FIFTH EDITION

COMPUTER SECURITY FUNDAMENTALS

DR. CHUCK EASTTOM

Computer Security Fundamentals

Fifth Edition

Dr. Chuck Easttom

Pearson

- 3—Pack and execute, hidden, asynchronously
- 4—Pack and execute, visible, synchronously
- 5—Pack and execute, hidden, synchronously
- 6—Execute only, visible, asynchronously
- 7—Execute only, hidden, asynchronously
- 8—Execute only, visible, synchronously
- 9—Execute only, hidden, synchronously

3. Enter the command line.
4. Enter the second file (the item you are surreptitiously installing).
5. Enter the operation.
6. When done with files, press Enter.

In Figure 5.1 you can see a demonstration that is appropriate for a classroom laboratory. In this example, two innocuous programs are combined into one Trojan horse. The programs chosen are simple Windows utilities that won't harm the computer. However, this example illustrates how easy it would be to combine legitimate programs with malware for delivery to a target computer.

This illustration is meant to show how easy it is to create a Trojan horse, not to encourage you to do so. It is important to understand just how easy this process is so you can understand the prevalence of malware. Any attachment or download should be treated with significant suspicion.

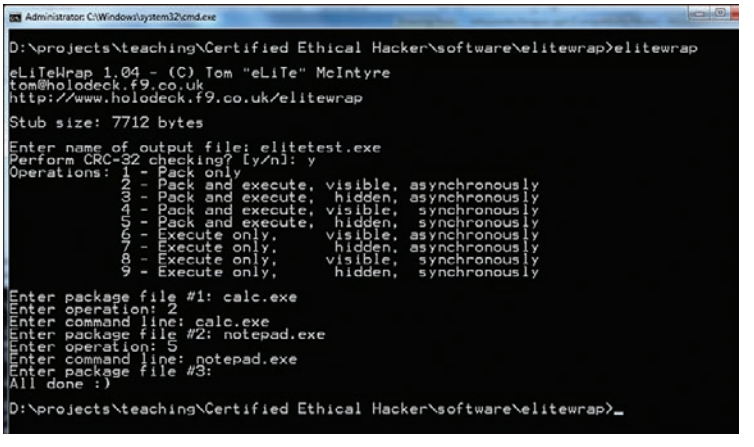

FIGURE 5.1 eLiTeWrap.

The Buffer-Overflow Attack

You have become knowledgeable about a number of ways to attack a target system: denial of service, virus, and Trojan horse. While these attacks are probably the most common, they are not the only methods. Another method of attacking a system is called a buffer-overflow (or buffer-overrun) attack. A buffer-overflow attack happens when someone tries to put more data in a buffer than the buffer was designed to hold. Any program that communicates with the Internet or a private network must take in some data. This data is stored, at least temporarily, in a space in memory called a *buffer*. If the programmer who wrote the application was careful, then when you try to place too much information into a buffer, that information is simply truncated or outright rejected. Given the number of applications that might be running on a target system and the number of buffers in each application, the chances of having at least one buffer that was not written properly are significant enough to cause any prudent person some concern.

Someone who is moderately skilled in programming can write a program that purposefully writes more into the buffer than it can hold. For example, if the buffer can hold 1024 bytes of data and you try to fill it with 2048 bytes, the computer simply loads the extra 1024 bytes into memory. If that extra data is actually a malicious program, then it has just been loaded into memory and is thus now running on the target system. Or, perhaps the perpetrator simply wants to flood the target machine's memory, thus overwriting other items that are currently in memory and causing them to crash. Either way, the buffer overflow is a very serious attack.

Fortunately, buffer-overflow attacks are a bit harder to execute than DoS attacks or simple Microsoft Outlook script viruses. To create a buffer-overflow attack, you must have a good working knowledge of some programming language (C or C++ is often chosen) and understand the target operating system/application well enough to know whether it has a buffer-overflow weakness and how that weakness might be exploited.

It must be noted that modern operating systems and web servers are not generally susceptible to common buffer-overflow attacks. Windows 95 was quite susceptible, but it has been many years since a Windows operating system was susceptible. Certainly Windows 7, 8, 10, or 11 cannot be compromised with this type of attack. However, the same cannot necessarily be said for all the custom applications developed to run on various systems. It is always possible that an Internet-enabled application, including but not limited to web applications, might be susceptible to this kind of attack.

Essentially, this vulnerability exists only if programmers fail to program correctly. If all programs truncate extra data, then a buffer overflow cannot be executed on a system. However, if a program does not check the boundaries of variables and arrays and allows excess data to be loaded, then that system is vulnerable to a buffer overflow.

The Sasser Virus/Buffer Overflow

Sasser is an older form of malware but one that demonstrates the use of a buffer-overflow attack. Sasser involves a combination of a virus (or worm) that spreads by exploiting a buffer overrun.

The Sasser virus spreads by exploiting a known flaw in a Windows system program. Sasser copies itself to the Windows directory as avserve.exe and creates a Registry key to load itself at startup. Therefore, once your machine is infected, you will start the virus every time you start the machine. This virus scans random IP addresses, listening on successive TCP ports starting at 1068 for exploitable systems—that is, systems that have not been patched to fix this flaw. When one is found, the worm exploits the vulnerable system by overflowing a buffer in LSASS.EXE, which is a file that is part of the Windows operating system. That executable is a built-in system file and is part of Windows. Sasser also acts as an FTP server on TCP port 5554, and it creates a remote shell on TCP port 9996. Next, Sasser creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm from the infected host. The infected host accepts this FTP traffic on TCP port 5554. The computer also creates a file named win.log on the C: drive. This file contains the IP address of the localhost. Copies of the virus are created in the Windows System directory as #_up.exe. Examples are shown here:

- c:\WINDOWS\system32\12553_up.exe
- c:\WINDOWS\system32\17923_up.exe
- c:\WINDOWS\system32\29679_up.exe

A side effect of this virus is that it causes your machine to reboot. A machine that is repeatedly rebooting without any other known cause may well be infected with the Sasser virus.

This is another case in which the infection can easily be prevented by several means. First, if you update your systems on a regular basis, those systems should not be vulnerable to this flaw. Second, if you ensure that your network's routers or firewall block traffic on the ports involved (9996 and 5554), you will prevent most of Sasser's damage. Your firewall should only allow traffic on specified ports; all other ports should be shut down. In short, if you as the network administrator are aware of security issues and are taking prudent steps to protect the network, your network will be safe. Many networks have been affected by this virus, however, indicating that not enough administrators are properly trained in computer security.

Spyware

In Chapter 1, "Introduction to Computer Security," spyware was mentioned as one of the threats to computer security. Using spyware, however, requires a great deal more technical knowledge on the part of the perpetrator than do some other forms of malware. The perpetrator must be able to develop spyware for the particular situation or customize existing spyware for his needs. He must then be able to get the spyware on the target machine.

Spyware can be as simple as a cookie used by a website to record a few brief facts about your visit to that website, or it could be of a more insidious type, such as a key logger. Recall from Chapter 1 that a key logger is a program that records every keystroke you make on your keyboard; this spyware then logs your keystrokes to the spy's file. The most common use of a key logger is to capture usernames

and passwords. However, this method can capture every username and password you enter and every document you type, as well as anything else you might type. This data can be stored in a small file hidden on your machine for later extraction or sent out in TCP packets to some predetermined address. In some cases, the software is even set to wait until after hours to upload this data to some server or to use your own email software to send the data to an anonymous email address. There are also some key loggers that take periodic screenshots from your machine, revealing anything that is open on your computer. Whatever the specific mode of operation, spyware is software that literally spies on your activities on a particular computer.

Legal Uses of Spyware

There are some perfectly legal uses for spyware. Some employers have embraced spyware as a means of monitoring employee use of company technology. Many companies have elected to monitor phone, email, or web traffic within the organization. Keep in mind that the computer, network, and phone systems are the property of the company or organization, not of the employee. These technologies are typically supposed to be used only for work purposes; therefore, company monitoring might not constitute an invasion of privacy. While courts have upheld this monitoring as a company's right, it is critical to consult an attorney before initiating this level of employee monitoring as well as to consider the potential negative impact on employee morale.

Parents can also elect to use this type of software on their home computer to monitor the activities of their children on the Internet. The goal is usually a laudable application—protecting their children from online predators. Yet, as with employees in a company, the practice may illicit a strong negative reaction from the parties being spied upon (namely, their children). Parents have to weigh the risk to their children versus what might be viewed as a breach of trust.

How Is Spyware Delivered to a Target System?

Clearly, spyware programs can track all activity on a computer, and that information can be retrieved by another party via a number of different methods. The real question is this: How does spyware get onto a computer system in the first place? The most common method is through a Trojan horse. It is also possible that when you visit a certain website, spyware may download in the background while you are simply perusing the website. Of course, if an employer (or parent) is installing the spyware, it can then be installed openly in the same way that an organization would install any other application.

Pegasus

The Pegasus spyware was seen first in 2016, and then variations of it were found in 2022. This spyware affects mobile phones, and there are versions for both iPhone and Android. Given our growing dependence on our mobile devices, mobile malware is at least as important as traditional computer malware. The 2022 version of Pegasus is able to track calls and locations, collect passwords, and read text messages. What makes Pegasus especially intriguing is that it was originally developed for the Israeli government.

Obtaining Spyware Software

Given the many other utilities and tools that have been mentioned as being available from the Internet, you probably will not be surprised to learn that you can obtain many spyware products for free or at very low cost on the Internet. You can check the Counterexploitation website (www.cexx.org), shown in Figure 5.2, for a lengthy list of known spyware products circulating on the Internet and for information about methods you can use to remove them. The SpywareGuide website (www.spywareguide.com) lists spyware that you can get right off the Internet should you feel some compelling reason to spy on someone's computer activities. Figure 5.3 shows the categories of malware that are available from this site. Several key logger applications are listed on this site, as shown in Figure 5.4. These applications include well-known key loggers such as Absolute Keylogger, Tiny Keylogger, and TypO. Most can be downloaded for free or for a nominal charge.

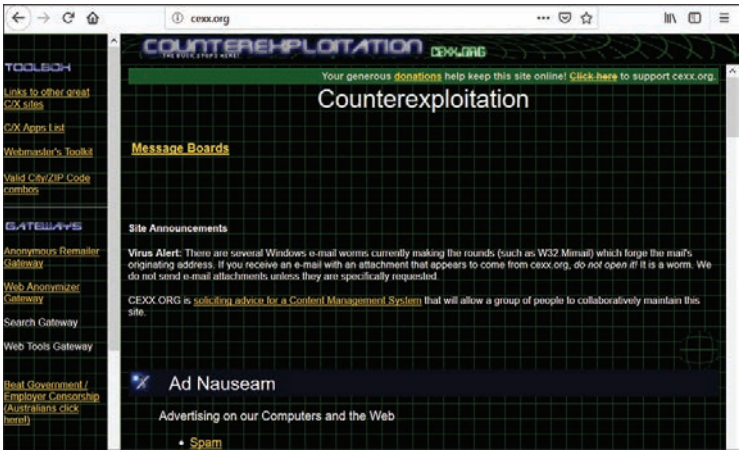

FIGURE 5.2 Counterexploitation website.

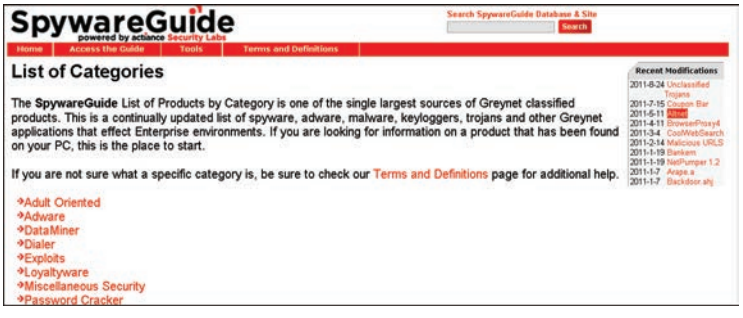

FIGURE 5.3 Malware categories at the SpywareGuide website.

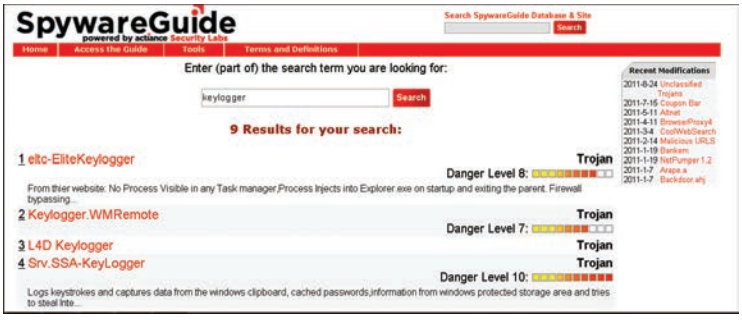

FIGURE 5.4 List of key loggers available through the SpywareGuide website.

Some well-known Trojan horses are also listed at this site (as shown in Figure 5.5), such as the 2nd Thought application, which downloads to a person's PC and then blasts it with advertisements. This particular piece of spyware is one that downloads to your PC when you visit certain websites. It is benign in that it causes no direct harm to your system or files; it also does not gather sensitive information from your PC. However, it is incredibly annoying as it inundates your machine with unwanted ads. This sort of software is often referred to as *adware*. Frequently, these ads cannot be stopped by normal protective pop-up blockers because the pop-up windows are not generated by a website that you visit but rather by rogue software running on your machine. Pop-up blockers only work to stop sites you visit from opening new windows. Websites use well-known scripting techniques to cause your browser to open a window, and pop-up blockers recognize these techniques and prevent the ad windows from opening. However, adware that launches a new browser instance bypasses the pop-up blocker's function.

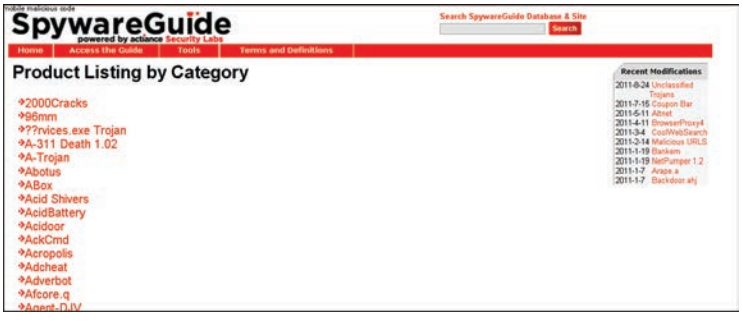

FIGURE 5.5 Trojan horses available at the SpywareGuide website.

Other Forms of Malware

This chapter and preceding chapters have discussed the most prominent forms of malware. There are, however, many other forms of attack. It is beyond the scope of this book to explore all of them, but you