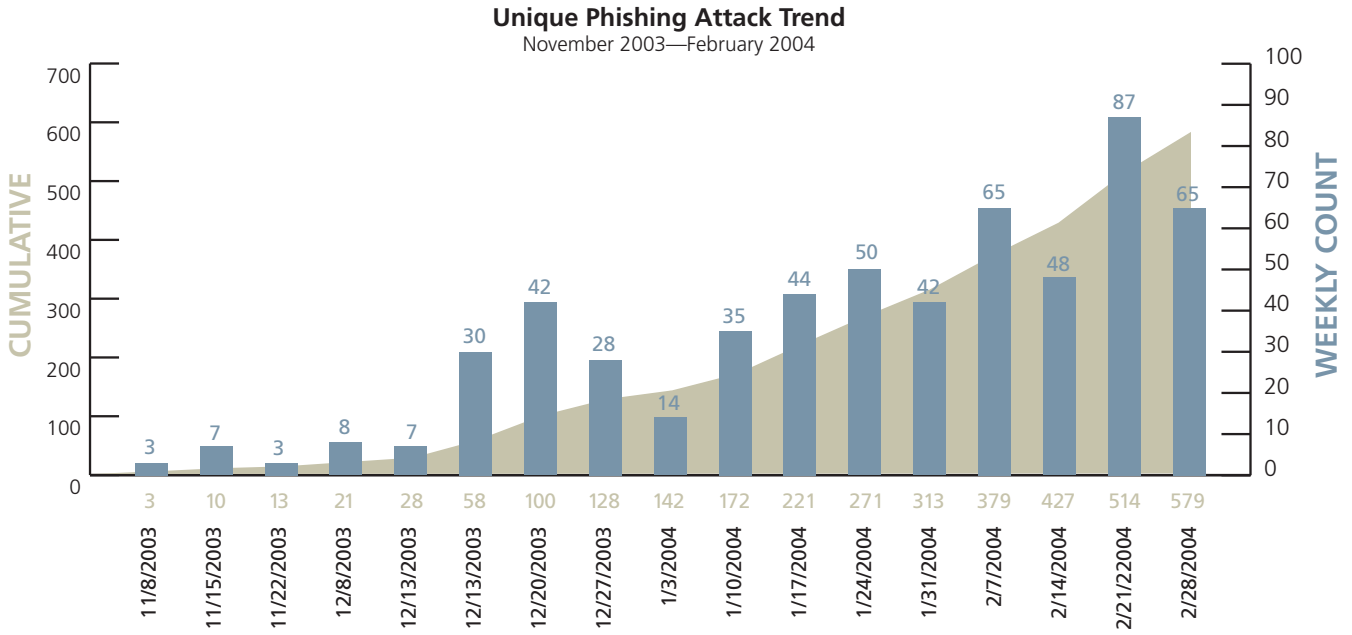

Figure 1: Unique phishing attack trend 2003–2004

Early attempts

The early phish for credit card details was less sophisticated. The e-mail contained a link to a Web site that looked like a legitimate Web site, but in fact was not. Very often the Web site address was not a domain, but simply an IP address such as 162.122.19.2, and the e-mails were often very poorly written, with bad grammar and spelling, and little attention to detail. As with anything new, phishing attacks evolved quickly and became harder to recognize, with more sophistication, better writing and spelling, and more convincing content. Phishers quickly became more proficient, often using HTML that contained images and graphics from legitimate banks or financial organizations. The links represented in these e-mails made them appear as if they'd been sent from the real corporation. This is very simple to do with HTML because the link can be given any name or description while the true destination remains hidden.

Systematic attacks

Toward late 2003, phishing took on a more sinister look and feel when individuals were *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 *Figure 2*.

The bait for these phishing attacks is usually through e-mail. An e-mail message with a link to a Web site is *spammed* out to a large number of people. The e-mail asks the reader to update personal and confidential information under the guise of "improving security systems" or because a potential breach of information has occurred.

Clicking on the link directs the reader to a Web page that very closely resembles that of a legitimate institution, but is actually a fake. Once entered on this page, personal information is stored, allowing a hacker to recover the information later.

Getting smarter

To the trained eye, it was still relatively straightforward to identify phishing Web sites. Consumers were told to ensure that the sites they visited contained the correct URL and generated the yellow padlock symbol in their browser's status bar to ensure the security of the site.

However, phishers were again one step ahead. An exploit in the Microsoft® Internet Explorer technology allowed scripts to cover the URL bar and hide the legitimate URL of real banks. The same technique allowed them to display a false padlock in the status bar.

Consumer awareness continues to grow and the phishers have responded. Instead of sending e-mails that persuade consumers to visit Web sites, *keylogging* Trojans are deployed. As soon as the user visits his or her bank's Web site, all the keys typed are logged and sent back to provide the hacker with the user's account number and passwords. The battle continues, with banks now using drop-down lists to select passwords as well as virtual keyboards, while the Phishers respond with *mouse loggers* and *screen grabbers* to obtain information. More and more sophisticated techniques are deployed by both phishers and companies because there is so much at stake.

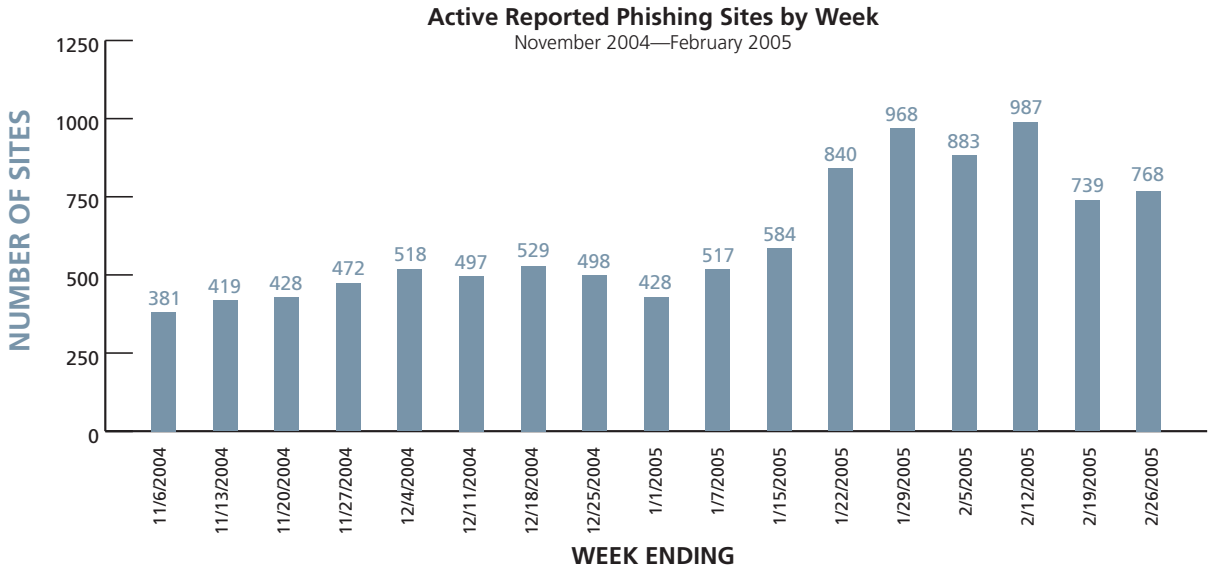

Figure 2: Number of active reported phishing sites November 2004–February 2005 (data from Anti-Phishing Working Group)

The financial impact

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

Regardless of the actual figure, 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 down these criminals.

More recently, phishing attacks were responsible for the compromise of tens of thousands of consumer banking and credit card records from firms that are paid to provide this information to legitimate entities. Phishing attacks by organized criminals have increased from 6,597 in October 2004 to 14,411 in April 2005, roughly a 45 percent rise over the past seven 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 simple text 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). The pharming technique modifies this file to relate the Web addresses of well-known banks and financial institutions with the IP address of a phishing site, so when users opens their browsers and enter the address of their bank, they get sent to the phishing site instead. There is no need click on links in e-mails or other communications.

The second pharming 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. Now when the user enters a Web address, it is looked up in the DNS server; if the DNS server doesn't know the corresponding 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 e-mail that contains a link to a phishing Web site, and when the DNS lookup for that address is done, this extra information is included with the URL of the bank. This process is best described through 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 and Pharming Mitigations with McAfee

Anti-spam blocks e-mail phishes

McAfee anti-spam products include specific rules and filters for e-mail phishes. Using a variety of heuristic identification techniques, e-mail phishes can be detected and blocked even if the specific e-mail phish has not been seen by McAfee or any other security company—the true "zero day" phishing attack. 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 percent for known and unknown phishing e-mails.

McAfee anti-spam products can be installed in a variety of places depending on your specific requirements and applications. Multiple products can be deployed in order to achieve optimum performance.

The first layer of protection is provided by McAfee Secure Messaging Service,™ which scans and cleans messages before they ever reach your network. This service is hosted by McAfee—there is nothing to install or manage on your network. Secure Messaging Service quarantines messages found to contain spam, phishes, inappropriate content, and viruses.

The second layer of protection is installed at the edge of your network in the form of an easily managed appliance. McAfee Secure Messaging Gateway is designed for large enterprises (typically over 1,000 users), and McAfee Secure Internet Gateway is designed for smaller enterprises. Both appliances deliver comprehensive protection against spam, phishes, inappropriate content, and viruses.

The third layer of protection is installed on your mail servers. McAfee SpamKiller® for Mail Servers runs on both Microsoft® Exchange and Lotus Domino servers and blocks spam with the same level of effectiveness as our gateway appliances.

Web filtering blocks phishing communications

McAfee Web filtering blocks users from reaching phishing sites via their Web browsers. In this way, McAfee Web filtering blocks the outbound transmission of confidential information. This is a second method of protection, completely separate from the one mentioned above.

McAfee Web filtering runs on McAfee Secure Web Gateway and Secure Internet Gateway appliances. Secure Web Gateway is an enterprise-class, high-performance Web security appliance solution that delivers comprehensive protection against Web-borne threats such as spyware, viruses, worms, and Trojans. With the optional Web-filtering module, Secure Web Gateway blocks outbound efforts to browse to phishing sites, or even to communicate with them.

McAfee Secure Internet Gateway provides the same Web-based anti-phishing protection as Secure Web Gateway. However, Secure Internet Gateway also includes e-mail filtering, as mentioned in the previous section. By combining both e-mail and Web security in one appliance, Secure Internet Gateway is an excellent solution for small and medium-sized businesses that demand simple and comprehensive solutions but not extremely high message throughput or Web throughput.

What about desktop protection?

McAfee VirusScan® Enterprise, with its integrated intrusion protection and firewall technology, can also protect against pharming and phishing. With the addition of a simple rule, VirusScan Enterprise can prevent a virus or Trojan from modifying the user's local host file, which is a common pharming technique. The VirusScan firewall technology prevents Trojans and backdoors from sending harvested data to the phisher, and also prevents the machine from 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 McAfee anti-virus scanning engine and McAfee AVERT™ Lab.

Host and network intrusion protection

Phishers often target poorly protected machines, using them either as a host for their phishing sites (by compromising a legitimate Web server), or to initiate *phish spam*, from which collected data can be harvested for exploitation at a later date. McAfee Host Intrusion Prevention® and McAfee IntruShield® solutions help protect enterprise resources from being hijacked by criminals for use in these ways.

Conclusions

Phishing and pharming, along with their associated identity thefts, continue 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 sums of money made by criminal organizations through these activities is huge, the complexity and frequency of attacks will continue to grow.

McAfee security solutions can prevent phishing attacks, block spam, detect Trojans and keyloggers, protect against pharming techniques, and block phishing Web sites. The McAfee range of proven, proactive security products provide multiple levels of protection against this growing threat.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com