High-Tech Talk

Computer Viruses: Delivery, Infection, and Avoidance

Klez. Melissa. Mydoom. Nimda. Like the common cold, virtually countless variations of computer viruses exist. Unlike the biological viruses that cause the common cold, people create computer viruses. To create a virus, an unscrupulous programmer must code and then test the virus code to ensure the virus can replicate itself, conceal itself, monitor for certain events, and then deliver its *payload* — the destructive event or prank the virus was created to deliver. Despite the many variations of viruses, most have two phases to their execution: infection and delivery.

To start the infection phase, the virus must be activated. Today, the most common way viruses spread is by people running infected programs disguised as e-mail attachments. During the infection phase, viruses typically perform three actions:

1. First, a virus replicates by attaching itself to program files. A *macro virus* hides in the macro language of a program, such as Word. A *boot sector virus* targets the master boot record and executes when the computer starts. A *file virus* attaches itself to program files. The file virus, Win32.Hatred, for example, replicates by first infecting Windows executable files for the Calculator, Notepad, Help, and other programs on the hard disk. The virus then scans the computer to locate .exe files on other drives and stores this information in the system registry. The next time an infected file is run, the virus reads the registry and continues infecting another drive.
2. Viruses also conceal themselves to avoid detection. A *stealth virus* disguises itself by hiding in fake code sections, which it inserts within working code in a file. A *polymorphic virus* actually changes its code as it infects computers. The Win32.Hatred virus uses both concealment techniques. The virus writes itself to the last file section, while modifying the file header to hide the increased file size. It also scrambles and encrypts the virus code as it infects files.
3. Finally, viruses watch for a certain condition or event and activate when that condition or event occurs. The event might be starting the computer or reaching a date on the system clock. A *logic bomb* activates when it detects a specific condition (say, a name deleted from the employee list). A *time bomb* is a logic bomb that activates on a particular date or time. Win32.Hatred, for instance, unleashes its destruction when the computer clock hits the seventh day of any month. If the triggering condition does not exist, the virus simply replicates.

During the delivery phase, the virus unleashes its payload, which might be a harmless prank that displays a meaningless message — or it might be destructive, corrupting or deleting data and files. When the Win32.Hatred virus triggers, it displays the author's message and then covers the screen with black dots. The virus also deletes several antivirus files as it infects the system. The most dangerous viruses do not have an obvious payload; instead they quietly modify files. A virus, for example, could change numbers randomly in an inventory program or introduce delays to slow a computer. One way antivirus software detects computer viruses is by monitoring files for unknown changes, particularly in file size. Because many computer viruses alter system and data files — files that should not change in size — changes in file sizes often are a key indication of an infection.

Other kinds of electronic annoyances exist in addition to viruses. While often called viruses, worms, Trojan horse programs, and rootkits actually are part of a broader category called *malicious-logic programs* or *malware*.

- A *worm*, such as the CodeRed or Sircam worm, resides in active memory and replicates itself over a network to infect machines, using up the system resources and possibly shutting the system down.
- A *Trojan horse* is a destructive program disguised as a real program, such as a screen saver. When a user runs a seemingly innocent program, a Trojan horse hiding inside can capture information, such as user names and passwords, from your system or open up a backdoor that allows a hacker remotely to control your computer. Unlike viruses, Trojan horses do not replicate themselves.
- A *rootkit* is a program that easily can hide and allow someone to take full control of your computer from a remote location, often for nefarious purposes. For example, a rootkit can hide in a folder on your computer, and the folder will appear empty. This is because the rootkit has instructed your computer not to display the contents of the folder. Rootkits can be very dangerous and often require special software to detect and remove. Rootkits are becoming more common. In fact, a recent study has shown that more than 20 percent of computers in the United States are infected with a rootkit. It is extremely important that you use caution when installing software from unknown sources.

Every computer user is susceptible to a computer virus. Studies show that an unprotected computer can be infected by a virus within minutes after being connected to the Internet. Due to the increasing threat of viruses attacking your computer, it is more important than ever to protect your computer from viruses. Figure 3-47 lists steps you can follow to protect your computer from a virus infection.

For more information, visit scsite.com/dc2011/ch3/tech and then click Computer Viruses.

Steps to Virus Protection

1. Install the latest Microsoft updates.
2. Purchase a reputable antivirus program.
3. After installing an antivirus program, scan your entire computer to be sure it is free of malware.
4. Update your antivirus definitions regularly.
5. Be suspicious of any and all unsolicited e-mail attachments.
6. Stay informed about viruses and virus hoaxes.
7. Install a personal firewall program.
8. Download software only if you are sure the Web site is legitimate.
9. Avoid as best you can visiting unscrupulous Web sites.

Figure 3-47 Guidelines to keep your computer virus free.