**Virus Propagation Techniques**

By definition, a virus must contain technology that enables it to spread from system to system, aided by unsuspecting computer users seeking to share data by exchanging disks, sharing networked resources, sending electronic mail, or using some other means. Once they’ve “touched” a new system, they use one of several propagation techniques to infect the new victim and expand their reach.

**Master Boot Record Viruses** The master boot record (MBR) virus is one of the earliest known forms of virus infection. These viruses attack the MBR—the portion of bootable media (such as a hard disk, USB drive, or CD/DVD) that the computer uses to load the operating system during the boot process. Because the MBR is extremely small (usually 512 bytes), it can’t contain all the code required to implement the virus’s propagation and destructive functions. To bypass this space limitation, MBR viruses store the majority of their code on another portion of the storage media. When the system reads the infected MBR, the virus instructs it to read and execute the code stored in this alternate location, thereby loading the entire virus into memory and potentially triggering the delivery of the virus’s payload.

Most MBR viruses are spread between systems through the use of infected media inadvertently shared between users. If the infected media is in the drive during the boot process, the target system reads the infected MBR, and the virus loads into memory, infects the MBR on the target system’s hard drive, and spreads its infection to yet another machine.

**File Infector Viruses** Many viruses infect different types of executable fi les and trigger when the operating system attempts to execute them. For Windows-based systems, the names of these fi les end with .exe and .com extensions. The propagation routines of fi le infector viruses may slightly alter the code of an executable program, thereby implanting the technology the virus needs to replicate and damage the system. In some cases, the virus might actually replace the entire fi le with an infected version. Standard fi le infector viruses that do not use cloaking techniques such as stealth or encryption.

A variation of the fi le infector virus is the companion virus . These viruses are self-contained executable fi les that escape detection by using a filename similar to, but slightly different from, a legitimate operating system fi le. They rely on the default filename extensions that Windows-based operating systems append to commands when executing program fi les ( .com , .exe , and .bat , in that order). For example, if you had a program on your hard disk named game.exe , a companion virus might use the name game.com . If you then open a Command tool and simply type GAME , the operating system would execute the virus fi le, game.com , instead of the fi le you actually intended to execute, game.exe . This is a very good reason to avoid shortcuts and fully specify the name of the fi le you want to execute.

**Macro Viruses** Many common software applications implement some sort of scripting functionality to assist with the automation of repetitive tasks. These functionalities often use simple, yet powerful programming languages such as Visual Basic for Applications (VBA). Although macros do indeed offer great productivity-enhancing opportunities to computer users, they also expose systems to yet another avenue of infection—macro viruses.

**Service Injection Viruses** Recent outbreaks of malicious code use yet another technique to infect systems and escape detection—injecting themselves into trusted runtime processes of the operating system, such as svchost.exe , winlogin.exe , and explorer.exe .

**Virus Technologies**

Multipartite viruses use more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.

Stealth viruses hide themselves by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally

Polymorphic viruses actually modify their own code as they travel from system to system.

Encrypted viruses use cryptographic techniques,

**Hoaxes**

No discussion of viruses is complete without mentioning the nuisance and wasted resources caused by virus hoaxes . Almost every email user has, at one time or another, received a message forwarded by a friend or relative that warns of the latest virus threat roaming the Internet

**logic bombs** are malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions such as time, program launch, website logon, and so on. The vast majority of logic bombs are programmed into custom-built applications by software developers seeking to ensure that their work is destroyed if they unexpectedly leave the company.

**Trojan Horses**

System administrators constantly warn computer users not to download and install software from the Internet unless they are absolutely sure it comes from a trusted source. In fact, many companies strictly prohibit the installation of any software not prescreened by the IT department. These policies serve to minimize the risk that an organization’s network will be compromised by a Trojan horse —a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network

**Worms**

*Worms* pose a significant risk to network security.

**Code Red Worm**

The Code Red worm received a good deal of media attention in the summer of 2001 when it rapidly spread among web servers running unpatched versions of Microsoft’s Internet Information Server (IIS). Code Red performed three malicious actions on the systems it penetrated

**Stuxnet**

In mid-2010, a worm named Stuxnet surfaced on the Internet. This highly sophisticated worm uses a variety of advanced techniques to spread, including multiple previously undocumented vulnerabilities. Stuxnet uses the following propagation techniques:

■ Searching for unprotected administrative shares of systems on the local network

■ Exploiting zero-day vulnerabilities in the Windows Server service and Windows Print Spooler service

■ Connecting to systems using a default database password

■ Spreading by the use of shared infected USB drive

**Spyware and Adware**

Two other types of unwanted software interfere with the way you normally use your computer. ***Spyware* monitors your actions and transmits important details to a remote system that spies on your activity**

***Adware , while quite similar to spyware in form, has a different purpose. It uses a variety of techniques to display advertisements on infected computers. The simplest forms of adware display pop-up ads on your screen while you surf the Web***

**Back Doors**

*Back doors* are undocumented command sequences that allow individuals with knowledge of the back door to bypass normal access restrictions. They are often used during the development and debugging process to speed up the workflow and avoid forcing developers to continuously authenticate to the system

**Protecting against SQL Injection - Perform Input Validation, Limit Account Privileges & Use Stored Procedures**

**IP Probes**

IP probes (also called IP sweeps or ping sweeps ) are often the first type of network reconnaissance carried out against a targeted network. With this technique, automated tools simply attempt to ping each address in a range. Systems that respond to the ping request are logged for further analysis. Addresses that do not produce a response are assumed to be unused and are ignored.

Dumpster diving is one of the oldest attacker tools in the book, and it’s still used today. The best defense against these attacks is quite simple—make them more difficult. Purchase shredders for key departments, and encourage employees to use them. Keep the trash locked up in a secure area until the garbage collectors arrive. A little common sense goes a long way in this area…