Chapter 1

Much Ado about Malware

In This Chapter

- Posing and answering common questions about malware
- Understanding the types of malware (the enemy)
- Figuring out what the malware is after
- Discovering what rootkits do and why they exist

Rootkits have their origin in the Unix world. They were created to replace standard Unix tools with versions that gave a user *root* or super-user privileges, while allowing their activity to remain invisible to other users. A rootkit's unique hiding ability was quickly seized upon by hackers with ill intent as an ideal way to provide cover for devious activities.

If you find a rootkit on your computer, you can pretty much be assured that something else is lurking there, but you won't know what that something is. As malware, rootkits are considered to be among the most insidious and pernicious programs because of their ability to conceal the unknown.

In order to secure your system from rootkits, you need to understand the fundamentals of malware. In this chapter, our goal is to fill you in on those truths, and clue you in to the different types of malware and its aims, as well as the basics of rootkits.

COPYRIGHTED MATERIAL

Some Common Questions (and Answers) about Malware

A few questions are quite common when people first hear about malware and rootkits; this section lists the main questions — and, more importantly, the answers to them.

- **What is malware?** The term *malware* is short for *malicious software*. Malware is created with the intent to enter, modify, or damage the other software on your computer without your knowledge and consent. Like other malware, well-crafted rootkits do all these things — yet remain entirely invisible to the computer user.
- **What's the relationship between rootkits and malware?** Rootkits' relationship to malware is twofold: To put a rootkit on a computer, other malware has to load it. And after the rootkit is loaded, it's often used to hide more malware. Rootkits created with malicious intent (some rootkits are benign or even beneficial) collectively make up a specific category of malware; however, not all malware programs are rootkits.
- **Who's vulnerable to malware?** Any computer or network connected to the Internet is a viable target for a malware or rootkit attack. If you are on a broadband or T1 connection, which allows for rapid transfer of data, then you become an even more attractive target to blackhat hackers (about whom more in a minute). Public computers are also vulnerable; someone could just walk by, slip in a disc, and install malware that way.
- **Who's responsible for malware and what do they want from me?** Malware programmers are often portrayed in the popular press as malcontents, angry at the world, expressing their frustrations with destructive behavior and activities. Although this can be true, the people behind malware are more likely trying to manipulate millions of people, governments, even the stock markets — ultimately in order to make money. The worst among them are criminal and terrorist organizations who exploit the often-lighter sentences imposed for Internet offenses to make pots of money — using malware to steal identities, put the squeeze on Internet-based companies with Distributed Denial of Service attacks, and disrupt commerce with other costly exploits. See the "The Many Aims of Malware" section later in this chapter for more information about what, specifically, those who write and spread malware want from you and your computer.

Knowing the Types of Malware

When you go up against malware, you need to know your enemy. In the sections that follow, you find out about the different types of malware that you need to protect your system from.

Rootkits can be used with any of the major forms of malware described in the following sections.

Viruses

A *virus* is a small program that inserts itself into other executable software. Every time that software is opened and used, the virus program will run, making copies of itself to insert into every document and executable file opened. This can cause damage to your computer software, including your operating system, by corrupting existing data on all your storage media and overwriting your files.

As long as a virus program is present in any software you open, it can spread to other computers when you share files and programs with others — over the Internet using e-mail or P2P (peer-to-peer) file-sharing networks, or via infected CDs, DVDs, or floppy disks. Viruses persist primarily in stored memory on physical media such as your hard drive. New viruses are not as common a threat now as in the past, but they can have the rootkit technology included in their designs.

Worms

Worms are programs that can copy themselves; they exist in RAM (random-access memory). They spread by sending themselves via e-mail, instant-message programs, and peer-to-peer (P2P) file-sharing networks to other computers in a network. Unlike viruses, worms do not insert themselves into other programs — and they rarely affect the files on your hard drive. Worms cripple computers by congesting the flow of information, slowing down the system by using up its resources, or crashing the system altogether — all by making multiple copies of themselves. *Unpatched* computers, — those without the software fixes that plug security holes, — are a bonanza for them. Worms have shut down large portions of the Internet, causing millions of dollars in damages before they were stopped. They can also be carriers of root-kits, backdoors, and trojans (which we describe next).

Trojans

Trojan Horse programs (now mostly referred to as just *trojans*) are malicious applications masquerading as something helpful or innocuous. Veritable "wolves in sheep's clothing," they can disguise a destructive program as something more benign, such as an image file. A harmless-looking `.gif` extension, for example, may hide the `.exe` extension of an executable file.

This treacherous type of program was originally called a "Trojan Horse" after the giant "gift" horse (with soldiers inside) that the ancient Greeks offered as a ploy to get inside the city of Troy in *The Odyssey.* In this case, the "soldiers" are executable files — invading programs.

Beware of program files with double filename extensions. By default, Windows hides double extensions.

To make sure you can see double extensions in Windows XP, you need to change just one setting. Here's how:

1. **Click Start, Control Panel, Folder Options.**
2. **Click the "View" tab, and then click Hidden Files and Folders ➪ Show Hidden Files and Folders.**
3. **To see filename extensions, uncheck the box beside** *Hide file extensions for known file types.*
4. **Click "Apply" and then click OK.**

   Now Windows will show all the extensions associated with each file.

Trojans can be contained in a Web site link if you haven't set your Web browser to block scripts. They can also come in as e-mail attachments that you open without scanning first, or be bundled with a program you download from the Internet. Whichever way they reach you, they usually require some action on your part to be installed on your computer.

Dialers

Two kinds of *dialers* exist — one good, one bad. The good one is installed as part of your operating system; it helps you connect to the Internet via an analog dialup connection. The other is malware, used to set up a fraudulent connection (usually to an expensive, long-distance telephone number) or to force downloads — all of which gets charged to your telephone bill — through particular Web sites. Malware dialers can be installed by trojans, ActiveX and JavaScript scripts, and from opening attachments in spam e-mails. (Users of DSL or Broadband connections are usually not affected by dialers.)

Backdoors

Backdoors are programs (or modifications to existing programs) that give outside users remote access to your computer without requiring user identification. Backdoors attempt to remain hidden or to "hide in plain sight" by appearing to be innocent. They can also be special passwords set up on a login system to the same effect.

Backdoors can be installed through weaknesses in an unpatched or unprotected Windows computer, either directly by blackhat hackers or with a trojan, virus, or worm. They can even be installed as "Easter eggs" by the original programmers of software (a practice considered highly unethical).

Easter eggs are hidden programs within software that can be triggered using specific commands. Professional programmers tuck them inside commercial software and then tell other programmers how to access them to get amusing animations or messages. But that "little something extra" can just as easily be malware.

Spyware (and malicious adware)

Currently considered to be one of the greatest threats to Internet and computer security today, *spyware* includes a wide range of applications that use stealth and trickery to fool users into installing them. Broadly speaking, spyware takes full or partial control of computer operations while denying your rights to privacy and to choose for yourself what runs on your computer — all for the benefit of strangers. Whether used "legitimately" or illegally, spyware is a way for malicious people to attempt to control, monitor, and profit from you against your wishes. (We discuss the aims of malware in more detail a little later in this chapter.)

Adware programs are often associated with spyware, because many adware programs monitor your browsing habits to target you with specific advertisements. The companies that provide these often-surreptitiously-installed bits of software are quick to point out that their programs are "not spyware," but it's really six of one, or half a dozen of the other. Legitimate adware programs differ from illegitimate applications; they only include advertisements as a way to offset their production and maintenance costs. Illegitimate adware bombards you with flashy pop-up ads that won't go away till you click a Close button (which may trigger more).

Some adware programs disguise themselves as beneficial toolbars or search aids when they are anything but that. Such adware/spyware tool bars can redirect your browser, bias your search results, or serve targeted pop-up advertisements. There are, of course, toolbars that are legitimate such as the Google Toolbar which do deliver on their stated promise. As a general rule of thumb, legitimate toolbars are easily removable through the Add/Remove programs feature of the Windows Control Panel. Adware toolbars are often a nightmare to remove, and often appear out of nowhere on your desktop.

The CastleCops Security Forum maintains a Toolbar research database, which can help you decide whether a toolbar is legitimate or not:

```
www.castlecops.com/CLSID.html
```

Just so you know: Legitimate applications are not spying on you, not reporting back to their companies, and not wasting your time by requiring you to close ad windows. By contrast, many illegitimate adware programs provide targeted pop-up ads and build marketing profiles on each user — without the user's knowledge or consent — that can then be sold to other advertising agencies.

You may also know of spyware applications that are considered legitimate and are commercially available. Typically these are for use in specialized circumstances, such as when a company secretly monitors the activities of its employees; parents do likewise with their children who use the family computer, schools monitor their students while online, and so on. Check the laws in your area before using such applications yourself. One of the authors know people who have permanently ruined their relationships with family, friends, and neighbors by using spyware on their computers to monitor their children (this is different from a parental control program). When you spy on your children, you are also spying on their friends. Spying on someone over whom you have no authority is also a crime in most jurisdictions. Employers and institutions can do it, but individuals or parents should avoid these applications entirely. They are like a Pandora's Box. Curiosity can kill your reputation.

Spyware is generally installed in the following ways:

- **Presenting the spyware as something it's not:** Usually these types of spyware and malicious adware are packaged in a way that offers a perceived benefit to you, such as
  - Helping you search the Internet for Web sites you want to view
  - Providing you with a special program that promises to increase download speeds
  - Pretending to remove a nonexistent spyware threat while creating a real one
- **Tricking you into believing that a user action is required:** This devious approach may provide (for example) a link that says `Click here to have all media content displayed on this page` — and after it's too late, you realize that your click enabled the installation of an unwanted program.
- **Bundling the spyware (something you don't want) with a program you do want:** Unlike the preceding example, you do in fact get the program you think you're getting — but you *also* get spyware programs you

didn't necessarily bargain for. Often, people actually agree to download these programs by accepting the program's license agreement. If you actually *read* the entire agreement (which few people do), you may find some legalese that mentions that by downloading this program, you *also* agree to download other programs bundled with the software. The agreement may not tell you what those "other programs" do — but (unfortunately) they may very well be spyware.

- **Peer-to-peer (P2P) file-sharing programs are a major vector for bundled spyware.** Although not all P2P programs come with a spyware payload, many unfortunately do. Furthermore, the practice of opening your computer to anonymous downloads can introduce additional malware to your computer from infected shared P2P folders. You have to ask yourself whether free is really free, and if the risk of acquiring a rootkit or trojan is really worth the trade off. Early versions of Kazaa, for example, included spyware.

A freeware program called EULAlyzer scans the *end user license agreement* (or EULA) of a program for "interesting words and phrases" that might need a closer look. It does not dispense any legal advice, but it helps translate convoluted terms that can crop up in long EULAs. You can download it at

```
www.javacoolsoftware.com/eulalyzer.html
```

- **Installing a connection that automatically downloads additional crud.** The connection is totally dependent on the provider of the malware, and is typically achieved by installing a backdoor (for a rootkit), or a Browser Helper Object (BHO) for ordinary spyware, though some overlap may occur. The connection is then used to download additional unwanted software or updates to existing software to further compromise the infected machine. Usually these remote transfers run in the background, and may only catch your attention by slowing down your Internet access and your computer.
- **Doing "drive-by" downloads:** In effect, this technique (also known as a *WMF (Windows Metafile) exploit* denies users the right to choose what to put on their computers by installing something they *didn't* choose. A *metafile* contains a bunch of instructions for what and how to display a graphic image. A *drive-by download* is accomplished when you browse to a malicious Web site that uses vulnerabilities in your browser and operating system to force the spyware onto your computer.

A too-easy way to get a drive-by download is to be online without a firewall. You can even get one from legitimate sites that have been hacked to provide malware-based advertising (or their ad-servers might pass along the drive-by in ignorance). By far the most common drive-bys occur to people who either cruise pornographic sites for thrills or fall for scams that send them to *spoofed* (carefully faked) Web sites. Bottom

line: The dark side of the Internet is just as dark as a big city downtown at night; getting a drive-by is like being mugged. The download uses vulnerabilities in unpatched operating systems and browsers — which is another good reason to get Microsoft updates. In addition to Internet Explorer, other kinds of browsers (such as Mozilla's Firefox or Seamonkey) need regular updates for the same reasons.

The Many Aims of Malware

In the past, the majority of computer hackers used to be content to create mischief and leave a signature of their work as a memento of a successful break-in. The more ruthless ones might destroy data or your operating-system files, or even corrupt your BIOS (the computer's setup information), making a reformat and reinstall inevitable. Their primary reward for such activities was essentially the challenge and conquest. They did it because they could.

The seedier aspects of the cyber-landscape have changed considerably in recent years. Malware thrill-seekers still exist, but today, most purveyors of malware are in it for financial gain. Anything that enables them to make money is fair game. Many operate far enough outside the realm of legitimacy to qualify as cyber-criminals. Rootkits in particular are a perfect tool to use in these exploits, because rootkits allow long-term continued access to your computer without detection.

The goals of malware are many — none of them good for you, the user. In the following list we describe the different goals of malware.

So what are these malware coders after? The answer may include any of the following:

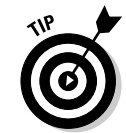
- **Data about your Web surfing:** By tracking your Web habits, they know what your interests are and what advertising should appeal to you in light of your browsing habits. Such spying enables commercial adware companies to serve targeted pop-ups suited to your personal preferences.
- **Control over your Web surfing:** In an even more invasive twist, your browser Start and Search pages may be hijacked to a Web site of the malware writer's choosing. If your browser is hijacked, then whenever you attempt to surf the Web, you're redirected to a Web site that bombards you with pop-up ads that the unscrupulous affiliate advertisers hope you'll click. Sometimes your browser remains frozen at a Web site where you will become a captive audience for an advertising campaign. When this happens, your entire surfing experience becomes defined by the adware infection.

A bunch of strangers you'll never know nor meet will benefit enormously from your new enslavement. They get their money from the agencies hired by companies to promote their products and services with advertising. No matter how the advertising is promoted (or how sleazy a technique this is), a certain percentage of the entrapped users *will* buy — increasing sales — always.

- **Your sensitive personal information:** Blackhat hackers may want your personal details to commit identity theft, enable bank-account access, or put fraudulent charges on your credit cards. Among the many ways they might try to get your information are the following:

  - **Deciphering weak passwords:** A weak password will allow an intruder easy access to your computer or network. This literally opens the door to all sorts of malicious activity and (in the case of a network) essentially guarantees access to many more computers. That's why using a safe-password generator and protection system is so critical. (We include such programs on this book's CD.) Flip to Chapter 4 for a refresher on how to make stronger passwords, and see the Appendix and Bonus Chapter 2 for more information on the password-related applications we have included on the CD.
  - **Using false security alerts to goad you into purchasing a program with hidden malware:** Some trojans may try to scare you by claiming that your computer is infected, when your computer is actually infected *by* the trojan they just planted on it!

    Your natural inclination will be to click the warning "bubble" — but *don't*. That click directs you to a bogus antispyware or antivirus Web site — which then attempts to con you into purchasing a useless "security" program to "remove" the nuisance threat. To make this scheme even more convincing, the security alerts intentionally mimic those of Windows, so victims are often fooled into thinking that the real Windows Security Center (instead of a cyber-swindler) is posting the alert. Deception and audacity reached a peak when the Vundo trojan used a near-perfect pop-up fake of the Windows Online Safety Center to redirect users to the Web site for the rogue WinFixer program. (Guess what it didn't fix.) The original WinFixer program is now known as WinAntiSpyware 2006 or WinAntivirus Pro. Same purpose, different name — and twins, no less.



Here's an online article with more information about schemes that try to annoy users into parting with their money in exchange for junk software:

```
www.websense.com/securitylabs/docs/WebsenseSecurity
        Labs20052H_Report.pdf
```

- **Using your system as a cloak for scam operations:** Some blackhat hackers want to hide behind your system and secretly put your computer or network to work for them. This is done by opening and maintaining an

Internet connection between your system (the server) and remote client computers controlled by the bad guys. *Remote-access trojans* (RATs) are used to commandeer your computer from the remote client by maintaining connections with an open, hidden port they have created. Once a RAT sets up shop, your system can be used for any number of nefarious tasks. In addition to identity theft, black marketeers can use your computer for anything — perhaps as a drop for illegal images or as a zombie for Distributed Denial of Service attacks against the Web sites of other businesses. A *zombie* is a computer slaved to an invisible network that attacks Web sites. When thousands of zombies are used in an attack, it's called a *Distributed Denial of Service (or DDoS)*.

Cases of malware installed by individuals acting alone do exist, but the greater threat to your life and liberty come in from (believe it or not) the cyber-version of the black market — and its sleazy cousin, the gray market:

- **Black-market groups are usually underwritten by criminal organizations who will go to any length to achieve their goals.** This includes using malware to record and transmit your personal information and financial transactions, and acquiring your passwords and debit- and credit card numbers. They know how to take you to the cleaners and then some. For example, with the right information, they can take out loans in your name, run your credit cards up in the twinkling of an eye, and clean out all your bank accounts.
- ***Gray-market groups* operate specifically to make money by using adware and spyware to promote advertising.** Some call this crew "corpirates," which succinctly describes what these people do. They can operate as regular businesses or corporations because their methods are less dramatic (and technically more legal) than those of the black-market groups. Secrecy and deception, however, are important parts of their work. Many of these groups provide fake security applications to the public — which then don't perform as expected, but deliver targeted pop-up advertisements to your computer instead. Once installed, such software is often hard to remove — and its Terms of Use are as convoluted as they are compromising to the rights of the computer user.

Many Internet businesses are mostly unregulated, unlike offline ones. Even though they are supposed to adhere to the laws of their countries of registration, they do pretty much whatever they like. Unsuspecting users who expect to be dealt with fairly online . . . are under a false impression. On the Internet, as in the old Wild West, (almost) anything goes! To learn more about these modern cyber-cor-pirates, please visit the SpywareWarrior Security Web site at

```
www.spywarewarrior.com/rogue_anti-spyware.htm
```

The Wild West aspect of online life even shows up in the common terms *blackhat* for malicious programs (and programmers) and *whitehat* for legitimate ones — reminiscent of the headgear worn by (respectively) bad guys and good guys in old Western movies.

Rootkits: Understanding the Enemy

A *rootkit* is a program designed to hide not only itself, but another program and all its associated resources (processes, files, folders, Registry keys, ports, and drivers). Rootkits can be *whitehat* (well-intentioned in purpose but still a potential security risk) or *blackhat* (malicious in nature). Malicious rootkits are often used to compromise and maintain remote control over a computer or network for illegitimate, — often criminal — purposes. Malicious rootkits do their work by hiding malware that installs a backdoor to allow an attacker to have unlimited and prolonged access to the infected computer.

A rootkit infection introduces a fundamental flaw into computer systems: Suddenly you can't really trust the integrity of the operating system or have any faith in the results it reports. Because of this flaw, you may be unable to distinguish whether your systems are pest-free or harboring some uninvited "visitor" that traditional scanners are unequipped to deal with.

When you go up against rootkits, you need to know your enemy. This section gives you the skinny on why they hide, how they survive, and why the little creeps exist in the first place. Chapter 7 discusses the more technical side of rootkits, describing in detail how they hide.

A Bit of Rootkit Lore

Rootkit technology is not new. In fact, rootkits have actually been in existence for over a decade. They were first developed for use on Unix-like operating systems (Solaris and Linux), and later evolved to encompass Windows platforms as well. The first public rootkit developed for the Windows NT platforms made its debut in 1999 when it was introduced by Greg Hoglund, a well-known security researcher and owner of rootkit.com. The unusual moniker *rootkit* is actually derived from *root* — a Unix reference (which implies root-level access to a system and administrator privileges) — and *kit* (which refers to the collective set of tools used to obtain that hidden and privileged access).

The discovery of the Sony Digital Rights Management (DRM) Rootkit by Mark Russonovich of Sysinternals suddenly thrust rootkits from relative obscurity to a position of prominence. Until the recent publicity barrage, rootkits had commanded little attention and had been implicated with a relatively small percentage of malware infestations. They were considered an intriguing but rarely encountered curiosity than an imminent threat. Enter the Sony rootkit exposé on October 31, 2005 — and suddenly rootkits took center stage. The Sony rootkit controversy has not only heightened public awareness, but it has also spurred the development of new rootkit technology and research, as well. These days, rootkits are regarded as a real and growing potential threat — and the security community has responded to this upgraded threat accordingly.

This unfolding scenario was bound to happen. As security vendors provided increasingly better solutions to combat nearly every type of pest, malware writers have responded by creating a stealthier and more tenacious breed of malware. Your basic Catch 22 scenario has developed. These new exploits are designed to outfox today's highly refined malware detection and removal programs. By embracing rootkits and their stealthy capabilities, cybercriminals have found a "new and improved"' way to launch an attack.

Stealth programs and rootkits represent a looming threat and the tide of the future. In fact, eweek's December 6, 2005 issue has reported that "More than 20 percent of all malware removed from Windows XP SP2 (Service Pack 2) systems are stealth rootkits, according to a senior official in Microsoft Corp.'s security unit." A more recent paper by the Microsoft Anti-malware Team entitled "Windows Malicious Software Removal Tool: Progress Made, Trends Observed" published on 6/12/2006, reports a more modest rootkit incidence of 14 percent. When the Sony DRM WinNT/F4IRootkit is factored out the figure drops to only 8 percent. Before you jump with joy over the apparent decrease in rootkit prevalence, let's put this in perspective. The June 2006 statistics represent incident rates on Windows 2000, Windows XP, and Windows Server 2003 computers, as opposed to only the extremely popular Windows XP SP2 platform. This would tend to lower the 2006 figures. The December 2005 statistics are not adjusted to exclude the Sony DRM rootkit and were released soon after its public discovery. It is likely more computers were affected by the Sony DRM rootkit at that time, and that would inflate the 2005 figures.

Microsoft has taken this threat very seriously. Apart from its rootkit tools (currently in development), it has incorporated rootkit detection and removal into a handy program called the Malicious Software Removal Tool (MSRT). A newly updated MSRT is delivered along with Windows updates every month — and it silently scans in the background for several commonly encountered rootkits. (Trying to root them out, so to speak.) In addition to rootkits, the MSRT also scans for some of the most pernicious but prevalent backdoor trojans and worms that known to be out there.

New Technologies, New Dangers

If you're like most of us, you may have faced many of the threats out there in cyberspace, putting security measures in place to protect your system from intrusion (and to remove any malware that does find a way to get in). It's true that many tools perform this function quite successfully when used in combination. But the fact that you're reading this book indicates that you may not be content with those security measures — or even confident that they're protecting you. If that's the case, you're right to be concerned.

With the appearance of rootkits on the scene, none of the brilliant tools developed for recognizing and removing malware threats can perform this function accurately. A rootkit can blind traditional security tools to the presence of malware programs, letting the invaders function unimpeded. If a rootkit makes its way into your system, conventional software scanners may still go about their business in the normal manner — scanning memory, processes, and Registry hives, producing scan results that smugly claim, `"no infection found."` The operating system is changed or tricked by the rootkit into reporting false results. In the end, both the scanners and the users are deceived. We can help you see past a rootkit's trickery.

Rootkits not only hide themselves, they also hide their malware-associated processes, files, Registry entries (on Windows systems), and ports. This malware-hiding capability is what makes rootkits so dangerous — and it is their whole reason for being. A rootkit, in and of itself, does not present a danger — it just makes danger easier. It only becomes dangerous when it is used to conceal illicit activity — or if it is exploited by other malware programs that seek to conceal their presence.

No operating system is immune

Rootkits are very platform-specific. Although Windows systems are by far their most frequent targets, rootkits were first developed on Unix systems. That is where the term comes from: *root* (administrative) access and *kit* (a Unix break-in tool). Linux, of course, is a derivative of Unix — so it has its own (smaller) subset of rootkits. You should also know that Mac OS X has a rootkit on record (see `www.theregister.co.uk/2004/10/25/mac_rootkit_opener/`).

Typically, malware writers invest their time writing programs that attack whichever platforms can reap them the most benefit — whether that means bragging rights (as in the early days) or illicit financial gain. No wonder so many malware programs are written for the popular Windows XP and Windows 2003 platforms — they get maximum exposure. Although malware writers usually won't waste their time writing for outdated Windows platforms or unpopular operating systems, any platform can attract their unwelcome attention by becoming more widely used.

But even though the rootkit serves to hide the activities and infected components installed on a system — as well as itself — all is not lost. Luckily, they have not yet reached the level of sophistication required to completely dupe all scanners. By understanding what rootkits are and how they work, you become better prepared to protect your computer or network from this security threat. The following sections explore these topics in more detail.

Why do rootkits exist?

As with many technological developments, rootkits have both good and bad uses. A rootkit by itself works like a hidden empty safe or vault. What matters is not the container itself, but whether it's ultimately used to store (so to speak) diamonds or vials of anthrax. A rootkit can hide a legitimate backup image of your operating system so your system can recover if it crashes — or the same little cache can tuck away a backdoor trojan. Although what's *in* a rootkit is of primary importance, there are ethical considerations at work. Legitimate uses for rootkits do exist — but many computer users oppose *any* use of a rootkit, regardless of whether its purpose is beneficial (whitehat) or malicious (blackhat). Some users object strenuously — and understandably — to anything being hidden from them on their own systems.

There is an even more compelling reason to object to including a rootkit of any kind — even a whitehat rootkit — in a program. Once a rootkit is known to exist, malware writers see it as an opportunity; They'll attempt to exploit its powers of concealment for their own benefit. Thus even whitehat rootkits pose a potential risk, which is why they're met with such criticism. A better technique is to employ encryption to ensure that critical data remains inaccessible and unaltered.

Any rootkit, regardless of its intended purpose, may be exploited by the bad guys to invisibly compromise a system.

All these efforts are aimed at hiding the presence of the intruder and the rootkit itself. Just as a thief who steals your wallet does not want to get caught, cyber criminals also try to maintain a low profile, so they can operate under a shroud of concealment.

Some deliver puppet masters

One common goal of a blackhat rootkit is to install a *puppet master* — to conceal a worm or trojan that takes over your computer and makes it a willing workhorse for malicious purposes. The usual technique is to hijack and

secretly maintain an open port that functions as a hidden backdoor, facilitating information transfer to and from your computer. Because the rootkit provides a shield of secrecy, such operations proceed stealthily and without interference. Your computer may have been recruited in such a manner to perform any (or all!) of the following dastardly deeds:

- **Launching Distributed Denial of Service attacks (DDoS) (or Night of the Cyber Dead):** The blackhat hacker may be recruiting your computer as a zombie or an unwitting accomplice to conduct a DDoS or Distributed Denial of Service attack on another system or network server.

  The object of a DDoS attack is to bombard a system or network with so much traffic that it becomes inaccessible to legitimate users. Computers are normally recruited en masse to launch a successful DDoS attack — all without the users' knowledge. Broadband subscribers who have "always-on" connections are particularly vulnerable to becoming members of the cyber-zombie army. Successful DDoS attacks have been launched against Microsoft.com, Apple.com, Yahoo, eBay, Amazon.com, and the Million Dollar Homepage (`www.milliondollarhomepage.com/`), to name only a few.

- **Sending spam e-mail:** An infected computer may be used to launch e-mail spam attacks against targeted computers by sending out a multitude of solicitous e-mails. The zombie computer owner gets blamed for spamming, and the true source of the spam remains anonymous. Many zombie computer owners often have no idea their systems are being used for such illicit purposes — and their first wake-up call may come in the form of a letter from their Internet Service Provider (ISP) which threatens them with suspension of service for spamming.

- **Hosting and distributing illegal material:** A rootkit may be used to conceal the fact that your computer has been recruited to store and distribute illegal or pirated content. Such content might include music or video libraries, or even criminal pornographic materials. Storing the content on the hard drive of a recruited victim's computer kills two birds with one stone: It enables the true content provider to conserve on their own hardware resources, but more importantly it enables them to dispense criminal content with little risk of being identified or prosecuted. This is because the evidence resides on the compromised system not their own.

Some are just spies

Rootkits that act as spies enable *keyloggers* and *packet-sniffers* — programs that hide on a user's system and (respectively) log the user's every keystroke and inspect the data transmitted to or from the user's system or network — to do their dirty work. Privacy? Forget it. And it gets worse. . .

- **Breaking the bank:** Keystroke logs can be correlated with Web page visits to aid in the extraction of private and sensitive data such as bank login information, credit card numbers, and the like. This information can then be transferred remotely to the bad guys' computer and used to conduct criminal financial transactions or commit identity theft. A rootkit is an ideal hacking tool because it allows an intruder to maintain a connection that cannot be detected by the user. This enables data transfer to progress without interruption.
- **Harvesting your habits:** Another less insidious — but very annoying — form of spying is practiced by adware companies; at least one of them is known to employ a rootkit to prevent the removal of its software (if you can't find it, you can't remove it). The collection and transmission of information that reveals a user's browsing habits is very valuable to commercial adware companies. This type of spying allows the companies to serve up targeted pop-up advertisements that are custom-selected to appeal to the user. The now-discontinued Apropos rootkit (distributed by the adware company ContextPlus, Inc.) performs this function — and frequently churns out new variants to dodge current removal techniques. Just when we thought it was safe to go back in the water, a new and even more devious adware rootkit has emerged — as if to take the place of the retired Apropos rootkit. Certain variants of Link Optimizer adware can be installed by the Gromozon rootkit, which arrives via a WMF (Windows MetaFile) exploit (on unpatched computers). This infection is extremely difficult to remove, and utilizes other sneaky techniques besides rootkit technology, to ensure its survival. For more information on this threat, please refer to the following description provided by Symantec, entitled "Gromozon.com and Italian spaghetti", and available at `www.symantec.com/enterprise/security_response/weblog/2006/08/gromozoncom_and_italian_spaghe.html`.
- **Sniffing the goods:** A *sniffer* is a common rootkit snooping tool that an intruder can install to capture all data transmitted over a network. Though network administrators may have legitimate uses for sniffers, a blackhat hacker uses a sniffer with a more devious intent. The captured data can be saved and analyzed to extract user login information. These stolen passwords are very valuable to an intruder, allowing an attacker to log on remotely and take anything the network has to offer — at the stolen password's privilege level. In this manner, an attacker can penetrate the network access files and retrieve all sorts of confidential and potentially valuable information.