**Types of Viruses**

There are many different types of viruses. In this section we will briefly look at some of the major virus types. Viruses can be classified by either their method of propagation or their activities on the target computers. It must also be noted that various experts differ slightly on how they group viruses. The taxonomy presented in this section is rather common, and I find it to be quite useful. It is one I have developed over the years.

**Macro Viruses**

Macro viruses infect the macros in office documents. Many office products, including Microsoft Office, allow users to write mini-programs called macros. These macros can also be written as a virus. A macro virus is written into a macro in some business application. For example, Microsoft Office allows users to write macros to automate some tasks. Microsoft Outlook is designed so that a programmer can write scripts using a subset of the Visual Basic programming language, called Visual Basic for Applications (VBA). This scripting language is, in fact, built into all Microsoft Office products. Programmers can also use the closely related VBScript language. Both languages are quite easy to learn. If such a script is attached to an e-mail and the recipient is using Outlook, then the script can execute. That execution can do any number of things, including scanning the address book, looking for addresses, sending out e-mail, deleting e-mail, and more.

**Boot Sector**

Boot sector viruses don’t infect the operating system of the target computer, but instead attack the boot sector of the drive. This makes them harder to detect and remove with traditional antivirus software. Such software is installed in the operating system, and to some extent only operates within the context of the operating system. By operating outside the operating system, a boot sector virus is harder to detect and remove. Multipartite viruses attack the computer in multiple ways—for example, infecting the boot sector of the hard disk and one or more files within the operating system.

**Stealth**

Stealth viruses are one of the largest groups of viruses. This category includes any virus that uses one or more techniques to hide itself. In other words, these are viruses that are trying to avoid your antivirus software.

The Trojan horse is an excellent way to hide a virus. By tying it to a legitimate program, it not only will trick the user into installing it, but it may also evade antivirus software.

A polymorphic virus literally changes its form from time to time to avoid detection by antivirus software. A more advanced form of this is called the metamorphic virus, which can completely change itself. This also requires a secondary module to perform the rewriting.

A sparse infector virus attempts to elude detection by performing its malicious activities only sporadically. With a sparse infector virus, the user will see symptoms for a short period, then no symptoms for a time. In some cases the sparse infector targets a specific program but the virus only executes every 10th time or 20th time that target program executes. Or a sparse infector may have a burst of activity and then lie dormant for a period of time. There are a number of variations on the theme, but the basic principle is the same: to reduce the frequency of attack and thus reduce the chances for detection.

Fragmented payload is a rather sophisticated method of hiding a virus. The virus is split into modules. The loader module is rather innocuous and unlikely to trigger any antivirus software. It will then download, separately, the other fragments. When all fragments are present, the loader will assemble them and unleash the virus.

**Ransomware**

It is impossible in modern times to discuss malware and not discuss ransomware. In fact, as I am writing this, in the past 48 hours the world has been hit with a massive ransomware attack. It began by attacking health care systems in England and Scotland, and spread far beyond those. That virus is the infamous WannaCry virus. While many people first began discussing ransomware with the advent of CryptoLocker in 2013, ransomware has been around a lot longer than that. The first known ransomware was the 1989 PC Cyborg Trojan, which only encrypted filenames with a weak symmetric cipher.

In general, ransomware works as a worm, then either disables system services or encrypts user files. It then demands a ransom to release those files/service.

**Trojan Horses**

You have seen the term *Trojan horse* used in this chapter, and you probably already have some idea of what it is. A Trojan horse is a program that looks benign but actually has a malicious purpose. You might receive or download a program that appears to be a harmless business utility or game. More likely, the Trojan horse is just a script attached to a benign-looking e-mail. When you run the program or open the attachment, it does something else other than or in addition to what you thought it would. It might

images Download harmful software from a website.

images Install a key logger or other spyware on your machine.

images Delete files.

images Open a backdoor for a hacker to use.

Finding virus and Trojan horse attack combinations is commonplace. In these instances, the Trojan horse spreads like a virus. The MyDoom virus opened a port on machines that a later virus, Doomjuice, would exploit, thus making MyDoom a combination virus and Trojan horse.

**FYI: Was MyDoom a Trojan Horse?**

Some experts say that MyDoom was not actually a Trojan horse because it did not pretend to be benign software. However, one could argue that the e-mail attachment that delivered MyDoom did indeed claim to be a legitimate attachment and, thus, could be classified as a Trojan horse. Whether or not you agree that MyDoom is a Trojan horse, it is certainly a good illustration of how malicious software can take multiple avenues to cause harm.

A Trojan horse also could be crafted especially for an individual. If a hacker wanted to spy on a certain individual, such as the company accountant, she could design a program specifically to attract that person’s attention. For example, if she knew the accountant was an avid golfer, she could write a program that computed handicap and listed best golf courses. She would post that program on a free web server. She would then e-mail a number of people, including the accountant, telling them about the free software. The software, once installed, could check the name of the currently logged-on person. If the logon name matched the accountant’s name, the software could then go out, unknown to the user, and download a key logger or other monitoring application. If the software did not damage files or replicate itself, then it would probably go undetected for quite a long time.

Writing such a program could be within the skillset of virtually any moderately competent programmer. This is one reason many organizations have rules against downloading any software onto company machines. I am unaware of any actual incident of a Trojan horse being custom tailored in this fashion. However, remember that those who create virus attacks tend to be innovative people.

Another scenario to consider is one that would be quite devastating. Without divulging programming details, the basic premise is outlined here to illustrate the grave dangers of Trojan horses. Imagine a small application that displays a series of unflattering pictures of Osama Bin Laden. This would probably be popular with many people in the United States, particularly people in the military, the intelligence community, or defense-related industries. Now assume that the application simply sits dormant on the machine for a period of time. It need not replicate like a virus because the computer user will probably send it to many of his or her associates. On a certain date and time, the software connects to any drive it can, including network drives, and begins deleting all files.

If such a Trojan horse were released “in the wild,” within 30 days it would probably be shipped to thousands, perhaps millions, of people. Imagine the devastation when thousands of computers begin deleting files and folders.

This scenario is mentioned precisely to frighten you a little. Computer users, including professionals who should know better, routinely download all sorts of files from the Internet, including amusing Flash animations and cute games. Every time an employee downloads something of this nature, the chance of downloading a Trojan horse exists. One need not be a statistician to realize that if employees continue that practice long enough they will eventually download a Trojan horse on to a company machine. A user can only hope it is not one as vicious as the theoretical one just outlined here.

**FYI: Using Trojan Horse Examples**

Readers are strongly cautioned against attempting to actually create any of these Trojan horse scenarios. Releasing such an application is a crime that will probably result in a lengthy prison sentence and serious civil penalties. These examples are provided simply to show you just how devastating a Trojan horse can be.

The people who create Trojan horses and viruses are quite creative. New variations pop up frequently. It is highly likely that someone else has already thought of something similar to the scenarios I present. The point of presenting these scenarios is to make sure that network administrators exercise the appropriate level of caution. To be totally frank, it is my wish that every network administrator have a certain level of paranoia regarding viruses and Trojan horses.