Michael Miller

Microsoft® Security Essentials

USER MANUAL

Microsoft Security Essentials User Manual is the unofficial user's manual for Microsoft's new free anti-malware program. It shows users how to use MSE to safeguard your computer from viruses and spyware, how to download and configure MSE, how to manually scan for malware, how to keep the program updated, and how to schedule regular maintenance.

shortcut

QUE®

www.quepublishing.com

There's a lot of bad stuff out on the Internet. I'm not talking about offensive content (although there's a lot of that, too), but rather those things that can infect your system and damage or hijack your computer and personal files. This type of malicious software, or *malware*, is a huge threat—but one you can guard against by using Microsoft Security Essentials.

How Big is the Malware Threat?

Malware is any type of software program that does intentional damage to your computer hardware or software. There are two primary types of malware—computer viruses and spyware. They both can cause big problems, and need to be protected against.

Let's start by examining the virus threat. It's not something that only happens to "the other guy." In fact, back in 2005 the United States Department of Justice estimated that 34% of all computers were infected with computer viruses. Assuming that there were approximately 500 million computers in use worldwide at that time, this means that more than 150 million computers were victims of virus attacks.

▶ **NOTE**
Note that we're discussing viruses and spyware separately. That's because, while their impact is similar, they're technically quite different beasts. A computer virus actually causes a lot more damage than does spyware—even though spyware is much more common.

And if you thought the virus threat was big, consider the incidence of spyware infection. A 2005 study by America Online and the National Cyber-Security Alliance found that 61% of users' PCs were infected by some form of spyware—twice as many computers as were infected by viruses. Even more startling, PCSecurityNews.com states that an infected PC has, on average, 24.4 spyware programs surreptitiously installed. That's a lot of spyware!

Understanding Computer Viruses

So what exactly is a computer virus? The technical definition is, a malicious software program designed to do damage to your computer system by deleting files or even taking over your PC to launch attacks on other systems. A virus attacks your computer when you launch an infected software program, launching a "payload" that often is catastrophic.

How Computer Viruses Work

Many viruses are hidden in the code of legitimate software programs—programs that have been infected, that is. When the host program is launched, the code for the virus is executed and the virus loads itself into your computer's memory. From there, the virus code searches for other programs on your system that it can infect; if it finds one, it adds its code to the new program, which, now infected, can be used to infect other computers.

If all a virus did was copy itself to additional programs and computers, there would be little harm done, save for having all our programs get slightly larger (thanks to the added virus code). Unfortunately, most viruses not only replicate themselves, they also perform other operations—many of which are wholly destructive. A virus might, for example, delete certain files on your computer. It might overwrite the boot sector of your hard disk, making the disk inaccessible. It might write messages on your screen, or cause your system to emit rude noises. It might also hijack your email program and use the program to send itself to all your friends and colleagues, thus replicating itself to a large number of PCs.

Viruses that replicate themselves via email or over a computer network cause the subsidiary problem of increasing the amount of Internet and network traffic. These fast-replicating viruses—called *worms*—can completely overload a company's network, shutting down servers and forcing tens of thousands of users offline. Although no individual machines might be damaged, this type of communications disruption can be quite costly.

Other viruses open a back door to your system that can then be exploited by the virus writer. These types of backdoor viruses turn your machine into a so-called *zombie computer*, which the hacker operates via remote control to perform all manner of nefarious tasks. Hijacked computers of this sort are responsible for a large number of computer attacks and spam campaigns.

In short, viruses are nasty little bits of computer code, designed to inflict as much damage as possible, and to spread to as many computers as possible—a particularly vicious combination.

How to Catch a Computer Virus

Obviously, you want to avoid any behavior that could infect your computer with a virus. Unfortunately, viruses are spread by contact with other computers, or data copied from other computers. So whenever you share data with another computer or computer user, you risk exposing your computer to potential viruses.

Just how can you catch a computer virus? Since there are many ways you can share data with others, there are also many ways a virus can be transmitted:

- Opening an infected file attached to an email message or instant message
- Launching an infected program file downloaded from the Internet
- Sharing a data CD, USB memory drive, or floppy disk that contains an infected file
- Sharing over a network a computer file that contains an infected file

Of all these methods, the most common means of virus infection is via email—with instant messaging close behind. Whenever you open a file attached to an email message or instant message, you stand a good chance of infecting your computer system with a virus—even if the file was sent by someone you know and trust. That's because many viruses "spoof" the sender's name, thus making you think the file is from a friend or colleague. The bottom line is that no email or instant message attachment is safe unless you were expressly expecting it—and even then, an expected file attachment could still be infected with a virus, without the sender knowing it.

Almost as risky is the act of downloading files from so-called file-sharing sites or peer-to-peer (P2P) networks. This is the type of infection found most often on PCs used by teenagers; the teen downloads what he thinks to be music or video files from a file-sharing site, and in the process infects his computer with one or more viruses. It's an extremely common occurrence.

Understanding Different Types of Computer Viruses

As you've just learned, a computer virus is a piece of software that surreptitiously attaches itself to other programs, and then does something unexpected. There are different kinds of viruses, however, each of which has its own unique character and intent:

NOTE
About a decade ago, file infector viruses accounted for probably 85% of all virus infections. Today that number is much lower, because other types of viruses are much easier to spread—and virus writers tend to go for the low-hanging fruit.

- **File infector viruses.** This is the most "traditional" form of computer virus. A file infector virus hides within the code of another program—a business application, a utility, or even a game. When the infected program is launched, the virus code is copied into your computer's memory, typically before the program code is loaded. By loading itself into memory separately from the host program, the virus can continue to run in your system's memory even after the host program is closed down.
- **Boot sector viruses.** The boot sector is that part of a hard disk, floppy disk, or bootable CD that is read into memory and executed when your computer first boots up, and a boot sector virus resides in the boot sector of these bootable disks. After it is loaded, the virus can then infect any other disk used by the computer, including the PC's hard disk.
- **Macro viruses.** These viruses are created with the macro code used by many of today's software applications—including (and especially) Microsoft Office. What makes macro viruses potentially more dangerous than file infector or boot-sector viruses is that macro viruses can be attached to document files, such as Word documents and Excel spreadsheets. Because data files are shared so freely, macro viruses are able to spread rapidly from one

machine to another—and run, automatically, whenever the infected document is opened.

- **Script viruses.** These viruses are similar to macro viruses, based on the scripting languages, such as Java and ActiveX, typically used on websites and in some computer applications. Viruses created with these scripting languages can be quite destructive; they can also spread very quickly because the script code can be inserted into web pages, Word documents, and Excel spreadsheets, attached to email messages, and even secretly embedded in email messages. For that reason, many of today's most common viruses are script viruses.

NOTE
Many spyware programs also function as Trojan horses.

- **Trojan horses.** This isn't technically a computer virus; instead, it's a program that claims to do one thing but then does something totally different. A typical Trojan horse has a filename that appears to be some type of harmless file, but when you run the file, it's actually a virus program that proceeds to inflict its damage on your system. It delivers its payload through deception, just like the fabled Trojan horse of yore. Trojan horses are often spread as innocent-looking attachments to email messages; when you click to open the attachment, you launch the Trojan program.

- **Rootkits**. This is a particular type of Trojan horse designed to take control of a computer's operating system. Rootkits obscure their presence on the host system by evading standard system security methods. Intruders use rootkits to gain backdoor access to a computer system without detection, then using that computer for various unauthorized activities.

NOTE
Zombie computers working together as botnets are thought to be responsible for most of the spam sent today.

- **Botnet Trojans.** A *botnet* is a collection of software robots, or “bots,” that run automatically on hijacked zombie computers. The computers are hijacked when they’re infected with a special kind of Trojan, called a botnet Trojan, which is designed specifically to allow remote control of a large mass of computers. The network of botnet computers is then used for various purposes, typically to send spam or conduct denial of service attacks on targeted websites.
- **Worms.** A worm, like a Trojan horse, isn’t technically a computer virus. Instead, it’s a program that scans a company’s network or the Internet for another computer that has a specific security hole. It copies itself to the new machine (through the security hole), and then starts replicating itself there. Worms replicate themselves very quickly; a network infected with a worm can be brought to its knees within a matter of hours.

Bottom line, it doesn’t matter what type of virus you’re talking about, it’s always bad news. Fortunately, you can protect your system by using an anti-virus program, such as Microsoft Security Essentials—which can also protect against spyware.

Understanding Spyware and Adware

Spyware is a type of malware that is similar to but different from computer viruses. Like a Trojan horse, spyware typically gets installed in the background when you're installing another program, without your knowledge or consent. Unlike a virus, however, spyware doesn't replicate itself; its job is to spy on your system, not to spread itself to other computers.

That's right, spyware surreptitiously sends information about the way you use your PC to some interested third party. And that's not a good thing.

How Spyware Works

Just what type of information does spyware monitor? Here's a short list of what a spyware program could do:

- Record the addresses of each web page you visit
- Record the contents of each email you send or receive—along with email addresses of people you correspond with
- Record the contents of all the instant messages you send or receive—along with the usernames and addresses of your IM partners
- Record the entire contents of each chat room you visit—and log the usernames and addresses of other channel members
- Record every keystroke you type with your computer keyboard—including usernames, passwords, and other personal information