StBERNARD Software

Protecting your Network Investment

## Fighting The Hidden Dangers

# Of Internet Access

## Table of Contents



Introduction

## Objectionable Content isn't the Only Threat

In today's business environment, it's difficult to imagine a workplace without access to the Web. Yet, much of the information available to employees on the Internet is not job related. What started as a productivity boon has gradually turned into a bandwidth and productivity drain with huge potential legal liabilities associated with inappropriate use of the Internet by employees. Huge lawsuits have resulted from employees downloading pornographic, racist or violent material from the Internet. In addition, network security can be compromised by the introduction of viruses, worms or Trojans through your Internet access.

*A recent study by America Online and the National Center for Supercomputing Applications found that 80 percent of PCs were infected by some form of spyware, and each infected PC had an average 90 different spyware packages installed.*

It seems the old threat that plagued HTTP traffic, inappropriate content, is no longer the only concern for IT administrators. In addition to worms and viruses, your Internet access is a gateway for all sorts of other threats such as spyware, malware, phishing and pharming. These unwanted programs are propagating at a rapid rate. Even if you manage to stop one threat, new ones are cropping up daily, to take its place. Recently legislation was introduced in the United States to offer organizations relief from some of these attacks. But as was discovered with the CAN-SPAM Act, these laws are more likely to drive cyber criminals offshore. And with the amount of money being made from even isolated attacks, it is not surprising that organized crime would be involved in launching highly sophisticated attacks that exploit an organizations need to have online availability to do business.

In response, organizations have sought ways to proactively control Web access, driving the development of a variety of Web filtering methodologies. However, the emergence and growth of new Internet content, combined with the need for simple network installation and straightforward ways to effectively manage large user communities, has made most of these alternatives too cumbersome to employ in a corporate environment. And without the ability to control the invasion of spyware and malware, filtering objectionable content alone won't protect your organization.

This eBook attempts to present some of the growing threats that exploit your organization's Internet access and to demonstrate how a dedicated appliance solution like iPrism can secure your network and prevent the downtime, loss of productivity and other problems associated with unmanaged Internet access.

Part 1

## Spyware can be Tougher than Viruses

Spyware began as and continues to be a controversial subject. Companies such as Weatherbug prefer the term adware and are averse to any portrayal of their agents as malicious intruders. They consider their business practices to be legitimate and another form of marketing. But one thing they cannot argue with is that spyware is widespread and it's growing.

*Sixty-five percent of businesses--big and small--surveyed by Forrester Research said they plan to put money into protecting their systems from malicious and prying software programs in 2005.*

**Works like a Mole**

According to a recent article in Security Pipeline, "In the world of espionage, spyware is closest to a mole. A mole will avoid any activity that might blow his cover; similarly, spyware applications are often content to hide on your system." That's one way to distinguish them – they are usually not intentionally downloaded and they hide, often residing secretly as just another data link library (DLL) file or registry setting.

**Personal Data at Risk**

Spyware stays in it's hiding place, making eradication almost impossible while it collects the user's information such as his messaging habits, browsing behavior and online preferences. More nefarious spyware programs can scout for credit card information or other personal data or even hijack your PC and hold it hostage, demanding payment in return for restoring it's functions.

**Remediation is Difficult**

The main difference between viruses and spyware is money. Spyware is driven by profits whereas viruses are usually driven by rogue programmers looking to make a name for themselves. And unlike viruses, which can make their presence known by interfering with computer performance or even damaging your network, spyware embeds itself deep within critical components of your operating system. There it can use up memory with it's host of executables that monitor activities and collect data. Although viruses are dangerous, their overt activities are easier to spot and repair. Because spyware is so covert, it can remain on workstations for a long time and be difficult to remediate.

**Perimeter Protection is Best**

Clearly, the most effective solution is one that stops spyware and malware at the perimeter, before they can embed themselves deeply within your network. One way to achieve this perimeter protection is with an Internet filter that identifies and stops spyware sites at the perimeter, before they have a chance to infect your internal servers.

iPrism® from St. Bernard Sofware offers perimeter protection to block sites known to carry spyware, malware and phishing. The iPrism exclusive iGuard™ 100% human reviewed database includes a category that stops these pernicious programs from ever reaching your networks. And the iGuard team analysts work continually adding new sites to the database. Your iPrism is automatically updated every day, making it easy to stay ahead of the constant spyware, malware and phishing exploits.

Part 2

## Phishing Sites are on the Rise

Among the most ominous threats facing online users today are fraudulent sites built to appear as real e-commerce websites. These copycat sites, which are often perfect imitations of the legitamite site, are home base for phishers– the word used to describe hackers who build these "phishing" sites to fool users into divulging personal information such as user name, social security number, password or credit card numbers. This information is then either sold or used by the hackers themselves to exploit unwary consumers.

*" …instead of breaking into the bank to take money, phishers are tricking users into handing over their account information, or rather the electronic keys to the vault,"*

*Paul Judge*
*Chief Technology Officer*
*CipherTrust. "*

**High Growth Rate in 2004**

According to the Anti-Phishing Working Group (APWG), an organization devoted to reporting on and ultimately thwarting this illegal activity, at least 5% of users are fooled by the spoofed sites and suffer the consequences of credit card fraud, identity theft and financial loss.

In their year-end report, APWG reported a steady increase in spoofed sites, which grew at a rate of an astonishing 24% per month throughout 2004. More growth is expected this year. They also report that financial institutions are by far the most frequently targeted enterprises, accounting for nearly 75% of counterfeit Web sites. Another industry targeted by phishers is ISPs, which made up 16% of the phishing sites uncovered by APWG's research.

**More Sophisticated Phishing**

In a related CNN story published in January 2005, it was reported that phishing attacks are also getting more sophisticated as they proliferate. Although the image of the lone hacker working his mischief in solitude may be the current stereotype, the CNN story characterized the new wave of phishers as more akin to organized crime than petty criminals devising isolated attacks. This more sinister threat comes in the form of highly coordinated offensives from sources in the U.S., Russia and other countries. Their increasingly complex methods have elevated the stakes as e-commerce enterprises rush to try and secure their network assets and keep their customers protected.

**Coordinated Phishing Attacks**

The more organized attacks appear on the surface to be common phishing events where users are directed to a spoofed site that looks legitimate. Unlike regular phishing sites however, these URLs are hosts to malicious applications that plant code in the visitor's computer. Once infected with malware (malicious applications), even if users leave the phishing site without giving any information, they won't be safe. The next time they try to access the legitimate site by typing the Web address into a browser, the malware automatically redirects them to the fraudulent site. Since an accurate URL was entered, users have no idea they are at a phishing site. The CNN article states that this method was used successfully in attacks spoofing several South American banks. In those attacks, phishers took advantage of a Microsoft vulnerability on machines that had not been remediated by patching. The implications are sobering for everyone. Imagine typing your bank's URL into your browser and not knowing if you are at the legitimate site or not!

*"Contrary to a typical phishing attack, where fraudsters send out hundreds of thousands of e-mails and hope for the best results possible, personalized phishing attacks target individual named accountholders at specific banks."*

*consumeraffairs.com*

Part 3

## Pharming Attacks - Coming to a DNS Server Near You?

**Phishing Attacks are Easier to Spot**

By now, most of us are familiar with phishing attacks and likely have seen one or two of these fraudulent communications. They might be emails that tell us our bank or Paypal account needs updating. Inside a typical message, there is a link to what looks like an official Web site but is actually a scam, some of them authentic-looking, some not. The phony website is designed to gather your personal account information, passwords, Social Security numbers and other information useful to thieves. Fortunately, most of us notice the bogus URL or the awkwardness of the content before any real damage can be done.

*"The reason pharming can be lucrative is because it can fool even fairly savvy computer users. This attack starts when hackers take advantage of the ever-growing number of peer-to-peer applications to help spyware, a Trojan horse, or a virus slip past a computer's defenses and lodge itself in the background of a user's PC."*

*Paul Korzeniowski*
*TechNewsWorld*

**Pharming is on the Rise**

But what happens when the URL is the right address? What happens when, instead of clicking on a link within an email, you type the URL of your bank directly into your browser address bar – as you've done a thousand times before – and you're taken to a familiar site where nothing seems amiss? Only later do you discover that it's not your bank's site at all.

You've just had an encounter with pharming. And the worst part is you might not even know anything is wrong until it's too late. For you, it might mean getting an invasion of spyware or malware on your workstation, or worse, the theft of your credit card or social security number. For your company, it might mean a damaging virus or worm or the theft of intellectual property.

**Follow the Money**

According to a recent article in *Computerworld*, hackers are committing fraud at alarming rates and using sophisticated, multilayered methods that can stymie current network security efforts. What's in it for cyber pharmers? It's all about the money. Successful pharmers can get more personal data in a short time and can cast a much wider net to get that information.

**Organized Crime Gets Involved**

And since a bigger net means more fish and more illegal profits, it is no surprise that organized crime is getting involved in these scams. According to an article in *USA Today*, “Pharmers generally come from overseas, such as China, Russia and Eastern Europe, experts say. They fear many are tied to organized-crime rings that buy and sell identity information.”

There are currently two ways pharming attacks occur – through domain hijacking or by DNS poisoning.

**Hijacking Your Trusted Domains**

Domain hijacking is the practice of stealing an organization or individual website name. This method typically relies on the victim’s lack of vigilance. In a common scenario, perpetrators send a phony or misleading registration transfer approval form, or a fraudulent transfer authorization to a website owner. These are usually timed to coincide with domain name renewals. Unwitting victims automatically ok the transfer or authorization, thinking it’s a legitimate renewal notice. In a related scam, cyber squatters purchase domain names that are identical to existing website addresses except for one or two letters and wait for visitors to misspell addresses. And it’s hard to tell when you’ve been spoofed. Cyber criminals build websites that are usually remarkably identical to the real ones. Visitors enter their personal data, thinking nothing is awry and the crime ensues.

*"...online crime is no longer predominately the purview of lonely teens seeking self-esteem, it is increasingly being propagated by organized crime gangs selling access to 'owned' machines."*

*WiKID Systems*

**DNS Cache Poisoning**

Another, even more sophisticated technique involves corrupting or “poisoning” a domain name system table by replacing a legitimate Internet address with a fraudulent site address. When this happens, a worm, spyware, a Web browser-hijacking program, or other malware can be downloaded to the user's computer from the rogue location. According to a recent TechTarget article, once an end user's computer has been infected with the nefarious code, all future requests by that user's computer for the compromised URL will be redirected to the bad IP address -- even if the "victim" server resolves the problem at its site. Cache poisoning differs from another form of DNS poisoning, in which the attacker spoofs valid e-mail accounts and floods the inboxes of administrative and technical contacts. However, the objective is always the same, spoofing legitimate sites in order to profit from unwitting visitors.

Part 4

## A Strategic Solution

No one is predicting that spyware, malware, phishing and pharming attacks will go away, anytime soon. In fact, these sorts of applications will likely become even more sophisticated in their methods. What is clear is that Internet access management is a critical component when developing a security strategy for your organization. You are faced with a myriad of threats that have one thing in common, they can enter through your unmonitored Internet access.

*"Being able to control and monitor our employees' Internet usage is extremely beneficial, and, with iPrism, managers can easily run reports to see what sites people are visiting and how frequently they are accessed. We are much more comfortable knowing that people are not accessing inappropriate Web sites."*
*--Tricia Davidson, Citrix Administrator, Berger Transfer & Storage*

**The ABC's of Secure Internet Access**

As an appliance-based web filtering solution, iPrism offers the unmatched security of a hardened and optimized O/S and fits easily into any network topology. Here are some outstanding features:

a. iPrism is a comprehensive Internet access management solution – no additional hardware or software is required.
b. iPrism has superior interoperability and works with any network topology. It's easy to install and configure and is virtually maintenance-free.
c. iPrism is easy-to-use with a central management console that lets you manage Internet access across your network from any machine that has a web browser.
d. Our unique 100% human-reviewed iGuard database includes 63 categories encompassing millions of URLs. Not only can you block access to objectionable sites such as those that are pornographic, violent or racist, you can also block sites known to carry spyware, malware and phishing.
e. iGuard database updates are sent daily to your iPrism over a secure connection.
f. You can generate a variety of management reports enabling you to monitor and report on your organizations Web activity.

Whether Internet dangers are hidden such as spyware, phishing and pharming, or obvious ones such as sites that have pornographic or violent content, your employees and networks aren't secure unless you are managing your organization's Internet activity. No one in today's treacherous cyberspace can afford the risks of lawsuits, lost productivity, loss of intellectual property or network threats that are the result of unfiltered Web access.

For more information about iPrism, visit the St. Bernard Software website www.stbernard.com/iprism or for immediate help, call **800-782-3762.**

For more information about St. Bernard Software and iPrism, visit us at http://www.stbernard.com or visit the iPrism product pages.

**Contact Information**

St. Bernard Software (North America, South America, Pacific Rim)
15015 Avenue of Science
San Diego, CA, 92128
Sales Phone: 800.782.3762
Sales Fax: 858-676-2299
Sales Email: sales@stbernard.com

St. Bernard Software (Europe, Asia, Africa)
Unit 4
Riverside Way
Watchmoor Park, Camberley
Surrey, UK
GU15 3YQ
Sales Phone: 44.1276.401.640
Sales Fax: 44.1276.684.479
Sales Email: sales@uk.stbernard.com