Malicious Software/Malware

Not all software performs beneficial tasks. Some software infiltrates one or more target computers and follows an attacker's instructions. These instructions can include causing damage, escalating security privileges, divulging private data, or even modifying or deleting data. This type of software is **malicious software**, or **malware** for short. The purpose of malware is to damage or disrupt a system. The effects of malware can range from slowing down a PC to causing it to crash, enabling the theft of credit card numbers, and worse. Simply surfing the Internet, reading email, or downloading music or other files can infect a personal computer with malware—usually without the user's knowledge.

Malware exists in two main categories: infecting programs and hiding programs. Infecting programs actively attempt to copy themselves to other computers. Their main purpose is to carry out an attacker's instructions on new targets. Malware of this type includes the following:

- Viruses
- Worms

As their name implies, hiding programs hide in the computer, carrying out the attacker's instructions while avoiding detection. Malware that tends to hide includes the following:

- Trojan horses
- Rootkits
- Spyware

The following sections describe each type of malware.

Viruses

A computer *virus* is a software program that attaches itself to or copies itself into another program on a computer. The purpose of the virus is to trick the computer into following instructions not intended by the original program developer. Users copy infected files from another computer on a network, from a flash drive, or from an online service. Alternatively, users can transport viruses from home and work on their portable computers, which have access to the Internet and other network services.

A computer virus acts in a similar fashion to a biological virus. It "infects" a host program and may cause that host program to replicate itself to other computers. The virus cannot exist without a host, and it can spread from host to host in an infectious manner.

The first virus recorded was the Creeper virus, written by researcher Bob Thomas in 1971. The Creeper copied itself to other networked computers, displaying the message "I'm the creeper, catch me if you can!" Thomas designed the virus as an experimental self-replicating program to see how such programs would affect computers on a network. Shortly after the Creeper virus was released, researchers unleashed the Reaper program to find and eradicate the Creeper.

Today, hundreds of thousands of known viruses infect programs of all types. The main concern with viruses is that they often attach themselves to common programs. When users run these infected programs, they are actually running virus code with their user credentials and authorization. The virus doesn't have to escalate privileges; the user who runs the infected program provides the virus with his or her authenticated credentials and permissions.

Over time, viruses have grown smarter. For example, some viruses can combat malware-detection programs by disabling their detection functions. Others compensate for the fact that files infected by a virus typically increase in size, making them relatively easy to detect, by spoofing the preinfected file's size. That way, it appears that nothing has changed.

Worms

A *worm* is a self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. The worm's purpose may be simply to reduce network availability by using up bandwidth, or it may take other nefarious actions. The main difference between a virus and a worm is that a worm does not need a host program to infect. The worm is a standalone program.

The first worm reported to spread "in the wild" was the Morris worm. Robert Tappan Morris wrote the Morris worm in 1988. The Morris worm attacked a buffer overflow vulnerability. The original intent of the Morris worm was to estimate the size of the Internet by spreading across the Internet and infecting computers running versions of the UNIX operating system. The worm spread faster than its author expected, however. In the end, the worm infected computers multiple times, eventually slowing each infected computer to the point it became unusable. The Morris worm was the first malware incident to gain widespread media attention and resulted in the first conviction under the U.S. 1986 Computer Use and Fraud Act.

Trojan Horses

A *Trojan horse*, also called a **Trojan**, is malware that masquerades as a useful program. Its name comes from the fabled Trojan horse in *The Aeneid*. In the poem, the Greeks, who had been at war with Troy for 10 years, construct a large wooden horse and offer it as a "gift" to the Trojans. The Trojans, viewing the gift as a peace offering, bring the horse into the city. That night, as the Trojans sleep, Greek soldiers hiding in the belly of the hollow horse climb out and open the city gates to admit the rest of the Greek army into the city. The Greeks soundly defeat Troy that night.

Similarly, Trojan horse programs use their outward appearance to trick users into running them. They look like programs that perform useful tasks, but actually, they hide malicious code. Once the program is running, the attack instructions execute with the user's permissions and authority.

The first known computer Trojan was Animal, released in 1974. Animal disguised itself as a simple quiz game in which the user would think of an animal and the program would ask questions to attempt to guess the animal. In addition to asking questions, however, the program copied itself into every directory to which the user had write access.

Today's Trojans do far more than just save copies of themselves. Trojans can hide programs that collect sensitive information, open backdoors into computers, or actively upload and download files. The list of possibilities is endless.

Rootkits

Rootkits are newer than other types of malware. They did not appear until around 1990. A rootkit modifies or replaces one or more existing programs to hide traces of attacks. Although rootkits commonly modify parts of the operating system to conceal traces of their presence, they can exist at any level—from a computer's boot instructions up to the applications that run in the operating system. Once installed, rootkits provide attackers with easy access to compromised computers to launch additional attacks.

Rootkits exist for a variety of operating systems, including Linux, UNIX, and Microsoft Windows. Because there are so many different types of rootkits, and because they effectively conceal their existence once installed on a machine, they can be difficult to detect and remove. Even so, identifying and removing rootkits is crucial to maintaining a secure system. A host-based IDS can help detect rootkit activity.

If you do detect a rootkit on your system, the best solution is often to restore the operating system from the original media. This requires rebuilding and restoring user and application data from backups, assuming these exist. This becomes more difficult if you have not completely documented the system. Preventing unauthorized access that can enable an attacker to install a rootkit is far more effective than attempting to remove an installed rootkit.

Spyware

Spyware is a type of malware that specifically threatens the confidentiality of information. It gathers information about a user through an Internet connection, without his or her knowledge. Spyware is sometimes bundled as a hidden component of freeware or shareware programs that users download from the Internet, similar to a Trojan horse. Spyware can also spread via peer-to-peer file swapping. Spyware has been around since the late 1990s, increasing in popularity after 2000. The rapid growth of the Internet enabled attackers to collect useful information from more and more unsuspecting users.

Once installed, spyware monitors user activity on the Internet. Spyware can also gather information such as email addresses and even passwords and credit card numbers. The spyware can relay these data to the author of the spyware. The author might use the data simply for advertising or marketing purposes but could employ it to facilitate identity theft.

In addition to stealing information, spyware steals from users by using their Internet bandwidth to transmit this information to a third party, as well as by consuming their computers' memory resources. Computers running multiple spyware programs often run noticeably more slowly than clean computers. Furthermore, because spyware uses memory and other system resources, it can cause system instability or even crashes.

Because spyware exists as independent executable programs, it can perform a number of operations, including the following:

Monitoring keystrokes
Scanning files on the hard drive
Snooping other applications, such as chat programs or word processors
Installing other spyware programs
Reading cookies
Changing the default homepage on the web browser