PART I

SYMANTEC ANTIVIRUS

CHAPTER 2

Security Risks and Threats

Terms and Techniques to Remember

- Threats
- Security risks
- Blended threats
- Social engineering
- Denial of Service
- Impact caused by security risks and threats

Security Risks

When computers were large monolithic devices standing alone and loaded from verified software packs provided directly by commercial vendors, applications were validated before installation and only an administrator with proper permissions could add new programs. Today, always-on high-speed broadband connectivity is common, and even dial-up users are able to maintain a high degree of constant connectivity to the Internet. Users are beset by a constant stream of toolbar helpers, cursor animations, browser plug-ins, and other types of software they are prompted to install.

The term *malware* (short for "malicious software") has been commonly used to refer to the traditional threats posed by viruses, Trojan horses, and worms. Over the

last few years, the risks introduced by a number of other types of programs, including spyware and adware, have been steadily increasing. Spyware programs can spontaneously pop up advertisements, hijack browser sessions, redirect browsers to select target sites, or compile tracking information on user browsing habits. They can make use of a user's computer resources without his or her informed consent, or even log a user's keystrokes and form data—including sensitive data such as credit card and personal information that might then be used for identity theft or other illegal actions.

Makers of these programs often package their wares in a bundle with other packages the user wants, such as in the case of Kazaa, a peer-to-peer file-sharing application. Packaged within Kazaa, users unknowingly agreed to allow Brilliant Digital Entertainment to make use of "unused" computer capacity when they selected to accept the very lengthy terms of service required to download and install Kazaa. Without realizing what they had done, these users had given an unknown company the right and ability to make use of their computer's storage, CPU, memory, and network connectivity as this clandestine agency saw fit.

Although Symantec and other security providers have identified thousands of different security risks, most fall into a few general categories of operation. These can impact the performance or security of an infected host, posing an ever-expanding threat that must be addressed if a user is to maintain an acceptable level of operational capacity.

Symantec recognizes a number of different types of security risks present in the modern network environment. Although some of these risks are present only when a computer is actively connected to a network, it is important to remember that other vectors can be used to transfer security risks of many types. Technologies such as flash drives, floppy disks, portable hard drives, CD-ROM and DVD optical media, and wireless connectivity provide avenues for the introduction of undesirable software onto unprotected computers.

Spyware

Spyware is software that has the capability to scan computers or monitor activity and relay information to other computers or locations in cyberspace. Among the information that can be actively or passively gathered and

disseminated by spyware are passwords, log-in details, account numbers, personal information, and individual files or other personal documents. Spyware can also gather and distribute information related to the user's computer, applications running on the computer, and Internet browser usage or other computing habits.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a computer known to the user. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user might unknowingly receive and/or trigger spyware by accepting an End User License Agreement from a software program linked to the spyware or from visiting a Web site that downloads the spyware with or without an End User License Agreement.

A survey in late 2004 examined the prevalence of spyware on consumer PCs. This survey found that more than two-thirds of all computers surveyed had some form of spyware present, commonly with multiple forms or variants present on a single computer. The burgeoning growth of these risks has reached such proportions that the Electronic Privacy Information Center (EPIC) has listed the need for antispyware, antivirus, and firewall software as the no. 3 item on their "Top Ten Consumer Privacy Resolutions."

Adware

Adware is designed to deliver advertising content to a user, often mining the user's browsing habits to provide directed advertising of products or services the user is most likely to want. As a result of this practice, many users see this type of software as somewhat innocuous, without realizing that this information is being gathered and may be sent to other parties elsewhere without their consent. Spammers often buy lists compiled by such programs to target a flood of unsolicited email to the user's address.

Browser-hijacking adware programs can redirect a user's home page to a different site, intercept search engine, or browsing URLs, and redirect the user to alternate locations or otherwise attempt to control the user's Web browser client. Programs such as Xupiter and CoolWebSearch are examples of this type of adware.

Hack Tools

These are tools that a hacker or unauthorized user can use to attack, gain unauthorized access to, or perform identification or fingerprinting of your computer. Hack tools generally do the following:

- Attempt to gain information on or access hosts surreptitiously, utilizing methods that circumvent or bypass obvious security mechanisms inherent to the system they are installed on.
- Facilitate an attempt at disabling a target computer, preventing its normal use.
- Facilitate attacks on third-party computers as part of a direct or distributed Denial-of-Service attempt.

One example of a hack tool is a keystroke logger, a program that tracks and records individual keystrokes, and can send this information back to the hacker.

Joke Programs

Mostly harmless, these programs generally create distractions by causing animated characters to wander around a user's screen randomly or by interrupting normal operations to display a fake computer crash message. Such programs are typically benign but can cost a business a great deal of lost time trying to eliminate programs from infected hosts.

Dialers

Dialers are a form of risk that intercept connectivity requests to a user's normal ISP and instead dial on their own to connect a user to an alternate phone service. Often these numbers are long-distance calls, sometimes dialing numbers with exorbitant per-minute toll fees. Although decreasing in number due to the expansion of cable modem and DSL broadband connectivity, these programs can cost users money and effort, and can also endanger user information.

Remote Access

Remote access programs allow an unauthorized user or remote terminal to interact with a user's desktop or other devices connected to a running computer. Some of these programs relay the desktop to a remote viewing client so that the originator can observe exactly what the user sees. Others actually allow the originator to take over a user's console by entering keystrokes or moving the mouse as if the hacker were sitting at the compromised computer's console.

A few of these programs can be used to surreptitiously access a computer's attached devices, such as webcams and microphones, to better spy on users without alerting them to this behavior. Although there are a number of valid uses for remote access clients in the modern business environment, most of these programs hide their existence from the user and can present an extreme risk to users working with sensitive or protected information, trade secrets, or other similarly valued data.

Summary

Table 2-1 details some of the typical impacts caused by security risks.

Table 2-1

Typical Impacts Caused by Digital Infections

Impact	Risks
Performance	Computer slowdown. Computer instability.
	Active conduit for download and installation of additional security risks.
Privacy	Release of confidential, protected, or sensitive information.
	Release of browser-tracking information, logged keystrokes, or other forms of data.
	Violations of privacy policies or legal requirements.
Operation	Infections can allow programs to spread to other computers, mobile devices, or network file shares.
	Infections can lead to data loss, corruption, or other forms of operational impairment to infected hosts.
Liability	In additional to legal issues surrounding violations of privacy laws, owners of infected hosts might find themselves liable for harm or loss caused by their infected computer's actions.

Removal of infections can also cost time, personnel, and possible loss of critical data within an enterprise. Viruses, worms, and Trojan horses can add significantly to the total cost of ownership (TCO) of a company's network.

Threats

Unlike security risks, threats can be much more malicious and widely distributed. Based on the manner in which a threat spreads and how it acts after infecting a new host, it is referred to as a virus, worm, Trojan horse, or blended threat.

Viruses

A virus is a program or code that replicates itself onto other files with which it comes in contact; that is, a virus can infect another program, a boot sector, a partition sector, or a document that supports macros by inserting itself or attaching itself to that medium. Most viruses only replicate, although many can do damage to a computer or to the user's data as well. Unlike worms, which are discussed later in this chapter, viruses generally require human action to propagate.

Risks from Viruses

Symantec has identified more than 10,000 variations of viruses, with multiple new viruses added to this list every day. Some of these simply seek to spread copies; others can be used to weaken a computer's defenses against later attacks in a process referred to as softening the target. Other viruses have deleted files of a particular type on local and network-shared file stores, while some are programmed to lie in wait until a particular date or time and then enact a preprogrammed process, such as attacking antivirus Web sites in an effort to create a distributed Denial-of-Service of a Web site.

Viral Propagation

Just as a biological virus can find its way to a new host by air, contact, or water, digital viruses can be transmitted between hosts via a number of different

avenues, including removable storage, downloads, network file shares, wireless connectivity, and email.

Removable Storage

Early virus propagation occurred when a medium, such as a floppy disk, was loaded into an infected computer. The virus copied itself to this medium so that when the floppy was inserted into another host, the viral code executed and spread to this new computer. Common removable media exploited by viral code included floppy disks, Bernoulli cartridges, removable drive platters, and any other form of medium that could carry the infection between computers. Today removable optical media and the ubiquitous USB flash drives provide a convenient transport mechanism between unprotected computers.

Downloaded Information

With the advent of networked operating systems and the development of the global Internet, users can transfer data without requiring a physical medium of transport. Data downloaded from Web sites, electronic mail, and peer to peer file-sharing services such as BitTorrent or Kazaa all provide a conduit for potential viral transmission. Users who download cracked applications or illegally downloaded audio and video files commonly encounter viral programs masquerading as the desired file. Legitimate users might find themselves attacked by a newly released virus if they visit an infected Web site or otherwise download virus-laden data.

Network File Shares

In modern network scenarios, multiple users often share common file storage on a centralized file server. This allows mobile users to access their data from the central repository without requiring that they always log on from a particular client computer, while also allowing centralized management of backup/recovery and file-storage policies. Some viruses can replicate themselves to an available file, potentially corrupting key data or providing a vector for transmission to other users who might access infected files from a shared directory that has been compromised in this manner.

Wireless Connectivity

Viral programs are evolving into forms capable of being transmitted via wireless connectivity, including Bluetooth and WiFi wireless data connections. As mobile devices employ greater data-sharing capabilities and expanding computer resources, many devices and embedded control computers might become capable of being infected by viruses.

Windows and the World

Because of the dominance of the Microsoft Windows® operating systems, on computers around the world, virus writers have focused on this platform and its common applications. However, other operating systems are not without risk; for example, viruses are now being seen infecting mobile devices such as cell phones, personal digital assistants (PDAs), and other mobile devices. Like their server and desktop-computing counterparts, these devices can also be vulnerable to viruses and other forms of threats.

BRAIN

One of the earliest documented computer viruses to strike systems "in the wild" was the BRAIN virus, which originated in Pakistan in 1986. The BRAIN virus is a boot-sector infector that spreads through infected magnetic media. When the computer starts, it reads the infected boot sector and loads itself into memory.

A nasty twist implemented by BRAIN is its stealth capabilities. BRAIN watches for attempts by user programs (such as antivirus systems) to read the boot sector and intercepts them. It feeds back a copy of an uninfected boot sector, making detection difficult.

PCs Are Not Alone

In July 2004, proof-of-concept threats were identified that were targeted at the Symbian operating system used by many mobile devices, including

personal digital assistants (PDAs), cell phones, vending machines, environmental controls, and many other forms of wirelessly connected electronics. Some of these threats were capable of taking advantage of the Bluetooth connectivity built into mobile devices to spread to nearby devices configured for Bluetooth access. Symantec lists 31 variations of SymbOS-based threats at the time of this text's writing.

As with biological viral infections, a digitally infected mobile device can potentially spread to other susceptible devices that passed close by—much like having a co-worker with the flu come to the office and share his or her biological virus with those who come too close. This is not limited to cell phones, laptops, and PDAs alone. *SC Magazine* recently detailed the potential for viral infection of the onboard computers on some late-model automobiles.

With the capability to infect other devices without direct contact, the potential for rapid viral propagation between automobiles and other devices becomes a very complex issue. Users passing through a crowd, walking past parked cars, or walking near other wireless devices in their office or home could find their personal devices infected simply by their proximity.

Executable Files

By attaching itself to an executable file, viral code can be executed by the operating system when the executable file is run. Some viruses are capable of renaming common executable files and duplicating themselves in place of the replaced application so that when a user attempts to open a common application such as notepad.exe, the virus executes in its place. A few of these viruses can attempt to hide their existence by also executing the renamed program the user sought after they have completed their own operation.

Kernel Attacks

In addition to normal executable files, the core executable component of the operating system, termed the *kernel*, can also be targeted by a virus.

File Attachments

With the growing use of email for personal and professional uses, file attachments have become a common means of viral transmission. Many viruses arrive in a user's inbox pretending to be from a known source, offering some type of information of interest to the target. Little does the user know, when he or she launches the attached file, a virus and is activated.

Macro Viruses

Within some applications, such as the Microsoft Office Suite of products, users can record macros, allowing a set of common tasks to be executed. Macro viruses append themselves to common file types, such as document (.doc) or spreadsheet (.xls) files, and execute their payload when an infected document is opened by the application or some other program capable of executing embedded macro code.

Direct Infection

Some viruses directly damage files by replacing the original file with a copy of the virus named the same as the deleted file, or by embedding their code within an existing file by discarding the original file contents beyond the file's header segment. Other viruses can attach their code to the beginning or end of existing files, to conceal the infection more effectively. Many viruses hide copies of their code within the System Restore on Windows XP computers, requiring that a user disable this feature to be able to remove the infection. Others write keys into the Registry that must be removed to clean out the viral code.

Boot-Sector Viruses

Boot-sector viruses directly infect the first sector of a computer's hard drive. When a computer is first powered on, its built-in programming is capable of performing only simple Power-On Self-Test (POST) operations and then accessing the first sector on the configured boot device (typically a hard drive). Code loaded from this boot sector directs the computer through

additional steps necessary to load software drivers and the operating system itself.

Worms

A worm is a program that makes and facilitates the distribution of copies of itself—for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm can do damage and compromise the security of the computer. It can arrive via exploitation of computer vulnerability or when a user clicks on an infected email.

The World's First Worm

The very first worm to terrorize the Internet occurred long before the word *Internet* became a household term. On November 2, 1988, a strange affliction struck the young Internet. Systems around the network suddenly began acting strangely, and network traffic grew at an exponential pace.

Internet experts quickly discovered that a new type of malicious code was spreading. This "worm" was infecting entire networks and quickly winding its way throughout the fledgling Internet.

Security officials responded quickly (at least, by 1988 standards) to dissect the worm and determine the methods by which it was spreading. Experts throughout government and academia (the two major players on the Internet in those days) convened a conference at the National Computer Security Center in Baltimore and developed a response plan.

Six days later, on November 8, the worm was declared eradicated. Authorities tracked down the worm's author, Robert Tappan Morris, a graduate student in computer science at Cornell University who claimed that the worm was an academic experiment gone wild. The courts didn't believe his claim and, after he was found guilty, sentenced him to a fine and community service under a felony violation of the Computer Fraud and Abuse Act.

Vulnerabilities

Worms have been developed to attack vulnerabilities in operating systems, services and daemons. Worms such as the Morris Worm (one of the first in-the-wild worm programs that impacted overall network performance, released in the late 1980s) spread through UNIX® and VAX™ computers that shared a common vulnerability, allowing execution of code through improperly secured debugging routines and other vulnerabilities.

Rate of Propagation

Unlike viruses, the automatic replication of worms can allow even seemingly benign worms to congest networks and impair recovery procedures. Although the Nachi worm downloaded an update from Microsoft to patch the very vulnerability it exploited, the worm generated considerable traffic and impacted network performance even for users who had already installed the patch on their own computers.

In March 2004, the Witty worm set a new record for the speed at which a discovered vulnerability has been used to generate a live worm program, a record that stands at the time of this text's writing. Less than two days after the initial advisory announcing a newly discovered vulnerability, the Witty worm was released to take advantage of the vulnerability before the operating computer vendor could develop and distribute a patch for this newly discovered security weakness.

Zero-Day

Many analysts predict that some type of "zero-day" threat will soon be developed, taking advantage of a totally unknown vulnerability to gain almost universal distribution across all unprotected computers on the Internet before developers have an opportunity to begin fashioning a countering patch or hot fix. Without antivirus protection, users would be faced with the decision to shut down their infected computer until a patch could be developed or to risk whatever threat the worm produced. Symantec AntiVirus™ and Symantec™ Client Security can aid in defending against many of the potential avenues that might be exploited if such a zero-day threat were ever to emerge by providing proactive defenses for vulnerable computers.

The popularity of the Microsoft Windows operating system has been suggested as one factor contributing to the incredible rate of propagation experienced by recent worm releases. However, the implementation of complex worms capable of spreading through many different vectors provides a strong indication that even if there were two or three equally dominant platforms sharing the market, worm authors would simply target vulnerabilities present in multiple platforms and so gain near the same distribution levels.

Trojan Horses

A Trojan horse portrays itself as something other than what it is at the point of execution. Although it might advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. A Trojan horse must be sent by someone or carried by another program, and can arrive in the form of a joke program or software of some sort. The malicious functionality of a Trojan horse is anything undesirable for a computer user, including data destruction or the compromise of a computer by providing a means for another attacker to gain access, bypassing normal access controls. Like spyware discussed earlier in this chapter, Trojan horses might offer interesting new games, desktop themes, or all manner of other enticements to a user, to get the user to install the Trojan package.

Once installed, a Trojan horse typically provides some type of apparent functionality to the user, while performing many other tasks behind the scenes, leaving the user unaware. Trojan horse programs often communicate with their creator through Internet Relay Chat (IRC) communications, allowing the creator to modify these programs once installed and even to publish updates that can be applied automatically by the program itself. Table 2-2 lists a few of the more common security risks posed by Trojan horse infections.

A subtype of the Trojan horse is the "back door," which refers to a programmatically created mechanism for bypassing normal security measures in accessing resources on the vulnerable computer. Occasionally, programmers put into place various hidden shortcuts in their code, designed to ease the

Table 2-2

Common Risks Carried by Trojan Horses

Risk	Examples
Remote access	Services can be enabled or ports can be opened.
	Remote-control utilities can be installed, allowing control of the computer's console.
Monitoring	Console duplication can allow shoulder-surfing by remote operators.
	Keystrokes, URL history, and other data can be collected and relayed to the creator.
Data relay	Unauthorized file-sharing services can be implemented, allowing the creator to distribute contraband data through the compromised host.
	Spam relay programs can be implemented, allowing the creator to hide the origin of spam messages.
Softening	Trojan horse programs can replace common applications on the host computer, creating vulnerabilities and softening the host's defenses.
	Trojan horse programs can also be used to coordinate mass network-scanning or network attack efforts, making it harder to detect the profiling scan or attack coming from tens of thousands of separate computers controlled by the creator of the program.

process of development or testing. Attackers might utilize one or more security risks to plant their own back-door program somewhere within the network.

Back doors are implanted by the attacker to allow later access to a computer. Remote-access tools can provide an attacker with a back door or allow the attacker to obtain sufficient information to bypass normal authentication measures using key-logged information. Back doors are particularly troublesome for network administrators responsible for tracking down the party responsible for network misuse.

Blended Threats

Blended threats combine the characteristics of viruses, worms, and Trojan horses with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats

can rapidly spread and cause widespread damage. Characteristics of blended threats include the following:

- **Causes harm**—Launches a Denial-of-Service (DoS) attack at a target IP address, defaces Web servers, or plants Trojan horse programs for later execution.
- **Propagates by multiple methods**—Scans for vulnerabilities to compromise a computer, such as embedding code in HTML files on a server, infecting visitors to a compromised Web site, or sending unauthorized email from compromised servers with a worm attachment.
- **Attacks from multiple points**—Injects malicious code into the .exe files on a computer, raises the privilege level of the guest account, creates world-read and writeable network shares, makes numerous Registry changes, and adds script code into HTML files.
- **Spreads without human intervention**—Continuously scans the Internet for vulnerable servers to attack.
- **Exploits vulnerabilities**—Takes advantage of known vulnerabilities, such as buffer overflows, HTTP input-validation vulnerabilities, and known default passwords to gain unauthorized administrative access.

Effective protection from blended threats requires a comprehensive security solution that contains multiple layers of defense and response mechanisms.

Blended threats such as Code Red spread by exploiting services running on vulnerable computers, which in Code Red's case was the Miscrosoft IIS service's HTTP implementation. Code Red took advantage of a flaw in the initial coding that allowed the arbitrary execution of code on the server hosting the IIS service. Others spread by taking advantage of vulnerabilities discovered in various services, such as the Windows DCOM Remote Procedure Call (RPC) vulnerability exploited by Blaster, or through code injection and buffer overflows, such as those generated by malformed UDP datagrams exploited by the SQL Slammer worm. Nimda and its variations made use of multiple vectors for transmission in a single package by spreading through vulnerable file shares and buffer overflows, or by sending itself as an email attachment.

Note
As an item of interest, Nimda is believed to be named because it spells *Admin* backward. Code Red gained its name from the caffeinated soda product popular at the time.

Blended threats are becoming increasingly sophisticated, allowing viruses, worms, and Trojan horses to spread through any of a number of different mechanisms, in case a vulnerable computer's defenses are only partially in place. This multifaceted attack strategy requires administrators to plan their network defense carefully, to contain multiple layers of defense and response mechanisms implemented at the client, server, and the gateway.

Proliferation of Viruses, Worms, and Trojan Horses

With dozens of new variations of viruses being released daily, one might ask who is developing so many sophisticated programs. Although the first exploits to take advantage of a newly discovered vulnerability are generally released by highly skilled programmers, the creation of viruses and worms requires no more skill than any other point-and-click GUI to create a seemingly infinite stream of new customized viral programs. Hundreds of ready-made GUI and command-line virus generators can be downloaded from the Internet, with names such as Acid Flowing Trojan Generator or the Batch-O-Matic.

By selecting options on a GUI, such as shown in Figure 2-1, a hacker might elect for his or her new creation to spread by one or many different means, using customized file names, polymorphic restructuring capabilities, and many other details that can make the newly generated program unique in its methods of attack and distribution. Because researchers also use these tools, they remain legal in most countries and are easily accessible through a simple Web search. The danger inherent in these tools is that, through their use, relatively unskilled hackers could generate continuous streams of new threats.

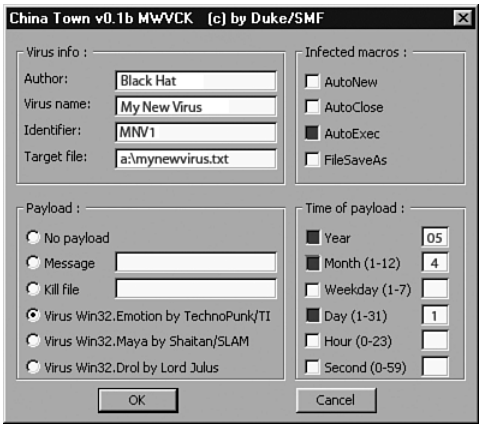

Figure 2-1 An example virus-generating GUI tool, configuring a virus called My New Virus to deliver a payload that will act on April Fools' Day 2005.

Polymorphism

Polymorphism is the capability of a program to generate offspring copies that differ from the parent because of a mutated ordering of operations or functionality within the code. Viruses, worms, and Trojan horses that implement polymorphism are more difficult to identify because of the continual mutation in each generation.

Common Attack Strategies

Attackers targeting a network can leverage combinations of the various security risks and threats to enact their nefarious plans for vulnerable computers. The least sophisticated attacks might corrupt or delete data, potentially requiring a complete reformatting and reload for infected computers. More sophisticated attacks can produce even less desirable results, including placing illegal content on targeted computers, exposing protected data, or even utilizing the compromised computers to levy attacks against secondary targets.

Social Engineering

Many hackers make use of the practice of social engineering, which is a psychological scam intended to get users to reveal information or to provide details useful for a successful network attack. Email-borne viruses employ this technique by presenting an innocuously named viral attachment with a From email address matching that of a known associate. Spyware and other security risks can provide attackers with information that can be used to improve social-engineering efforts, such as by allowing a phishing attack to mimic a site the user is known to frequent.

Bots and Botnets

Botnet is a term used by the FBI to describe a group of compromised hosts controlled by a remote attacker, as illustrated in Figure 2-2. Communicating with their creator through Internet Relay Chat (IRC) or other anonymous methods of communication, compromised computers can reside quietly for a lengthy time until given a command to attack a chosen target. These networks can also be used to crack encryption keys and other CPU-demanding tasks, distributing a huge task among tens of thousands of personal computers located around the globe.

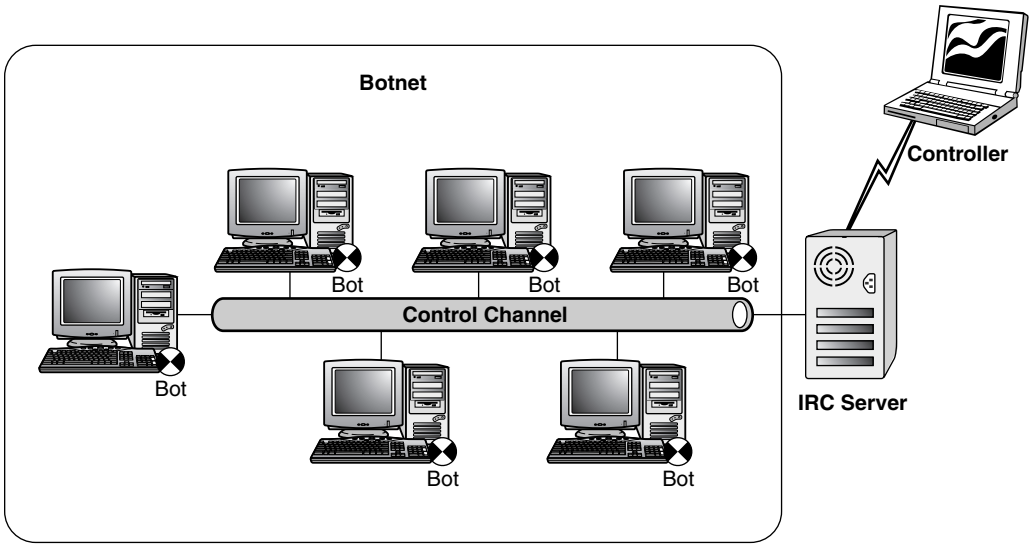

Figure 2-2 An idealized example of an IRC-controlled botnet.

Sometimes referred to as zombies compromised computers (bots) are often traded as coin of the realm among hackers seeking access within a particular network. Large botnets are status symbols among some groups, where their originators might fight silent wars against one another using corporate, educational, personal, and even governmental hosts as their playing pieces. Compromised bots in secure networks, such as .gov and .mil sites, can often be traded for thousands of compromised .edu and .com hosts, all traded by the controlling hacker to purchase status, bragging rights, or access to target networks. These transactions occur while the true owners remain unaware that the compromised computers are being bought, sold, and used as a weapon against other networks.

Beyond their value as currency among the various hacker communities, botnets are commonly used in various malicious ways:

- **Distributed–Denial-of-Service attacks**—The most common use of botnets is the massed coordinated attack against a target site or address to saturate the target's bandwidth or capability to respond to legitimate connections. These attacks have been levied against high-profile sites through the use of thousands of compromised bots scattered around the world. The distributed nature of these attacks makes it more difficult for the target to filter out only the undesirable traffic.
- **Remote control**—Bots provide their controller some measure of control over the compromised computer, allowing the introduction of malicious programs, back doors, spyware, or any of the other security risks previously discussed.
- **File sharing**—Botnets are sometimes used to host contraband files, cracked software titles, audio files, and even entire DVDs that have been ripped and stored on compromised computers with high-bandwidth broadband connections. By replacing valid services on compromised hosts, these bot programs can be configured to serve as HTTP or FTP servers that might appear valid to a cursory audit of the network.

Compromised computers in highly secure or limited-access areas are highly valued by controllers of these botnets, along with computers with high levels of connectivity and large storage capacity. Because of this, commercial targets are commonly identified for attack to compromise servers and other

well-connected computers. Educational sites are also commonly targeted because they are generally comprised of large numbers of relatively new computers installed in default configurations, connected to wide-bandwidth Internet backbones, and supported by limited numbers of staff that take publicly posted holidays.

Root Kits

Extending the qualities of a Trojan horse or a back door, root kits replace or modify elements of the operating system to provide an attacker greater control over compromised hosts. These programs can replace or modify the system kernel, system binaries, or other elements of the host's operating system, often allowing an attacker's later efforts to pass unnoticed, provided with stealth and cover by the modified system binaries.

Implementations of root kits can replace common user interface functions, allowing an attacker to conceal their implanted services from the Task Manager or to hide files from the explorer interface when a user attempts to check for unexpected files that might reveal the compromise. Root kits can be used to implant a known master password or other mechanism for bypassing the normal protections of the host computer.

Root kits provide the greatest level of control over a compromised host because they target directly the basis for all other applications running on a computer. Attackers who can successfully deploy a root kit can be considered to "own" the compromised computer at a functional level to such an extent that only a full reformat-and-reload can be certain to remove the damage done. Protection strategies are vital to protect against this level of compromise, where backup and recovery strategies might provide the only path back to a functional network environment.

Impact of Security Risks and Threats

Viruses, worms, and Trojan horses can corrupt data on a user's computer, infect other computers, weaken computer security, or provide back doors into protected networked computers. Although seemingly less dangerous than

viruses that can corrupt digital content on a user's computer, spyware, adware, and other forms of security risk also represent a significant problem to small businesses, their users, and the company networks. All types of threat and security risk can seriously impair business operations, network use, and computer performance while performing many tasks unknown to the user of an infected computer. Some of the areas of impact are discussed here.

Capacity

All software operating on a computer consumes a portion of the host computer's resources, whether its hard drive storage, CPU processing power, computer memory, or network bandwidth. Any threat or security risk resident on a computer can seriously impair the performance. They add to the load placed by normal use by consuming additional memory, processor or network resources as they perform their task, monitoring keystrokes, searching for private information, and possibly sending that data to a central location. In addition to this, the threat could be a virus or worm attempting to propagate or launch an attack against another computer or network

Your Computer Held Captive

It is easy to see how each small package can combine with others to quickly overwhelm a computer, much like Gulliver found himself bound by the many tiny strands woven by the miniscule Lilliputians in the classic tale *The Travels of Gulliver.* Each individual software package might consume only a tiny fraction of a computer's capacity, but when taken together in large numbers, these packages can rapidly overwhelm normal operations.

Time

In addition to time lost because of operational slowdown caused by the weight of a computer's parasitic population, computer users could lose time clicking to close the endless stream of advertisements that suddenly appear, or while attempting to navigate back through a redirected session to find meaningful Web content. Administrative staff are also overburdened

responding to user issues stemming from the security risks and threats prevalent on computers.

Undesirable Content

A myriad of pop-up advertisements and browser redirection by various security risks often expose users to undesirable content, notably graphic images inappropriate in the workplaces. Distracting materials or contraband images can, at best, be an impediment to a user's focus on work and can, at worst, present legal liabilities for the organization.

Unexpected Hazards

In one instance, an investigation of a user's computer brought about by complaints filed by a co-worker who claimed a hostile workplace environment was being created by the user's pornographic screen saver. Unknown to the user, acceptance of a bundled desktop themes package had also included installation of a spyware program that presented advertising images as a changing screen saver—often advertising materials of a decidedly mature theme.

Data Harvesting

Data-harvesting is particularly troubling within the modern corporate setting because many different legal requirements exist to mandate protection of client information in a number of different industry settings. As mentioned earlier, legislative requirements in the U.S. include the Children's Online Privacy Protection Acts (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Educational Rights Protection Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and a wide assortment of other privacy and information-control laws. Violations of these provisions, even when inadvertently caused by spyware data harvesting, can carry heavy penalties for both individual users and their companies' owners and board members.

Users must also be concerned about data-harvesting programs when their own private information is being distributed without their knowledge;

such data can be used in a number of different scams to drain users' bank accounts, make use of their credit, or enact identity-theft crimes. These are merely some of the threats posed by data-harvesting programs that might have meaning to the user and their employer. Businesses conducting research, operating under protected network mandates, or involved in protecting trade secrets or other valuable information might find that unexpected spyware programs are busily transferring sensitive data elsewhere beyond their control.

Computer Security

Security risks such as spyware can perform any number of actions without the user's knowledge once installed, with or without the knowledge of the user. Because of this, these programs can cause almost any type of security breach. Coupled with viral threats, automated computer-profiling utilities, and many other tools employed by hackers, a seemingly innocuous game, screen saver, animated cursor, or toolbar could open the door wide to any type of mischief desired by the software's author.

Instability

Instability of computer systems infected by security risks and threats could be an intentional effect desired by the program's author, in the case of a malicious program, or a side effect of these unwanted applications competing for similar resources, along with the fact that they are often not well written or tested as with most commercial software. In addition to these difficulties, spyware can compromise computer operations through hijacking and browser redirection or when replacing normal components of the operating system.

Business Issues

IT staff are faced with increasing pressures to comply with regulations, increase the mobility of their workforce, provide access to the extended workforce, and increase the breadth of their value and supply chains, as well as prevent the latest Internet attacks from wreaking havoc on the infrastructure.

At the same time, they must maintain service-level agreements, keep executives out of jail, and keep hackers from preying on end users utilizing the network.

Many companies today live with a false sense of security. They believe that perimeter security alone is sufficient to keep unwanted intruders from the spread of security risks and threats. To the contrary, it is too easy for these to enter a company network and never touch perimeter security. For example, imagine that a mobile user takes a laptop to work at home. While at home, the user connects to a local ISP and accesses infected Web sites or downloads personal email with infected attachments. The user then reconnects to the corporate network the next day and launches an infected attachment from a local email download. Another example is the remote user who uses a VPN to access corporate resources. The remote user accesses a local ISP before initiating the VPN client. It is very easy for the user to access an infected Web site or download infected personal email. When a VPN tunnel is established, the client is essentially behind the corporate perimeter. The threat infestation can be sitting in memory and immediately take advantage of open file shares and Web server vulnerabilities to spread its payload.

To stay protected from the increasing number of methods and techniques that security risks and threats are utilizing, it is apparent that a "defense-in-depth" approach is required, creating multiple layers of protection around your computers and valuable data. Such an exhaustive approach is required because there are new and innovative types of security risks and threats, some of them using multiple methods and techniques to propagate themselves. It is now necessary to protect all endpoints with comprehensive security that prevents intrusions from either entering or spreading from client machines. Providing this level of protection on the client requires three crucial technologies:

- Antivirus software, to protect against known security risks and threats
- A client firewall, to block suspicious incoming and outgoing network traffic
- Intrusion detection and prevention, to identify and block known and unknown Internet intrusions such as those that are used in Denial-of-Service attacks (DoS)

Symantec documented more than 1,400 new vulnerabilities between July and December 2004. In addition to all the new vulnerabilities appearing, significant risks are still posed by old attacks. In the same 6 month period, the most common attack is one that emerged in January 2003, the Microsoft SQL Server Overflow Attack. This was used by 22% of all attackers. This highlights the need for an integrated approach to blended threats: inspect traffic before it gets on the computer.

Symantec Client Security plays a critical role in allowing customers to adopt this holistic and proactive security paradigm. Symantec has long tracked the evolution of security threats and has prominently exposed the rise in sheer number of threats. What is also evolving is the nature and type of threats. Today we see network-based threats that are designed to take advantage of widespread vulnerabilities, to compromise as many computers as possible in the least amount of time.

Targeted attacks, phishing, and spyware have become the spam of 2004. These attacks use multiple attack vectors that exploit unannounced vulnerabilities, phishing attacks, and insider threats. These attacks are motivated by extortions, information theft, and organized crime. Payloads are for the purpose of theft, data export, and destruction. Social engineering will continue to illustrate the ongoing need for end-user education.

What's To Be Done?

At first glance, it might seem that the only way to avoid the security risks and threats prevalent in today's interconnected world is to avoid using the Internet, to never download any content, and to never read active-content email messages. However, this is not practical in the business world. A number of steps should be taken to reduce the risks to an organization:

- **Install detection and protection software**—With the number of security risks and threats constantly expanding, all computers should have software installed to provide real-time detection and protection against identified security risks and threats.

Symantec Client Security
Symantec Client Security helps keep client systems safe by providing comprehensive and proactive protection against blended threats, spyware, unauthorized network access, and mass-mailer attacks, with vulnerability-based detection.

- **Perform regular software maintenance**—Regularly review and apply new updates, service packs, and hot fixes to the applications and operating system on computers to provide the best possible protection.
- **Secure browser settings**—Ensure that Web browser security settings are set to the highest level that still allows proper operation.

Tip
Corporate administrators who oversecure browsers, blocking highly desired functionality, might find that users work to actively circumvent these protections and so weaken security overall.

- **Educate Users**—Ensure end users are aware of the dangers of downloading content from unknown sources and opening attachments from unknown Senders. Inform staff to carefully read all "terms of service" agreements, and never select buttons on pop-up.

Note
Users should also be wary of anything offered for free, whether it is a game, a funny desktop theme, a file-sharing application, or a toolbar promising faster downloading. As a very old cautionary saying goes, "Anything that seems too good to be true will be."

Detection

Because of the huge number of threat and security risk variations that exist, detection of new infections must be performed in many different ways. Table 2-3 lists a few of the most common methods of identification used by Symantec AntiVirus and Symantec Client Security.

Table 2-3

Detecting Security Risks and Threats

Method of Detection	Detects This Type of Threat
Auto-Protect	Auto-Protect is your best defense against security risks and threats. Whenever you access, copy, save, move, or open a file, Auto-Protect scans the file to ensure that a virus has not attached itself. Auto-Protect includes SmartScan, which scans a group of file extensions that contain executable code and all .exe and .doc files. SmartScan can determine a file's type even when a virus changes the file's extension. For example, it scans .doc files even when a virus changes the file extension to one that is different from the file extensions that SmartScan has been configured to scan.
Memory scan	Viruses, worms, and Trojan horses copy themselves into a computer's random-access memory (RAM), where they can reside and copy themselves onto other forms of storage media or across network file shares to other vulnerable computers.
Boot sector scan	Boot-sector viruses hide on a medium's master boot record or within its partition tables.
Floppy drive scan	Removable media, such as floppy disks, CD-ROMs, and flash drives, can harbor viruses, worms, or Trojan horse programs. Before the computer is allowed to access files on removable media, the media is scanned for software threats.
File scan	Infected files can be identified by comparing each file present on a computer against a definitions file that contains the signatures of all known threats and security risks.
Archive scan	Viruses, worms, and Trojan horse programs can hide within compressed file stores such as .zip, .arj, .lzh, .rar, and .exe self-extracting archives. By scanning each compressed file within these archives, infected files can be identified in the same manner as other forms of file scanning.
Heuristics	Symantec's Bloodhound engine provides a heuristic analysis to detect unknown threats by analyzing program structure, behavior, and other attributes. This allows newly emergent threats to be detected by observing their behavior where no signature exists. Heuristic analysis also protects against polymorphic threats, which can reconfigure the internal architecture between iterations.

Virus definitions files should be updated regularly to enable identification of newly emergent threats and security risks.

Responding to Detected Threats

Symantec AntiVirus and Symantec Client Security perform various types of scanning to detect known patterns identifying security risks and threats in much the same way that biological infections are detected within the human body. To follow the biological analogy, antivirus programs act to provide a computer with a form of digital immune system, one that rapidly adapts to protect against new threats.

The Definitions File

Signatures of known threats and security risks are maintained in a set of files known as the virus definitions files. These files contain signatures that are used to identify infections, although the definitions file does not contain live viral code and so does not pose a threat to the host computer's operation. Automatic updates to these definitions can be delivered to client computers from their parent server in the managed environment or directly from Symantec LiveUpdate.

Symantec AntiVirus and Symantec Client Security respond to files that are infected by threats or security risks with a first action and a second action. By default, when a virus is detected by Auto-Protect or during a scan, an attempt is made to clean the virus from the infected file. If the file cannot be cleaned, the second action is to log the failed cleaning attempt and move the infected file to quarantine so that the virus cannot spread, which denies you further access to the file. When a security risk is detected by Auto-Protect or during a scan, the infected file is quarantined and attempts are made to remove or repair the changes that the security risk has made on the computer. Quarantining the security risk ensures that it is no longer active on your computer and also ensures that Symantec AntiVirus or Symantec Client Security can reverse the changes, if necessary. If the first action cannot be done, the second action is to log the risk and leave it alone.

Outbreak Response

Handling threat and security risk outbreaks within the network requires planning and preparation beforehand to minimize the impact on network operations. The key to an effective response is the outbreak plan. Table 2-4 details an example outbreak plan.

Table 2-4

Example Outbreak Plan

Task	Description
Maintain current definitions	Ensure that antivirus definitions are regularly updated.
Map network topology	Prepare a network map to ease isolation and cleaning of infected computers. This map might include: ■ Subnet boundaries and gateways ■ Server names and IP addresses ■ Client names and IP addresses ■ Network protocols ■ Key service details (such as WINS, DNS, DHCP, and catalog servers) ■ Shared resources and network file shares
Document security solutions	Prepare a map of firewall, gateway, antivirus, and other security applications within the enterprise. This map might include: ■ Server-protection applications ■ Workstation-protection applications ■ Security appliances ■ Update mechanisms and schedules ■ Alternate update options if normal update methods are unavailable ■ Document logs available for outbreak tracking
Perform backup and recovery	Develop a backup plan and test-recovery practices regularly to ensure that backup and recovery operations function as expected, that backup media remains viable, and that staff responsible for recovery are experienced in the steps required for recovery.
Isolate infected computers	To protect the network from further compromise, it is important to have in place a policy for isolating infected computers from the enterprise network.

continues

Table 2-4 continued

Example Outbreak Plan	
Task	**Description**
Identify the threat	Identification of the threat responsible for the infection is critical to removal and recovery procedures. Security and antivirus logs can provide details about the threats found.
Respond to the threat	Removal and recovery procedures vary among different viruses, worms and Trojan horses. Details on known and newly emergent threats and security risks can be found at `http://securityresponse.symantec.com/`.

Conclusion

Internet connectivity, email and the web, now vital for small business, pose many risks to computer systems and the privacy of the company's data. The onslaught of viruses, worms, and Trojan horses, compounded with the increasing problem of spyware, adware, and blended threats continue to attack an organization's network through multiple methods.

Without effective network-defense and disaster-recovery practices a business is constantly at risk. Defense requires continually updated products such as Symantec AntiVirus or Symantec Client Security, and a well-defined outbreak-response plan to identify and deal with this ever-expanding problem. Symantec AntiVirus and Symantec Client Security provide an effective barrier against security risks and threats, facilitating their identification and removal, and protect sensitive and private company data. Without this protection, companies might find themselves faced with an administrative nightmare, including time consuming and costly full system reloads to recover lost data.

Chapter Review Questions

Question 2-1

Which of the following are types of security risks? Select all that apply.

- ❑ A. Adware
- ❑ B. Dialers
- ❑ C. Hack tools
- ❑ D. Joke programs
- ❑ E. Spyware

Question 2-2

Spyware can impact computer performance and security in which of the following ways? Select all that apply.

- ❑ A. Overwhelming computer capacity
- ❑ B. Wasting time
- ❑ C. Displaying graphic content
- ❑ D. Harvesting sensitive data
- ❑ E. Weakening computer security
- ❑ F. Causing programs to fail

Question 2-3

What are some of the ways that computers can be protected from threats and security risks? Select all that apply.

- ❑ A. Update software regularly
- ❑ B. Run unknown applications received via email
- ❑ C. Make use of a firewall application
- ❑ D. Make use of an antispyware application

Question 2-4

Which of the following best describes a virus? Select the best answer from those provided.

- ❍ A. A malicious program capable of spreading itself automatically
- ❍ B. A malicious program that makes use of many different vectors of transmission
- ❍ C. A malicious program that usually requires user interaction to spread
- ❍ D. An application that provides some form of desirable functionality while also performing other undesirable tasks hidden from the user

Question 2-5

Which type of virus can execute before an operating system is loaded? Select the best answer from those provided.

- ❍ A. Macro virus
- ❍ B. File virus
- ❍ C. Boot-sector virus
- ❍ D. Blended threat

Question 2-6

A blended threat is what type of program? Select the best answer from those provided.

- ❍ A. Both a virus and a worm
- ❍ B. A program that can change itself during replication
- ❍ C. A program that spreads using many different methods and techniques
- ❍ D. A program capable of targeting only a single operating system
- ❍ E. Both a virus and a Trojan horse

Question 2-7

Which of the following best describes a worm? Select the best answer from those provided.

- ❍ A. A program capable of spreading itself automatically
- ❍ B. A program that makes use of many different vectors of transmission
- ❍ C. A program that usually requires user interaction to spread
- ❍ D. A program that provides some form of desirable functionality while also performing other undesirable tasks hidden from the user

Question 2-8

Why do worms impact an organization much more than most viruses? Select the best answer from those provided.

- ❍ A. Worms can spread by many different means.
- ❍ B. Viruses automatically replicate themselves.
- ❍ C. Worms can relay data without the user's knowledge.
- ❍ D. Worms automatically replicate themselves.

Question 2-9

Which of the following best describes a Trojan horse? Select the best answer from those provided.

- ❍ A. A malicious program capable of spreading itself automatically
- ❍ B. A malicious program that makes use of many different vectors of transmission
- ❍ C. A malicious program that usually requires user interaction to spread
- ❍ D. An application that provides some form of desirable functionality while also performing other malicious tasks hidden from the user

Chapter Review Answers

Answer 2-1

Answers **A**, **B**, **C**, **D**, and **E**, are all correct. Common forms of security risks include adware, spyware, dialers, hack tools, and joke programs. In addition to these, browser cookies and applications pretending to be antispyware tools can pose risks to users.

Answer 2-2

Answers **A**, **B**, **C**, **D**, **E**, and **F** are all correct. Security risks can impact computer performance and security by consuming all available computer capacity

or causing computer instability that requires frequent reboot or application restart actions. They can also waste user time through both distraction and removal requirements, or can display undesirable content such as graphic images. Security risks can threaten user privacy and security by harvesting sensitive data, profiling a user's computer for exploitable vulnerabilities, or directly impairing normal security procedures.

Answer 2-3

Answers **A**, **C**, and **D** are correct. Best practices recommended to reduce risks include regular software updates, secure browser settings, careful browsing, and the use of antivirus, antispyware, and client firewall applications such as those provided in Symantec Client Security. Running unknown applications received via email is never recommended, as this is a common way to be infected by security risks and threats.

Answer 2-4

Answer **C** is correct. A virus is a malicious program that requires user interaction or some other form of enacting process to infect a computer and spread.

Answer 2-5

Answer **C** is correct. A boot-sector virus can execute before an operating system is loaded, making later removal more troublesome than many other types of infection. Early detection before infection is highly desirable in all cases, but nowhere more so than with boot-sector infections.

Answer 2-6

Answer **C** is correct. Blended threats combine the characteristics of viruses, worms, Trojan horses with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage.

Answer 2-7

Answer **A** is correct. A worm is a program that is capable of spreading without relying on user interaction. Because of this behavior, worms can spread to all network-connected vulnerable computers in a very short period of time.

Answer 2-8

Answer **D** is correct. Worms can impact an enterprise much more than most viruses because worms can self-propagate to all vulnerable computers. This allows a much wider distribution of newly released worms, which can also saturate a network's connectivity by attempting to spread to all available target addresses.

Answer 2-9

Answer **D** is correct. A Trojan horse is best described as an application that provides some type of desirable functionality while hiding other functions from the user.