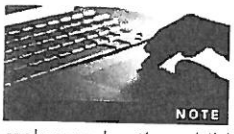
Chapter 3: Network and Computer Attacks

As an IT security professional, you need to be aware of attacks an intruder can make on your network. Attacks include unauthorized attempts to access network resources or systems, attempts to destroy or corrupt information, and attempts to prevent authorized users from accessing resources. You must have a good understanding of both network security and computer security. Network security involves protecting the network infrastructure as well as stand-alone systems. Therefore, computer security is necessary to protect computers and laptops that aren't part of a network infrastructure but still contain important or confidential information. Protective measures include examining physical security, right down to checking door locks, and assessing the risks associated with a lack of physical security.

This chapter gives you a strong foundation on what attackers are doing. Just as law enforcement personnel must be aware of the methods criminals use, you must know what computer attackers are up to. How can a denial-of-service attack be used to shut down a company? How can worms and viruses be introduced into a company's corporate database? How can a laptop or desktop computer be removed from your office with little risk of the intruder being caught or stopped? In this chapter, you get an overview of attack methods and protective measures. To understand the importance of physical security, you also learn that an unscrupulous in-house employee can pick a lock in seconds.

Malicious Software (Malware)

Many network attacks are malicious, initiated to prevent a business from operating. **Malware** is malicious software, such as a virus, worm, or Trojan program, introduced into a network for just that reason. The main goal of malware used to be to destroy or corrupt data or to shut down a network or computer system. The goal today is about making money. Scores of cybercrime organizations have warehouses full of programmers who do nothing but write malware with signatures unknown to antivirus programs. The following sections cover different types of malware that attackers use.



Security Bytes

Security professionals know that the Russian Business Network (RBN, also known by many other names) is one of the most well-structured cybercrime organizations in existence. The RBN's specialty is creating malware; hosting child pornography, spam, and phishing Web sites; and committing identity theft. RBN has employed experienced and dangerous computer programmers and hackers. When you learn how to use a security tool, remember that the bad guys are learning how to use it, too. Don't give up, however! The good guys need good hackers who can give the bad guys a run for their money.

Viruses

A **virus** is a program that attaches itself to a file or another program, often sent via e-mail. The key word is "attaches." A virus doesn't stand on its own, so it can't replicate itself or operate without the presence of a host. A virus attaches itself to a host file or program (such as Microsoft Word), just as the flu attaches itself to a host organism, and then performs whatever the creator designed it to do. For example, Figure 3-1 shows a virus attached to a .zip file. The virus sender uses a common ploy: purported naked pictures of his wife. This ploy lures a naive computer user into clicking and therefore running the attached infected file.

The bad news about viruses is that there's no foolproof method of preventing them from attaching themselves to computers, no matter how skilled you are as a security professional. Many antivirus software packages are available, but none can guarantee protection because new viruses are created constantly. Antivirus software compares signatures (programming code) of known viruses against signatures of every file on a computer; if there's a match, the software warns you that the program or file is infected. These signatures are kept in a **virus signature file** that the antivirus software maintains. If the virus isn't known, however, the antivirus software doesn't detect a match. Therefore, updating virus signature files regularly is crucial. Many antivirus software packages offer automatic updates. For example, with Symantec Antivirus, administrators can configure a server that handles pushing antivirus updates to client computers in an organization.

Macro Viruses

A **macro virus** is a virus encoded as a macro in programs that support a macro programming language, such as Visual Basic for Applications (VBA). For example, you can write a macro, which is basically a list of commands, in Microsoft Word that highlights a document's contents (Ctrl+A), copies the selected data (Ctrl+C), and then pastes the information into a different part of the document (Ctrl+V). Macro commands that open and close files, however, can be used in destructive ways. These commands can be set to run automatically as soon as a file is opened or clicked on, as in an e-mail attachment. The most infamous macro virus is Melissa, which appeared in 1999. It was initiated after a user opened an infected document; the virus then sent an e-mail message to the first 50 entries it located in the infected computer's address book.

In the past, viruses were created by programmers who found the challenge of creating a destructive program rewarding. Today, even nonprogrammers can create macro viruses easily. In fact, anyone with Internet access can find many Web sites to learn how to create a macro virus step by step. This easy access adds to the problems you must deal with as a security professional. It's helpful to put yourself in computer criminals' frame of mind and, like an FBI profiler, try to understand how they think. A good place to start is visiting Web sites of virus creators and seeing what they have to say.

Worms

A **worm** is a program that replicates and propagates itself without having to attach itself to a host (unlike a virus, which needs to attach itself to a host). The most infamous worms are Code Red (covered in Activity 3-3), Nimda, and Conficker. Theoretically, a worm that replicates itself multiple times to every user it infects can infect every computer in the world over a short period. This result is unlikely, but as with many pyramid schemes, it's easy to see how a worm can propagate throughout an entire network and even across the Internet.

Table 3-2 describes some of the most infamous worms that have cost businesses millions of dollars as a result of lost productivity caused by computer downtime and time spent recovering lost data, reinstalling programs and operating systems, and hiring or contracting IT personnel. Security professionals are also working to protect automated teller machines (ATMs) from worm attacks, such as the Slammer and Nachi worms. Cyberattacks against ATMs are a serious concern for the banking industry and law enforcement agencies worldwide.

Trojan Programs

One of the most insidious attacks against networks and computers worldwide takes place via **Trojan programs**, which disguise themselves as useful programs and can install a backdoor or rootkit on a computer. **Backdoors** or **rootkits** are programs that give attackers a means of regaining access to the attacked computer later. A rootkit is created after an attack and usually hides itself in the OS tools, so it's almost impossible to detect. Back Orifice is still one of the most common Trojan programs used today. It allows attackers to take full control of the attacked computer, similar to the way Windows XP Remote Desktop functions, except that Back Orifice works without the user's knowledge. The program has been around since 1999, but it's now marketed as an administrative tool rather than a hacking tool.

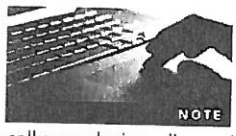
Spyware

If you do a search on the keyword "spyware," you'll be bombarded with hundreds of links. Some simply tout spyware removal, but some install spyware on a computer when the user clicks the Yes button in a dialog box asking whether the computer should be checked for spyware (see Figure 3-2). When you click the Yes button, the spyware installation begins.

A **spyware** program sends information from the infected computer to the person who initiated the spyware program on your computer. This information could be confidential financial data, passwords, PINs—just about any data stored on your computer. You need to make sure users understand that this information collection is possible, and spyware programs can register each keystroke entered. It's that simple. This type of technology not only exists but is prevalent. It can be used to record and send everything a user enters to an unknown person located halfway around the world. Tell users they shouldn't assume that physical security measures, such as locked doors, are enough to keep all intruders out.

Adware

The difference between spyware and **adware** is a fine line. Both programs can be installed without users being aware of their presence. Adware, however, sometimes displays a banner that notifies users of its presence. Adware's main purpose is to determine a user's purchasing habits so that Web browsers can display advertisements tailored to this user. The biggest problem with adware is that it slows down the computer it's running on.



Security Bytes

Network security begins with each user understanding how vulnerable a computer is to attack. However, being aware of malware's presence, just as you're aware of unscrupulous telemarketers who call you during dinnertime, can better equip you to make valid decisions. If someone offers to sell you property in Tahiti for $99.95 over the phone and asks for your credit card number, you'd refuse. Computer users should be just as skeptical when prompted to click an OK button or install a free computer game.