Understanding Virus Behavior in 32-bit Operating Environments

Executive Summary

Personal computer viruses pose a significant threat to today's business environment. As users share more information both over networks and through floppy diskettes, the rate of virus outbreaks continues to increase. The DOS environment has traditionally experienced the greatest number of viruses, now in the range of over 5,000. In recent years, however, a number of new viruses have been written that specifically target the Windows platform.

Will we see viruses that directly target 32-bit operating system environments such as the emerging Windows 95? Unfortunately the answer is yes. While Windows 95 introduces technologies that bring new power to users, it also allows greater opportunities for viruses. For example, Windows 95 has no file-level protection, which means any unprotected drives and files that are shared on a peer-to-peer network can be quickly infected when any computer on that network becomes infected. In addition, Windows 95 has no built-in anti-virus capabilities, making it critical for corporations and individuals to enhance their systems with a third-party anti-virus solution.

This paper examines computer viruses and their impact on 32-bit operating systems. It explains why these systems are susceptible to virus attacks and how emerging technologies may actually speed the transmission of viruses. It then describes the technologies available to detect and eradicate viruses and summarizes Symantec's anti-virus solution for 32-bit operating system environments such as Windows 95, Windows NT, and OS/2.

Computer Viruses and How They Spread

A computer virus is a small program written to alter the way a computer operates—without the permission or knowledge of the user. A virus need meet only two criteria. First, it must execute itself, often placing some version of its own code in the path of execution of another program. Second, it must replicate itself. For example, it may copy itself to other executable files or to disks that the user accesses. Viruses can invade desktop machines and network servers alike.

Types of Viruses

PC viruses fall into two major categories: program (or parasitic) viruses and boot sector viruses. Program viruses infect program files. These files typically have extensions such as .COM, .EXE, .OVL, .DLL, .DRV, .SYS, .BIN, and even .BAT. Examples of known program viruses include Jerusalem and Cascade. Boot sector viruses infect the system area of a disk—that is, the boot record on floppy diskettes and hard disks. All floppy diskettes and hard disks (including disks containing only data) contain a small program in the boot record that is run when the computer starts up. Boot sector viruses attach themselves to this part of the disk and activate when the user attempts to start up from the infected disk. Examples of boot sector viruses are Form (the most prevalent virus today), Disk Killer, Michelangelo, and Stoned. A third class of viruses, known as multipartite viruses, infects both boot records and program files.

How Viruses Spread

The most common way a boot virus spreads is by starting a computer with an infected floppy diskette in drive A:. Often this happens accidentally by leaving a data disk in drive A: when starting the computer. The infected floppy diskette immediately writes its code to the master boot record (MBR). The MBR runs each time a computer is started, so from then on, the virus runs each time the computer is started. The MBR runs no matter what operating system you are using (DOS, Windows 95, OS/2, Windows NT, UNIX, etc.), so a virus can infect any type of operating system. Once the virus has infected the computer, it has two primary jobs: to propagate itself to other computers and to activate its "trigger" (the event that causes the virus to perform its task). To propagate itself to other computers, a virus needs to find a "carrier." A carrier can be a file or it can be another floppy diskette. Most boot sector viruses will infect any floppy diskette that is inserted into the floppy drive. When another system is inadvertently started with this floppy diskette in its boot drive, that system becomes infected too. If the virus infects a file as a carrier and the file is run on another user's system, the virus gains control and infects more files or the boot sector of the second system.

Virus Damage

Most viruses have a "payload," the action or destruction the virus performs. Some viruses are programmed to damage the computer by corrupting programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses, however, can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and the bugs may lead to system crashes and data loss.

Viruses in a Windows 95 Environment

Windows 95 runs DOS programs, Windows 16-bit programs, and Windows 32-bit programs. To retain compatibility with previous versions of Windows, Windows 95 operates very much like Windows 3.1 under DOS. Windows 95, like DOS, first starts in what is called real mode. In real mode, programs and device drivers from CONFIG.SYS and AUTOEXEC.BAT can be loaded. Following this load process, the graphical component of Windows 95 starts up. Once Windows completes start- up, the user can run a DOS program by starting a DOS box. The DOS box contains a copy of all programs run during the initial system startup, including any virus code that may have been loaded. Unfortunately, this means every DOS box started will always have the same programs - including viruses—that were loaded before the graphical component of Windows 95 started, and multiple DOS sessions can result in many infections.

In previous versions of Windows, DOS managed the file system. This changes with Windows 95. Windows 95 manages the file system by employing device drivers and 32-bit programs. Windows 95 needs to ensure the integrity

of the file system is preserved. To accomplish this, DOS programs (and viruses) are blocked when they try to write directly to a hard disk unless they use special Windows 95 specific code to do so. However, writing directly to floppy diskettes is still permitted from within Windows 95. That's great for viruses, but bad for users: A virus can still behave and work in the very same manner as it does from the hard drive. And as great as Windows 95 is, it can do little to stop it.

When the user inadvertently boots with an infected floppy diskette in the drive, the virus can still infect the MBR. The virus loads each time the computer is started and installs itself in each DOS box. Then, when the user accesses the floppy diskette, the virus can propagate itself to that floppy diskette and thereby spread to other computers.

In addition, with DOS, there is no file-level protection in Windows 95. Viruses that use files to propagate are still able to do so under Windows 95. This is consistent across other 32-bit operating systems such as OS/2 and Windows NT, which also allow writing to files. Thus, program viruses can propagate exactly as they always have in the DOS environment.

How New Technologies Can Help Viruses Spread

Some of the technologies that make Windows 95 so attractive actually help propagate viruses across the network. For example, the workgroup networking environment is very susceptible to rapid virus-spreading. Again, since Windows 95 has no file-level protection, unprotected drives and files that are shared on a peer-to-peer network can quickly become infected when any of the computers on that network become infected.

Potential New Viruses

In the anti-virus community, there are discussions of new types of viruses that may emerge because of the features found in Windows 95. One possible type of virus is an OLE2 virus. This type of virus could easily spread by disguising itself as an OLE2 server of any common service. Then, when an OLE2 client asks an OLE2 server to provide this common service, the virus could actually gain control. It could propagate itself to other files or computers, then run the original OLE2 server it replaced. The application wouldn't even know that it was talking with a virus rather than the actual OLE2 server. And if the OLE2 server were on a completely different network computer, the virus could quickly spread itself throughout the network.

Another possible type of virus is a shell extension virus. Microsoft has made the shell in Windows 95 completely extensible to allow for customization. Technically, a virus could be one of those extensions. Windows 95 requires no validation for shell extensions, so a virus could be written as an extension that could gain control and propagate itself.

Another type of virus that could become popular is a Virtual Device Driver (VxD) virus. A Windows 95 VxD has complete control over the entire computer system. It can write directly to a hard disk if programmed to do so. It has the same privileges as the Windows 95 kernel, so it has a wide latitude of control over the system. With Windows 95, Microsoft has added the ability to load VxDs dynamically—a VxD doesn't need to be in memory at all times, but only when needed. That means that a virus could have a small amount of code that activates a dynamic VxD, which could then cause severe disruptions to the computer. Because there are no restrictions on what it can do, a VxD virus could bypass any type of protection mechanism you may have employed.

Another area that may present new opportunities for viruses is the proliferation of easy-to-use programming tools for Windows. In the past, virus writers required a more intimate knowledge of assembly language and the operating system to create TSRs to propagate. For Windows, viruses can be written in high-level languages with visual programming toolkits by more novice programmers. These viruses are also harder to detect since they look very much like all the other programs a user is running.

Greater technology usually brings with it greater risks and complexities. Windows 95 offers significant new advantages to computer users. It also presents new opportunities and challenges to virus writers. The behavior of these individuals in the past leads to the conclusion that they will look at Windows 95 as fertile ground. Virus writers, like users, are attracted to the new and most prevalent technologies. The scenarios described in this paper represent just a few of the new types of viruses that can appear. MIS managers have already determined this themselves (PCWeek 8/22/94). They predict that the new application Install Wizard in Windows 95, which helps the user to install a new program from a floppy diskette, will provide a very easy way for a virus to spread itself. It is only a matter of time before virus writers discover new and innovative ways of infecting computers.

Other 32-Bit Environments

Viruses are not restricted just to DOS or Windows. A virus can infect any type of computer, no matter what operating system it is running. Nevertheless, most viruses are DOS viruses, because of the preponderance of DOS machines operating around the world. Virus writers are like other software developers in their desire to develop for the biggest market.

In 32-bit environments, just as in DOS, when the computer is started, specific code is run each time. If this code is replaced by a virus, then the virus code runs instead. For example, if you have a computer running Windows NT, you may inadvertently boot from an infected floppy diskette when you start your computer. This infected floppy diskette replaces the master boot record (MBR) on your hard disk with its virus code. Then, every time your system is started, the virus code runs and your system is infected with a virus. The virus then attempts to propagate itself to other computers by loading itself in memory and waiting for a floppy diskette to be accessed. It loads into memory with the assumption that DOS will load next.

For NT, OS/2, and a number of other advanced operating systems, DOS isn't loaded immediately. Instead, these operating systems load their own system files, which overwrite the virus in memory. The computer is still infected, but the virus can't spread since its propagation code has been overwritten in memory by the operating system. However, the virus can still deliver its payload. When the infected computer first starts up, the virus runs. At that point, the virus might do just about anything, including format the hard disk. On operating systems other than DOS and Windows 95, infections are just as likely to occur and payloads are just as likely to be triggered; however, the virus is unable to easily propagate itself since the operating system will overwrite the propagation virus code in memory.

Symantec's AntiVirus Solution for Windows 95

Norton AntiVirus products are essential for every Windows 95 installation because the operating environment does not have built-in anti-virus capabilities. The Norton AntiVirus for Windows 95 and the Norton AntiVirus for NetWare with support for Windows 95 provide protection using an innovative and advanced technology that detects the ever-increasing number of known and unknown viruses while it minimizes intrusion on end users and system administrators.

Norton AntiVirus for Windows 95 is the new version of Symantec's award-winning virus-protection product and is designed specifically for the Windows 95 environment. It provides the most advanced and comprehensive virus protection available, combining several advanced technologies to deliver protection from both known and unknown viruses. These technologies not only detect viruses, but they also repair files damaged by those viruses. Scans run automatically, providing continuous protection.

Conclusion

Viruses are just as much a threat in 32-bit environments as they are in DOS and Windows environments. The number of viruses will continue to increase and become more sophisticated, taking advantage of the new features in Windows 95. The lack of anti-virus software included in the operating system makes it more important than ever to use third-party tools that monitor and protect systems from virus infection.

Because Windows 95 is a brand new operating system, utilities designed for DOS and Windows 3.1 do not support it reliably. Symantec's Norton AntiVirus for Windows 95 and Norton AntiVirus for NetWare 2.0 provide both individual users and enterprise managers with complete protection solutions for the 32-bit operating system environment.

Further Reading

This document is one of a series of papers on Symantec's enterprise network strategy and its network management product offerings. Additional papers include:

- Addressing Today's Access to the Enterprise Network
- Workstation Access Control: A Key Element in Securing Enterprise
- Networks
- Reducing Network Administration Costs with Remote Workstation Recovery Tools
- Using Backup Products for Enterprise-wide Storage Management
- Enterprise Developer: Creating Client/Server Applications in an Enterprise Environment
- Managing Distributed Networks with the Norton Enterprise Framework Architecture
- Improving the Bottom Line with Project Management Software
- Trends in Project Management Software: Open Connectivity and Client/Server Architecture
- Using Remote Control Software to Gain Access to the Enterprise Network
- Building the Ecosystem: Enabling the Next Generation of Client/Server Computing
- Why Norton Utilities is a Natural Complement to the Windows 95 Environment
- Managing Desktop Interface Across the Enterprise
- A Strategy for the Migration to Windows 95
- Understanding File Management and Windows 95

For copies of these papers or information about Symantec enterprise network products, call 1-800-453-1135 and ask for P162. Outside the United States contact the sales office nearest you.

About Symantec

Symantec Corporation is a leading software company with award-winning application and system software for Windows, DOS, Macintosh, and OS/2 computer systems. Founded in 1982, Symantec has grown rapidly through the success of its products and a series of 15 acquisitions resulting in a broad line of business and productivity solutions. The company has several enterprisewide products that have been introduced recently and others that are under development.

Symantec's acquisitions have strongly influenced the company's innovative organization. The company is organized into several product groups that are devoted to product marketing, engineering, technical support, quality assurance, and documentation. Its finance, sales, and marketing organizations are centralized at corporate headquarters in Cupertino, California.