Realtime
publishers
"Leading the Conversation"

The Shortcut Guide™ To

Protecting Business Internet Usage

sponsored by

SurfControl®

Dan Sullivan

Copyright Statement

Chapter 2: The Evolving Landscape of Protecting Internet Access

Business Internet use is subject to a dynamic environment in which both external and internal threats adapt to preventive measures as well as emerging opportunities. For example, computer viruses were once transmitted via diskettes shared among PCs. Later, they leveraged the communications capabilities of the Internet. Since then, they have incorporated multiple techniques to avoid detection. As viruses became more sophisticated, so did the countermeasures for detecting and stopping them. This chapter will examine the evolving nature of threats and countermeasures, in particular, it will examine:

- Common inbound threats
- Common outbound and intra-organizational threats
- Growing complexity of threats
- Increasingly sophisticated countermeasures

As this chapter will demonstrate, the wide variety of threats facing business Internet use requires a broad range of countermeasures. There is no single solution that will preserve the integrity of business operations on the Internet.

Common Inbound Threats

Inbound threats are threats that originate from outside an organization and use Internet connectivity to damage, disrupt, and steal corporate assets. By now, the list of common inbound threats is familiar to IT professionals and includes:

- Viruses, worms, and other malware
- Spyware
- Spam
- Phishing scams
- Denial of Service (DoS) attacks

In each case, these threats have become more sophisticated over time as developers of these tactics become adept at avoiding detection and increasing the effectiveness of their programs and content.

Viruses, Worms, and Other Malware

Malware, or malicious software, is a collection of types of programs that are designed to disrupt and damage systems. Malware began as relatively benign viruses spread between PCs and did little more than display messages. By the late 1990s, malware took a distinct turn toward damaging infected systems by deleting the contents of hard drives, as in the case of the CIH Virus released in 1998. Since then, new forms of malware have been created and even the basic virus has acquired newer and more sophisticated techniques.

Viruses

Viruses are malicious but relatively simple programs that depend upon other programs to propagate. They consist of two essential parts: a mechanism for exploiting other programs to propagate and a payload (see Figure 2.1).

Form and Function

The propagation mechanism can either attach the virus to an operating system (OS) object, such as a boot sector or a file, or use a feature of an application, such as macros, to spread. Email viruses were once a popular form of virus, but antivirus and email scanning technologies are well adept at dealing with these, and properly protected email systems are not nearly as likely to fall victim to this type of attack as they once were. (Email worms, a different type of malware, have been responsible for some of the fastest spreading attacks. These are described later).

The payload of viruses is the code that actually causes damage. The payload can be more annoying than disruptive, as in the case of early viruses, or it can cause substantial damage.

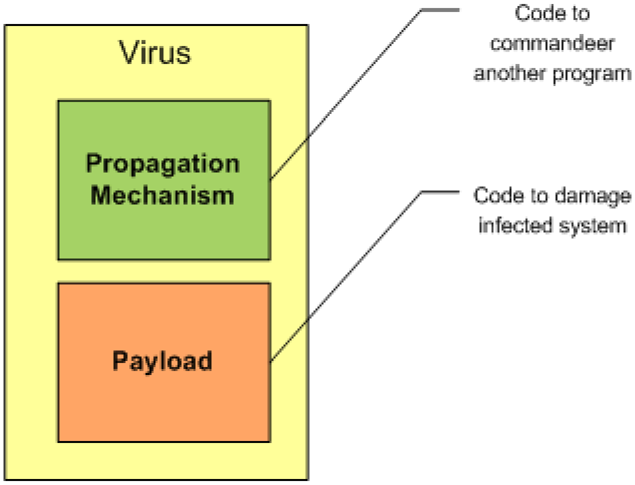

Virus
Propagation Mechanism
Payload
Code to commandeer another program
Code to damage infected system

Figure 2.1: Computer viruses have two main parts: a propagation mechanism and a payload.

Creating an early virus required at least a basic knowledge of assembly language programming and basic computer and OS architecture. The advent of macro viruses opened the world of malicious software to even those with only rudimentary programming skills. Those aspiring malware writers for whom even macro programming was too challenging did not have to wait long before the advent of virus generators. These are programs that can be used by anyone with basic computer skills to select a few parameters, such as the type of damage to do (for example, delete files); the generator then creates a program. The last step for the virus "writer" is to simply unleash the malware. Fortunately, the more easily developed viruses, such as macro viruses and generated viruses are easily detected and dispatched by antivirus software.

> 🕮 For a brief history of computer viruses, see Brian Krebs' "A Short History of Computer Viruses and Attacks" at http://www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html.

Virus Detection

Viruses are programs and so are instantiated in binary files that are executed on target machines. This simple and obvious fact makes it relatively easy to detect viruses (at least early viruses): find a pattern of 1s and 0s in the binary file of the virus that is not likely to be found in any other program. Antivirus programs scan files for this pattern, or signature, as it is typically called. If the signature is detected in the program, the file is likely to be the virus. First generation antivirus software essentially consisted of a library of virus signatures and a pattern-matching program. As new viruses were discovered, their signatures were added to libraries. (This is the reason it is so important to keep antivirus software up to date).

Virus developers responded to signature-based detection by first encrypting viruses. The encryption process takes the virus binary file as input and outputs another file without the patterns found in the original. This was a slight improvement from the virus developer's perspective, but it was a short-lived solution. Antivirus researchers quickly found the Achilles' heel of this technique: the encrypted virus file had to be decrypted before executing, and so the program had to include a decryption module. That module could not be encrypted, so signatures were identified for the decryption module, and encrypted viruses were once again vulnerable to signature-based detection.

Continuing the pattern of response and counter-response that has characterized the evolution of malware, virus developers introduced a number of mutating techniques, including:

- Oligomorphic viruses, which change their decryption modules by introducing extra computer instructions that change the patterns in the binary file without changing the functionality of the program when the virus copies itself.
- Polymorphic viruses are similar to oligomorphic viruses but these change their decryption modules and can use different decryption methods in successive generations.
- Metamorphic viruses do not use encryption but carry their source code with them. When they reproduce, they add random instructions or change the order of instruction in such a way that does not change the behavior of the program. The virus then recompiles itself on the target machine. These viruses are especially a threat to Linux and UNIX systems, which often have compilers installed.

Although signature-based detection has proven itself efficient and effective in many cases, the emergence of mutating viruses required a different approach. Rather than look at patterns in a file to detect mutating viruses, many antivirus programs now simulate the execution of the program and look for patterns in the behavior that are characteristic of viruses. A defining characteristic of viruses is that they depend upon other programs to propagate; not all malware has that limitation.

Worms: Fast Spreading Malware

Worms are similar to viruses, and in fact many people refer to worms as viruses, but they are distinct. The functional difference between the two is that worms do not depend upon another program to propagate; they leverage vulnerabilities in networks, OSs, or application programs to spread.

Take the SQL Slammer worm, for example—a worm that exploits a vulnerability in Microsoft SQL Server and Microsoft Desktop Engine 2000. The worm first sends a large amount of data to a vulnerable server causing a buffer overflow (a condition that occurs when a program accepts more data than it can hold, resulting in some program code being overwritten in memory by that data). The data sent to the server is crafted to cause the server to send out messages to randomly selected IP addresses. If the message is received by a vulnerable host, it too becomes infected and starts spreading the worm.

SQL Slammer has a number of characteristics that are worth noting:

- It is a small worm, using a 376-byte message to deliver it.
- By sending messages to random IP addresses, it targeted the widest possible range of machines.
- The propagation code is simple and therefore spreads rapidly.
- SQL Slammer had no distinct payload; the very act of spreading was itself an attack on the Internet. The worm effectively shutdown segments of the Internet within minutes.

> ✎ In addition to the worms' characteristics, it should be noted that the systems that were infected played a significant role in the spread of the worm.

First, SQL Slammer exploited a known vulnerability; Microsoft had provided a patch for the problem months before SQL Slammer struck. Had systems managers and database administers applied the appropriate patch in a timely manner, the worm could not have spread. Second, many users of desktop applications that use the Microsoft Desktop Engine 2000 did not know they had a vulnerable application. The combination of poor patch management, the widespread distribution of a vulnerable program, and the deployment of a relatively simple worm created a perfect storm of Internet traffic.

There are several lessons to be learned from the SQL Slammer incident:

- Develop and follow patch management procedures.
- Use vulnerability scanners to detect vulnerabilities, especially when complex applications are running.
- Desktop applications are becoming increasingly complex and can become targets of worms and other malicious software.
- Peripheral defenses, such as firewalls, should be configured to allow minimal traffic in and out of a network. The vulnerability exploited by SQL Slammer was in a name resolution service. If there is no need for resolving names of databases outside the firewall, that traffic should be blocked.
- Content entering a network should be scanned. Content-filtering systems and intrusion prevention systems (IPSs) can help reduce the likelihood of a successful attack.

> 🕮 For a detailed analysis of the spread of SQL Slammer, see Robert Beverly's "MS-SQL Slammer/Sapphire Traffic Analysis" at http://momo.lcs.mit.edu/slammer/. For a description of the vulnerability exploited by the worm, see http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0649.

Viruses and worms are the most well-known forms of malware but there are others.

Other Forms of Malware

Two other types of malware, Trojan horses and rootkits, are common threats. Both are concealed programs and can damage and disrupt business operations.

Fooling Users: Trojan Horses and Botnets

Trojan horses are malicious programs that spread by accompanying other, often legitimate programs. Users download a legitimate program and in the process unknowingly install malware on their system. For example, someone might download a browser toolbar that purportedly provides weather information when in fact, in addition to the weather service program, the downloaded program also sends a worm or virus to the machine.

As the dynamics of malware begin to take on economic dimensions, Trojan horses can be used to commandeer computers for use in networks of compromised hosts used to perform tasks for the malware developer. These compromised hosts, known as *botnets*, can receive instructions by monitoring Internet service provider (ISP) chat rooms and Internet relay chats (IRCs) or checking ftp sites for commands, which might include:

- Download or upload files—for example, to store and distribute bootleg music files
- Send spam using a simple email server installed on the compromised host
- Launch a Distributed Denial of Service attack (DDoS)
- Scan for personal information on the infected computer, such as account numbers, Social Security numbers, usernames, and passwords

The economic drivers behind these types of attacks will continue to drive the development of Trojan horses and botnets. For example, a 20-year-old California man purportedly earned $60,000 selling access to botnets to spammers and hackers, according to NetworkWorld. (Source: Ellen Messmer, "Botnets Get Nastier" http://www.networkworld.com/news/2005/110705-botnets.html).

For more information about the botnet threat, see Martin Overton "Bots and Botnets: Risks, Issues and Prevention" available at http://www.astalavista.com/media/directory06/uploads/4729cea4b5b6a2bbacb8410f9e1a4d45.pdf.

Of course, Trojans and botnets are of little use to their developers if their malware is discovered and removed. To keep control of systems, the developers must keep their programs hidden.

Rootkits Cover Tracks

Rootkits are programs devised to remove traces of activity on a system and to prevent detection of actively running programs. For example, when a task list is displayed in Windows, as shown in Figure 2.2, the rootkit must alter the results of the listing to prevent its own name from appearing.

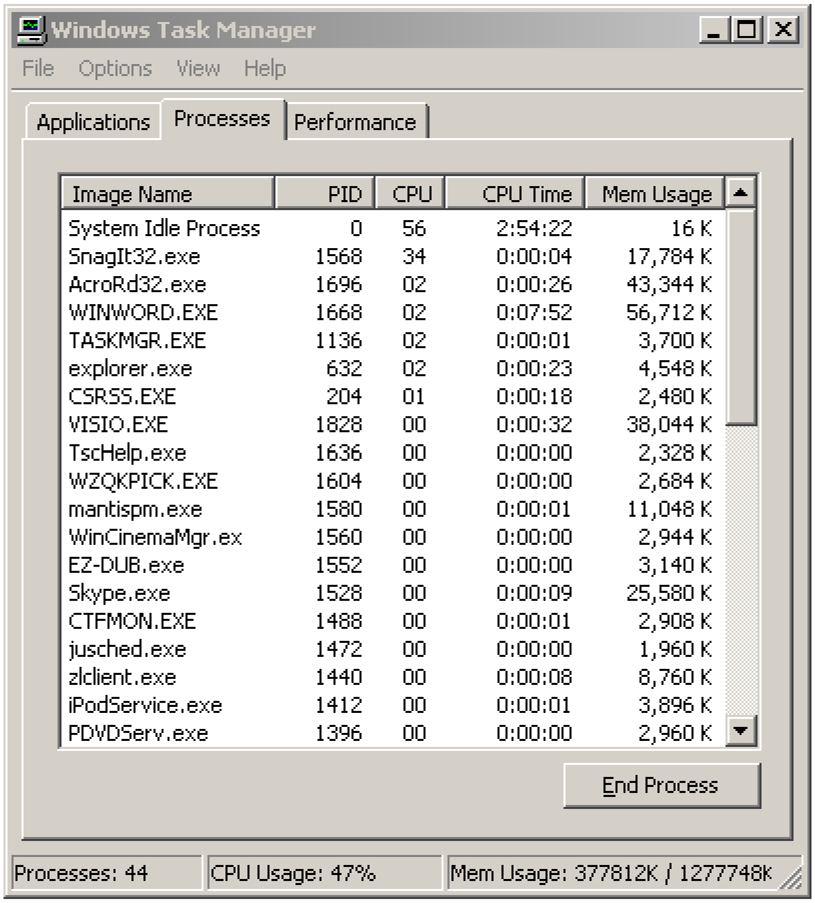


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	56	2:54:22	16 K
SnagIt32.exe	1568	34	0:00:04	17,784 K
AcroRd32.exe	1696	02	0:00:26	43,344 K
WINWORD.EXE	1668	02	0:07:52	56,712 K
TASKMGR.EXE	1136	02	0:00:01	3,700 K
explorer.exe	632	02	0:00:23	4,548 K
CSRSS.EXE	204	01	0:00:18	2,480 K
VISIO.EXE	1828	00	0:00:32	38,044 K
TscHelp.exe	1636	00	0:00:00	2,328 K
WZQKPICK.EXE	1604	00	0:00:00	2,684 K
mantispm.exe	1580	00	0:00:01	11,048 K
WinCinemaMgr.ex	1560	00	0:00:00	2,944 K
EZ-DUB.exe	1552	00	0:00:00	3,140 K
Skype.exe	1528	00	0:00:09	25,580 K
CTFMON.EXE	1488	00	0:00:01	2,908 K
jusched.exe	1472	00	0:00:00	1,960 K
zlclient.exe	1440	00	0:00:08	8,760 K
iPodService.exe	1412	00	0:00:01	3,896 K
PDVDServ.exe	1396	00	0:00:00	2,960 K

Processes: 44 CPU Usage: 47% Mem Usage: 377812K / 1277748K

Figure 2.2: The Windows Task Manager would reveal the existence of a rootkit process if the rootkit did not alter the listing.

Rootkits similarly have to hide files on hard drives and entries in the Windows registry. They usually accomplish these tasks by intercepting messages to application programming interface (API) functions in the OS. Because so many of the utilities used by end users depend on these services, those utilities may not reveal the existence of a rootkit.

Many virus and malware scanners detect and remove rootkits. In addition, specialized tools can be used to scan disks for binary files of known rootkits. They can also analyze the behavior of systems by comparing the results of an API function call with results obtained by another method; for example, analyzing the low-level details of disk storage.

> 📖 Specialized tools may be able to detect some rootkits. RootKitRevealer is a free rootkit detection tool available from http://www.sysinternals.com/utilities/rootkitrevealer.html.

The purpose of worms and viruses is to disrupt, but not all malware has such obvious consequences. Trojan horses, botnets, and rootkits can function together to commandeer sizeable networks of computing resources without destroying the resources. Economic factors will continue to drive the evolution of malware and one form, spyware, is especially problematic.

> 📖 Malware developers are increasingly targeting businesses. See Deborah Gage "Cyber criminals turn their attention to the Corporate World" at http://www.baselinemag.com/article2/0,1540,1953539,00.asp.

Spyware and Information Theft

Spyware, like Trojan horses and botnets hidden with rootkits, can operate undetected and apparently cause no harm, when, in fact, information is being stolen. The purpose of spyware is to quietly collect information and send it to the person of group deploying the spyware. Spyware takes on many forms, including:

- Keyloggers
- Video frame grabbers
- Homepage hijackers
- Tracking cookies

Used in conjunction, these tools can provide attackers with information about bank accounts, government identification numbers, and other personal and financial information.

Stealing Information with Keyloggers and Video Frame Grabbers

Keyloggers are programs that intercept keystrokes as they are sent from the OS to an application. (There are also hardware versions of keyloggers, but they are not the same type of threat as software-based keyloggers). These tools are especially useful for capturing usernames and passwords. For example, a keylogger might record www.mybank.com followed by sjohnson and then max123. This is easily identified as a bank site Web address followed by a likely username and password. Even with just one side of a Web interaction (the results returned are not available to the keylogger), the attacker can gain valuable information by analyzing patterns in the keystrokes.

Other information can be gleaned by stealing screenshots (pictures of the computer screen at a given time) of online activity. Consider an executive who receives an email with updated sales projections. She opens the spreadsheet but does not type anything. A keylogger is of no use here, and even if keystrokes were detected, they could not provide sufficient context to determine the contents of the spreadsheet. Video frame grabbers, however, can copy the contents of the system video buffer at regular intervals and send images back to the attacker.

Devices infected with keyloggers and video frame grabbers can capture virtually any information that is typed or displayed. Other forms of spyware are more of an annoyance than a threat to information loss.

Benign Spyware?

Tracking cookies are used by advertisers to analyze online behaviors and browsing patterns in an effort to more effectively target advertisements. For example, when a user visits Site 1, a tracking cookie is placed on the user's computer. When the user then browses to Site 2, an Internet ad service company scans for known cookies, such as those from Site 1. When one is found, the advertising system will push adds to someone with interests related to Site 1 and Site 2. Although this type of spyware does not steal information, many consider this type of tracking a violation of privacy. In addition, Site 2 now knows that the user visited Site 1 and can capture and sell that information to organizations that analyze Internet browsing behavior.

Another problematic technique used by some advertisers to drive page hits on their sites and create opportunities to display advertisements is homepage hijacking. When a user visits a site or downloads a program, the user's browser is reset to point the homepage to one controlled by an advertiser. Now each time the browser is opened, it visits the desired homepage, which increases the page's exposure, resulting in a financial gain for the attacker (who is paid each time a user accesses the page). A specialized program, called a browser helper object, may also be installed to reset the homepage back to the advertiser's page if the user attempts to reset the homepage.

Tools are readily available to detect and remove spyware, but it is more efficient to prevent it from entering a system to begin with. The same is true of spam.

Spam and Email Management

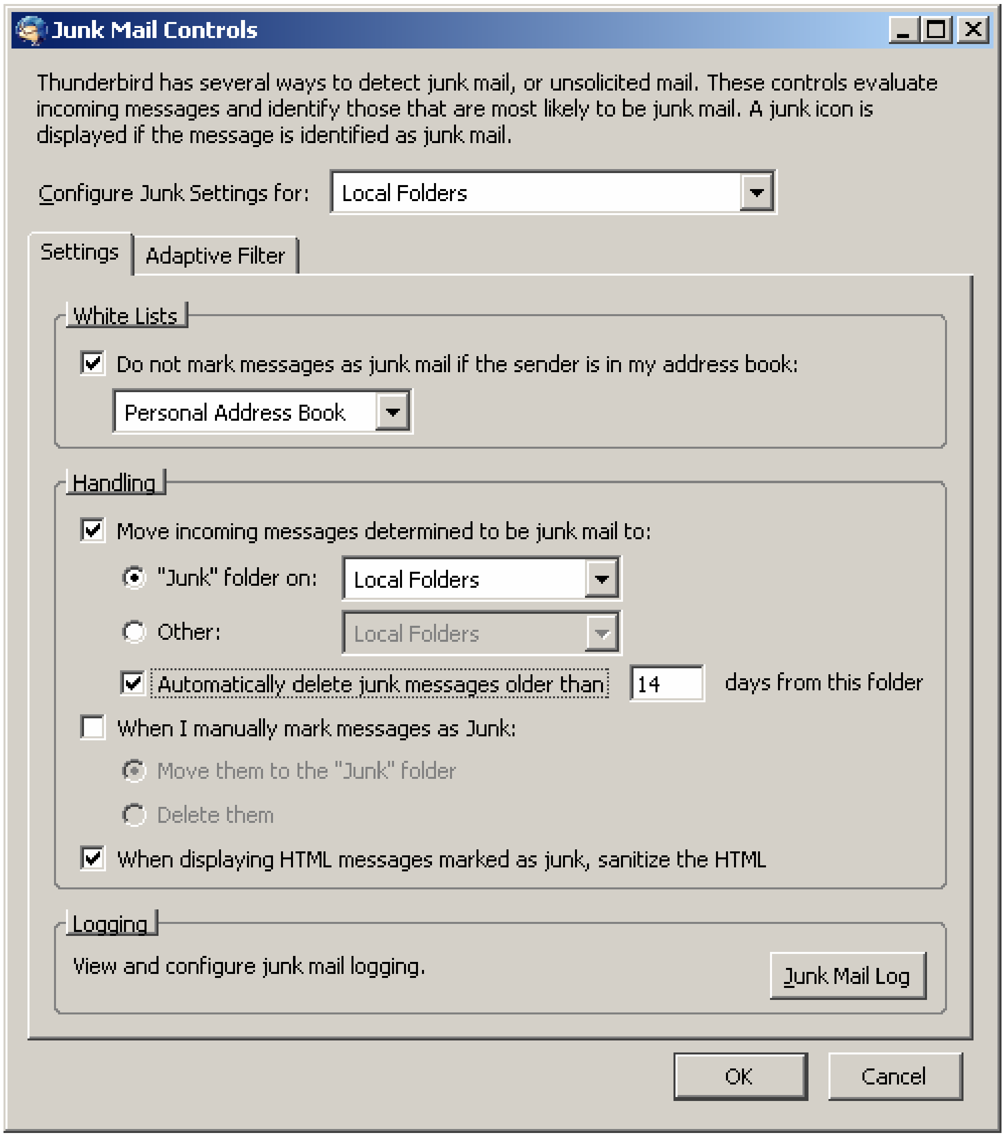
Spam is unwanted and unsolicited email—and no one with an email address apparently is immune to it. We've all likely had enough experience with spam to know what it is; the question is what do you do about it? There are a few basic options (in addition to just putting up with it):

- Detect and delete on the client device
- Detect and quarantine on the email server
- Detect and block at the network perimeter

Each approach has benefits and drawbacks, and in practice, two or all three of these techniques may be used.

Client Detection of Spam

Client detection of spam requires the least centralized management and provides users with a great deal of control over how spam is handled. As Figure 2.3 shows, users can configure where spam, also referred to as junk mail, is stored, if it is automatically deleted, and whether to apply additional security measures, such as sanitizing HTML messages for questionable code.



Junk Mail Controls

Thunderbird has several ways to detect junk mail, or unsolicited mail. These controls evaluate incoming messages and identify those that are most likely to be junk mail. A junk icon is displayed if the message is identified as junk mail.

Configure Junk Settings for: Local Folders

Settings | Adaptive Filter

White Lists

☑ Do not mark messages as junk mail if the sender is in my address book:

Personal Address Book

Handling

☑ Move incoming messages determined to be junk mail to:

● "Junk" folder on: Local Folders

○ Other: Local Folders

☑ Automatically delete junk messages older than 14 days from this folder

☐ When I manually mark messages as Junk:

● Move them to the "Junk" folder

○ Delete them

☑ When displaying HTML messages marked as junk, sanitize the HTML

Logging

View and configure junk mail logging.

Figure 2.3: Email clients, such as Firefox Thunderbird, provide several controls for automatic spam detection and removal.

A disadvantage of client-side spam management is that the spam will still consume network and email server resources prior to reaching the client. Once on the client, spam will continue to occupy storage space until the spam is purged. In addition, spam may carry other threats such as phishing lures (described later), viruses, or other malware. Rather than download the spam to the client device, email administrators may quarantine it on the email server.

Server-Side Spam Management

Server-side spam management provides for centralized management of spam. Policies can be enforced at the server level, providing consistency across the organization. This model also allows email administrators to monitor the size of quarantine folders, volumes of spam, and common sources of spam.

Other advantages apply to end users. Their storage space is no longer consumed by junk mail, and spam containing malware is not resident on their machines. Users still have to manage their quarantined messages or accept system defaults for deleting messages after a specified period of time. Like client-side management, this model requires storage for spam. However, because spam is centrally managed, email administrators can purge quarantine folders as needed to recover storage. When multiple email servers are used or when organization policy dictates that spam should be deleted rather than quarantined, network filtering is an option.

Network-Based Spam Management

With network-based spam management techniques, email content is scanned and spam is identified before it reaches the email server. This method is especially appealing for organizations that simply delete spam; there is no need to process or store it on the email server or the client device. This technique also conserves bandwidth by blocking the transmission of spam.

> ✎ Network-based email scanners can also be configured to quarantine spam.

It is also a useful approach when multiple email servers are in use because multiple email servers can be protected by a single anti-spam appliance or application. As Figure 2.4 shows, the further into the network the spam reaches, the more decentralized its management becomes.

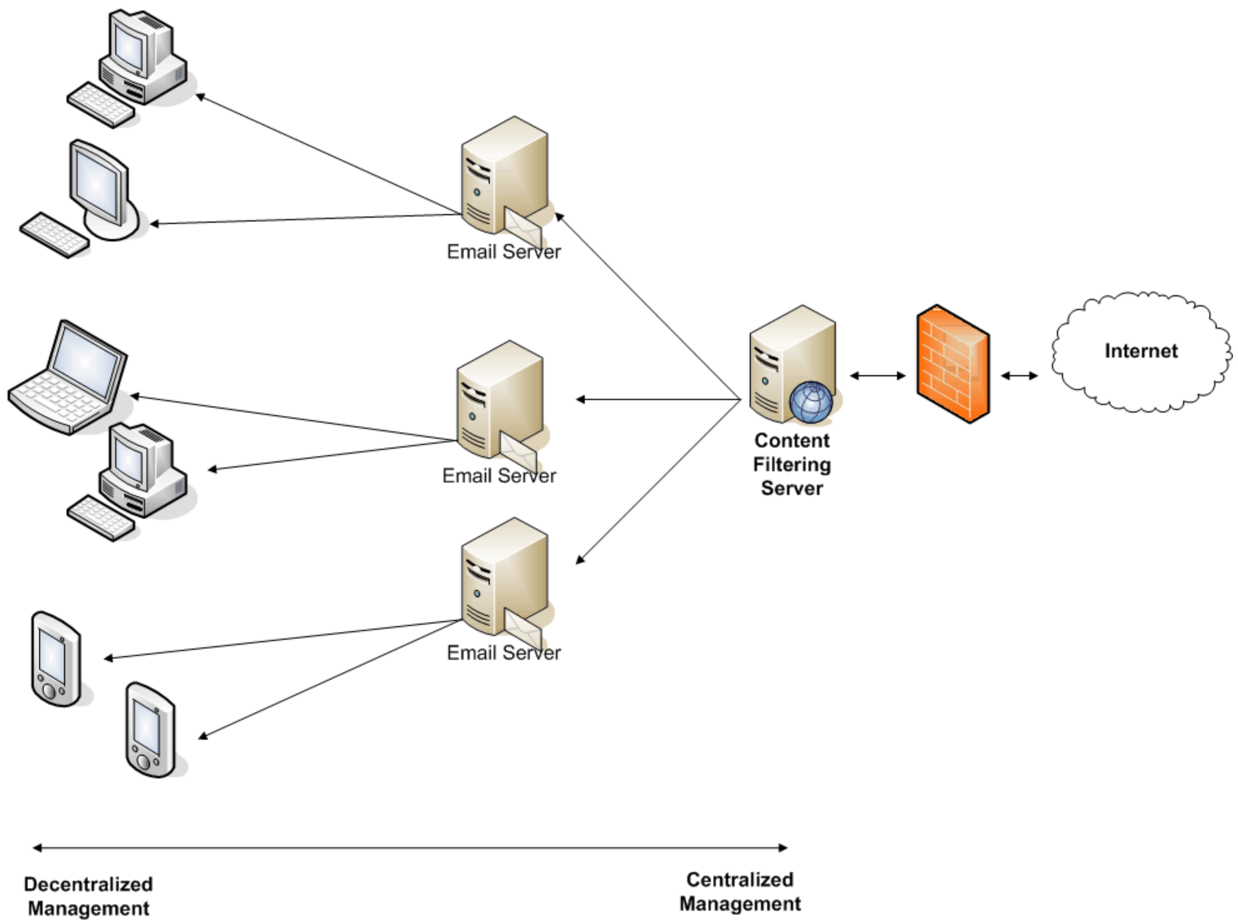


Figure 2.4: Spam filtering can occur at multiple points in the network; the closer to the client the spam controls are applied, the more decentralized the management.

Phishing uses a form of spamming with the intent of defrauding the recipient but often includes other components in addition to the email message.

Phishing and Fraud

Phishing is a fraud scheme in which victims are tricked with misleading forged email or Web sites into revealing personally identifying information or sending funds to a criminal. At first, phishers used widely recognized brands to trick victims; banks were a common target as were popular e-commerce sites such as eBay and PayPal. These messages were sent to a large number of potential victims in an attempt to lure the greatest number of victims. The mass emailings, though, were easily detected, and as email users adapted to the threat of phishing, the phishers had to adjust their approach.

Phishing Basics

With phishing, a message is sent to a potential victim, purportedly from a legitimate business. The message contains a request for some action on the recipient's part, such as confirming a new email address added to an account, updating account information, or verifying a recent transaction to prevent identity theft. (Phishers are at no loss for a sense of irony). This first step is known as the "lure;" it is followed by the "hook."

Typically, the phishing message will contain a URL of a bogus site that appears to be a legitimate site of the hijacked brand. At the bogus site, the victim is prompted to supply personal information, account numbers, and so on. Even when victims are careful to read the URL supplied in the message, the apparent URL and the actual target location may be different.

> 📖 For examples of phishing emails and hijacked brands, see the Anti-Phishing Working Group archives at http://www.antiphishing.org/phishing_archive.html.

A more targeted method of phishing, known as *spear phishing*, uses regional and less widely known brands. Phishers also limit the number of phishing messages sent to reduce the chance of detection. Regardless of the brand used or the number of potential victims targeted, the techniques are essentially the same.

Countermeasures and Responses

A combination of growing awareness among consumers and efforts by businesses are making successful phishing scams more difficult. For example, some banks now allow customers to choose an identifying image that is displayed when they log into the site. It would be virtually impossible for phishers to display the correct image at a bogus site. (This assumes a sufficiently large number of images to choose from and the absence of other information, such as a copy of the selected image captured by a Trojan horse.)

Despite improvements in phishing prevention, attacks continue. In April 2006, the Anti-Phishing Working Group received 17,490 reports of unique phishing attacks and 11,121 unique phishing sites. These sites are short lived, averaging just 5 days online. These attacks are occurring around the world, although the United States receives the most phishing attacks. In a recent 12-month period, the United States has led the world with 35 percent of phishing attacks, followed by China with 17 percent, and Germany with 4.5 percent; other countries accounted less than 3 percent of attacks each. The United States hosts the most phishing sites with 26.3 percent, followed by China with 21.2 percent, and the Republic of Korea with 7.2 percent.

> 📖 Phishing statistics are from the Anti-Phishing Working Group, http://www.antiphishing.org. A world map of showing the distribution of phishing attacks is available at http://www.antiphishing.org/crimeware.html. For an archive of phishing messages, see http://www.antiphishing.org/phishing_archive.html.

Mosaic of Inbound Threats

Viruses, worms, spam, phishing scams, Trojan horses, keyloggers, and video frame grabbers are just some of the threats to the integrity of business Internet use. The list of threats can sound intimidating, but remember that countermeasures are available to reduce the risk of these threats. Many countermeasures are technical, but some are organizational policies that define appropriate use of IT equipment. The countermeasures used to control inbound threats also support the control of outbound threats.

Outbound and Intra-Organizational Threats

The notion of being one’s own worst enemy applies too often to information security. Not all threats originate outside the network perimeter. Two in particular, offensive content in the workplace and information leaks, are threats to business Internet use.

Offensive Content in the Workplace

Legislation, case law, and administrative law have established minimal standards in the United States for appropriate working conditions. Although employers are free to establish many aspects of the workplace, they must prevent the emergence of a hostile work environment. A hostile work environment is one in which employees feel harassed, intimidated, or abused. The Internet is emerging as a factor in preserving the integrity of the workplace.

The Internet is in some ways a reflection of society at large. With enough effort, someone can probably find material on every topic that exists in some form in the world’s cultures. Many are edifying and many are divisive, degrading, and offensive. Keeping the latter out of the business environment is one of the responsibilities of management.

Types of offensive content that can make their way into the workplace if not properly controlled include sexually explicit material, hate speech, and offensive language. Some statistics are worth noting regarding content inappropriate for the workplace:

- 70 percent of Internet pornography is downloaded during normal business hours
- 14 percent of interviewees admit to forwarding inappropriate emails to friends or coworkers
- 29 percent of interviewees know someone that their current employer has punished or reprimanded for sending inappropriate email
- 44 percent of interviewees either do not have acceptable use policies in their organization or do not follow them

> 📖 These statistics and others are available in SurfControl’s “Virtual Image Agent: Data Fact Sheet” available at http://www.surfcontrol.com/general/guides/email/Virtual_Image_Agent3.pdf.

Without proper controls to prevent this material from entering and circulating within an organization’s network, an organization leaves itself at risk for unauthorized and unsanctioned use of its network resources that could lead to a hostile work environment. In addition to inappropriate material entering the organization, the Internet can be used to send confidential information out.

Information Loss

Euphemisms such as "data spills" and "data leaks" have been employed to describe security breaches in businesses and government agencies. This choice of terms may be the product of a misunderstanding of the impact of disclosing private and confidential information—an attempt to minimize the organization's responsibility by reducing the apparent effects of the breach, or, perhaps worst of all, these disclosures have become so common that we are no longer too concerned about them. Regardless of the reason, these terms do not adequately describe the problem faced by organizations depending on the Internet as part of their operation:

- A breach at KDDI, Japan's second largest mobile provider, disclosed personal information about 4 million subscribers in June 2006 (Source: "Japan's KDDI Report Massive Personal Data Leak" at http://www.forbes.com/finance/feeds/afx/2006/06/13/afx2811559.html).
- A breach at BJ's Wholesale Club in 2004 exposed an undisclosed number of credit card numbers; dozens of banks reissued tens of thousands of credit cards in response (Source: Bob Sullivan, "Credit Card Leaks Continue at Furious Pace" http://www.msnbc.msn.com/id/6030057/).
- In February 2006, a contractor sent names and Social Security numbers of current and former employees of Blue Cross Blue Shield of Florida to a home computer (Source: Privacy Rights Clearing House, http://www.privacyrights.org/ar/ChronDataBreaches.htm).

> 🕮 For a sobering list of breaches and information loss reported since the well-publicized ChoicePoint breach in February, 2005 see http://www.privacyrights.org/ar/ChronDataBreaches.htm. As of June 2006, the Privacy Rights Clearinghouse site reported 85,149,886 instances of personal information being lost, stolen, or otherwise disclosed.

Privacy violations could have been covered up in the past. Now legislation and government regulations are requiring more of these incidents to be reported to customers. The state of California, for example, requires customers who live in California to be notified if their personal information is disclosed through a new law called the California Information Practice Act (often called Senate Bill 1386 or SB-1386). Federal legislation, such as the Health Insurance Portability and Accessibility Act (HIPAA) and Gramm-Leach-Bliley Act, specify privacy rules for healthcare and financial service providers, respectively.

In addition, there is the risk of lost consumer confidence; no company wants to be the next poster child for data security breaches. CardSystems Solutions, a credit card processor, lost contracts with Visa and American Express after the processor reported that 40 million accounts were at risk of fraud because of poor data management. In addition to privacy losses, intellectual property can be lost.

Intellectual property, such as product designs, process models, strategic plans, and other business-critical information, has obvious economic value to competitors. As the economic motives behind cybercrime continue to grow, intellectual property should be adequately protected. Perpetrators may be outsiders or employees, contractors and others with access to this guarded information. One of the measures that can address the potential theft of proprietary information is appropriate Internet access safeguards. The threats themselves are growing more sophisticated but fortunately so are the countermeasures.

Growing Complexity of Threats

Earlier, this chapter examined specific types of threats, such as viruses and keyloggers. As with any successful technology, malware has built on past achievements. Viruses have become more difficult to detect thanks to encryption and metamorphic techniques. The shortcomings of keyloggers are compensated for with video frame grabbers. Not surprisingly, malware developers have started to combine multiple types of malware into a single application known as a blended threat. They are also using multiple methods to spread malware applications. These are called multi-vector threats. Today, IT professionals should assume that blended, multi-vector threats are the least state of the art malware they will have to content with—and if history is any indicator, it will just get worse.

Take the Nimda malware for example. Released in September 2001, it attacked Windows OSs using several methods to replicate, including:

- Email
- Network shared drives and folders
- Compromised Web sites
- Microsoft IIS vulnerabilities
- Backdoors left by other worms

The worm spread quickly in part because it could use multiple vectors.

📖 For details about Nimda, see F-Secure's description at http://www.f-secure.com/v-descs/nimda.shtml.

Malware can carry multiple payloads including viruses, worms, Trojan horses, and keyloggers. The advantage from the malware developers' perspective is that if only one countermeasure is in place to block the effects of one threat, the other threats may still succeed. This is similar to the rationale for using multiple vectors; if one fails, another might succeed. For this reason, it is imperative that IT security professionals adopt a layered, multifaceted approach to systems security. No single method, even if it is 100 percent effective against a threat, will protect systems subject to multi-vector, blended threats. Defenses must be at least as sophisticated as the threats.

Blended threats have been around for several years. The attack-with-breadth approach can be countered using techniques described in the next section. So how are malware developers responding? What is the next step in the evolution of malware? There are probably several techniques and methods that will emerge, but one broad pattern is the use of targeted malware.

Consider the rapidly growing number of phishing keyloggers, for example, which track specific actions and sites to gain information. The Anti-Phishing Working Group found the number of such reported programs has grown from 260 in April 2005 to 2683 in April 2006. Like spear phishing, which is a more targeted variation of phishing, malware has become more precise in its focus. The most troubling indication of this trend is reported by the research group Compute Economics:

> The bad news is that the nature of malware (viruses, worms, Trojans, spyware, adware, and other malicious code) is changing from overt threats targeting operating system vulnerabilities and users generally, to more focused, covert attacks targeting specific companies or business sectors (Source: Computer Economics, "2005 Malware Report: Executive Summary" at http://www.computereconomics.com/article.cfm?id=1090).

Targeted attacks are likely to continue to grow in sophistication as the motives for malware development shift from vandalism and desire to demonstrate one's technical prowess to economic drivers. What worked for Willie Sutton, the famed bank robber who said he robbed banks "because that's where the money is" works today for cybercriminals.

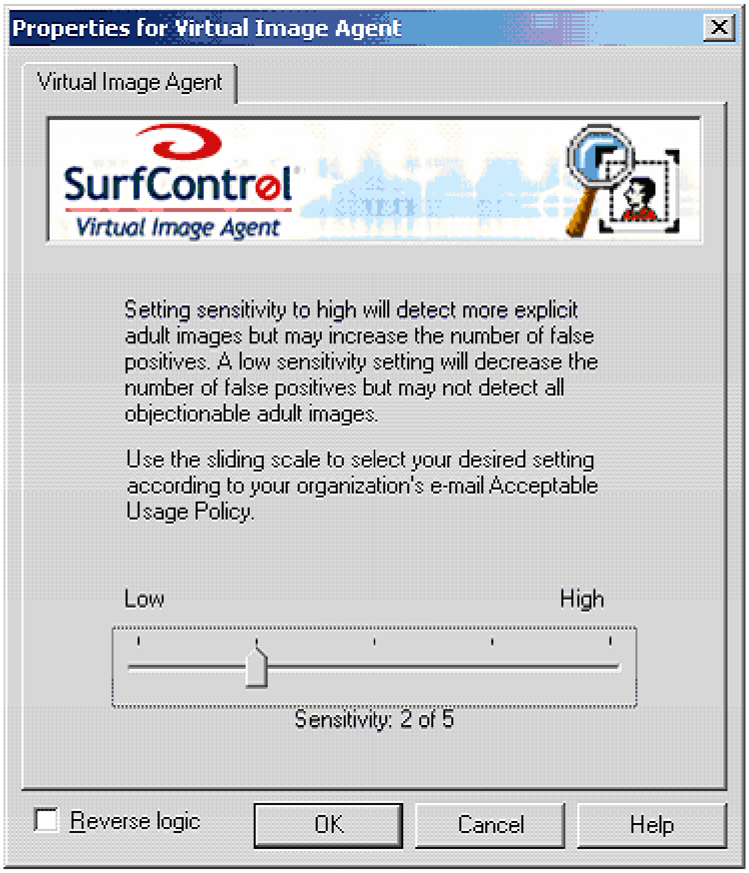
Increasingly Sophisticated Countermeasures

The purpose of this chapter is not to instill fear, uncertainty, and dread among readers and certainly not to paint a picture so drastic that you succumb to a fatalistic sense of inevitable loss. At the same time, security problems are growing and it's time for us as IT practitioners to deploy and manage *all* the countermeasures necessary to protect our organizations. The following list highlights guidelines (which will be developed further in later chapters):

- Use multipoint countermeasures
- Use multiple technologies to counter threats
- Use real-time threat information
- Define and implement a vulnerability scanning policy
- Define and implement a patch management policy
- Define organization-level information security policy

Do not depend on a single point solution to counter a threat (see Figure 2.5). For example, network firewalls do not protect laptops when they are not connected to the network. Deploy personal firewalls and configure appropriately. Similarly, network-based content filtering can detect and dispatch spam, viruses, and other malware only when the traffic is routed through the network. Mobile devices may use several networks with varying levels of protection. Security should be deployed at the network as well as the device levels whenever practical.

We have seen that signature-based detection will not always identify polymorphic and metamorphic viruses; for those, behavior-based detection is required. In the case of content filtering, keyword scanning can identify offensive language but does not help control inappropriate images sent across the network. New image scanning technologies can be configured to control problematic images to the degree appropriate for a particular organization.



Setting sensitivity to high will detect more explicit adult images but may increase the number of false positives. A low sensitivity setting will decrease the number of false positives but may not detect all objectionable adult images.

Use the sliding scale to select your desired setting according to your organization's e-mail Acceptable Usage Policy.

Sensitivity: 2 of 5

☐ Reverse logic

Figure 2.5: Multiple technologies, such as text and image filtering programs, should be used to counter the full range of threats facing business Internet use.

Threats can move quickly. Malware, such as SQL Slammer, Code Red, and Nimda, can exploit vulnerabilities in widely deployed systems and spread faster than countermeasures can be deployed. Countermeasures must be in place before an attack to be of significant value. Real-time databases of threats maintained by centralized organizations can consolidate information from multiple sources and distribute it to subscribers. For example, sites with content that is banned from an organization's network can close down and start up frequently. A centralized resource of information about such sites can provide a cost-effective means to keep up with changes.

One of the most important countermeasures an organization can deploy is a well-designed set of security policies. All the antivirus software, firewalls, IPSs, and content-filtering applications will not protect an organization if they are not deployed in a coordinated manner, maintained effectively, and monitored to ensure they are functioning in compliance with the needs of the organization.

Do not underestimate the importance of security policies. Developing them can be time consuming, but they are essential. Start with sample policies at the SANS Institute's Security Policy Project available at http://www.sans.org/resources/policies/.

The International Organization for Standardization (ISO) has developed a set of security best practices in the standard ISO-17799; information is available at http://www.iso-17799.com/, http://www.iso17799software.com/ and http://iso-17799.safemode.org/.

Summary

Business Internet use is subject to a wide range of threats that seem to be constantly evolving and adapting to both countermeasures as well as new opportunities. Despite these changes there are fundamental characteristics that do not change:

- Threats can emerge from both inside and outside an organization.
- No single countermeasure will protect an organization's information assets.
- A coordinated, policy driven response to organizational security is required.

Organizations that understand the dynamics of threats and respond appropriately will lower their risks; those that do not are essentially playing Russian roulette hoping their company or agency will not be struck by any of the myriad threats on the Internet.