MCAFEE
Network Security & Management

White Paper

An Introduction to Computer Viruses (and other Destructive Programs)

McAfee
2710 Walsh Avenue
Santa Clara, CA 95051
Tel: 408-988-3832
Fax: 408-970-9727
BBS: 408-988-4004
Internet: mcafee.com
Web Server: www.mcafee.com
America Online: MCAFEE
CompuServe: GO MCAFEE

An Introduction to Computer Viruses (and Other Destructive Programs)

Table of Contents

A virus is a computer program that executes when an infected program is executed. Therefore only executable files can be infected. On MS-DOS systems, these files usually have the extensions .EXE, .COM, .BAT or .SYS. Another class of files called overlay files can also be infected. These files often have the extension .OVL, although other extensions such as .OV1 are sometimes used.

By definition, a virus infects other programs with copies of itself. It has the ability to clone itself, so that it can multiply, constantly seeking new host environments. The most harmless viruses do only that, simply replicating and spreading to new systems. Or the virus program may damage other programs and/or alter data, perhaps self-destructing when done. The only evidence viruses like this leave is the destruction they have inflicted on the infected system. This makes it very difficult to develop defenses against the virus.

Virus programs, like the infectious microorganisms that are their namesakes, are often small. Only a few lines of program code are required to write a simple virus. The implication is clear: viruses can be easily hidden in healthy software and therefore prove very difficult to find.

Viruses can infect any computer, from a small laptop to a multi-million dollar mainframe. Anyone who owns a personal computer can create a virus program. This means virus development tools are widely available. Once written, a virus can be transmitted over telephone lines or distributed on infected disks to other systems, where it can reproduce in microseconds to damage the biggest systems thousands of miles away. These two facts make it virtually impossible to trace any virus back to the person who originally wrote it.

An Introduction to Computer Viruses (cont.)

Computer viruses may be benign and result only in amusement or slight annoyance. The best known example of such a virus are some versions of the 'Stoned' virus which simply write "Your computer is stoned" on the monitor. Other viruses are more malignant and malicious, destroying or altering data. Once a virus is active in a host computer, the infection can spread rapidly throughout a network to other systems.

A virus may attach itself to other programs and hide in them. Or it may infiltrate the computer's operating system. All computer operating systems, (for example, MS- and PC-DOS, Unix and Macintosh OS) are vulnerable, some more than others.

Viruses enter computer systems from an external software source. Just as flowers are attractive to the bees that pollinate them, virus host programs are deliberately made attractive to victims. Often the attraction will be a new game made available for downloading from a computer bulletin board. Or it may be disguised as an executable file attached to an electronic mail message from a friend or business associate.

Viruses can become destructive as soon as they enter a system, or they can be programmed to lie dormant until activated by a trigger. This trigger may be a predetermined date or time. The well-known Michelangelo virus, for example, has a trigger set for Michelangelo's birthday (March 6). Another type of triggering mechanism watches for a specific, common sequence of keystrokes. For example, some older viruses were set to go off when '123' was typed. Since many systems used that sequence to start Lotus 1-2-3, any infected computer on which Lotus was regularly used was likely to have trouble with this virus. And it can be even worse. Even if a contaminated system appears to have been disinfected, there is a pernicious form of virus that can reappear to create fresh problems.

Destructive Non-Virus Programs

Aside from viruses, there are other threats to user systems, including:

- Worms
- Trojan Horses
- Logic Bombs

As well as being potentially destructive by themselves, each can also be used as a vehicle to propagate any virus.

Worms

Viruses are far from the only maverick programs that can disrupt a computer system. Worms are constructed to infiltrate legitimate data processing programs and alter or destroy the data. Often what people believe is a virus infection is, in fact, a worm program. This is not as serious because worms do not replicate themselves. But the damage caused by a worm attack can be just as serious as a virus, especially if not discovered in time. For example, suppose a worm program instructs a bank's computer to transfer funds to an illicit account. The fund transfers may continue even after the worm is destroyed. However, once the worm invasion is discovered, recovery is much easier because there is only a single copy of the worm program to destroy since the replicating ability of the virus is absent. This capability may enable it to re-infect a system several times. A worm is similar to a benign tumor while a virus is like a malignant one.

Trojan Horses

A Trojan Horse is a destructive program that has been disguised (or concealed in) an innocuous piece of software. Indeed, worm and virus programs may be concealed within a Trojan Horse. Trojan Horses are not viruses because they do not reproduce themselves and spread as viruses do.

The mythical story of the original Trojan Horse is well known. When Greek warriors concealed themselves in an

An Introduction to Computer Viruses (cont.)

attractive wooden horse and left it outside the gates of the besieged city of Troy, the Trojans assumed it was a friendly peace offering and took it in. The Greek warriors then leaped out and wreaked havoc. Trojan Horse software works on the same principle. A program may seem both attractive and innocent, inviting the computer user to copy (or download) the software and run it. Trojan Horses may be games or some other software that the victim will be tempted to try.

For example, members of the Inner Circle club (a group of hackers) once created a Trojan Horse chess program. They used it to play chess with the system operator who discovered they had broken into the Canadian mainframe computer he was guarding. The operator thought he had been clever in catching the hackers; what possible harm could be caused by playing chess with them? He was wrong. While the computerized chess match was in progress, the Trojan Horse software allowed the hackers to gain access to accounts of increasing importance. Another popular medium for Trojan Horses is attractive graphics programs which are posted on computer bulletin boards.

In another famous example of how Trojan Horse programs can do serious damage, a New Jersey executive copied a graphics enhancing program from a Long Island-based computer bulletin board. In short order, the executive discovered it was a Trojan Horse. Unfortunately, the discovery was made when the enclosed virus destroyed 900 files on his system. While it was wrecking these files, it notified the executive that something was amiss by displaying the message "Arf, arf! Got you!" on his monitor.

Trojan Horses are usually more subtle, especially when they are used for embezzlement or industrial espionage. They can be programmed to self-destruct, leaving no evidence other than the damage they have caused. A Trojan Horse is particularly effective for the common banking crime known as 'salami slicing' in which small sums unlikely to be noticed are sliced off a number of legitimate accounts and moved to a secret account being operated by the thief.

Logic Bombs

Writing a logic bomb program is similar to creating a Trojan Horse. Both also have about the same ability to damage data, too. Logic bombs include a timing device so it will go off at a particular date and time. The Michelangelo virus is embedded in a logic bomb, for example. Other virus programs often include coding similar to that used in logic bombs, but the bombs can be very destructive on their own, even if they lack the ability of the virus to reproduce. One logic bomb caused major problems in the Los Angeles water department's system.

Logic bombs are usually timed to do maximum damage. That means the logic bomb is a favored device for revenge by disgruntled former employees who can set it to activate after they have left the company. One common trigger occurs when the dismissed employee's name is deleted from payroll records. On one occasion, a student left a logic bomb timed to explode and wipe out his university's records well after he had collected his degree and was long gone. This example illustrates the pernicious nature of logic bombs which can be written literally decades before they explode.

The built-in delay has been used to hold software "hostage" until a ransom is paid. These ransom demands are usually announced via a message to the user warning them to "pay up and we will tell you how to turn off the bomb". Logic bombs can also be insurance for suppliers or consultants who set up a computer system, causing data to be destroyed if their bills are not paid. This threat was used when a Maryland library refused to pay for a system that did not function properly; fortunately the bomb was found

An Introduction to Computer Viruses (cont.)

before any data could be damaged. When trying to assess whether a computer system has fallen victim to a virus, logic bomb, worm or Trojan Horse, the key factor is whether the maverick program has the ability to reproduce. Only viruses can make copies of themselves and attach the copy to new files.

Types of Viruses

There are several different types of viruses that can infect PC systems, including:

- Boot sector viruses
- File infecting viruses
- Polymorphic viruses
- Stealth viruses
- Multi-partite viruses

Each is described in this section.

Boot Sector Viruses

Boot sector viruses are those that infect the boot sector (or master boot record) on a computer system. They first move or overwrite the original boot code, replacing it with infected boot code. They will then move the original boot sector information to another sector on the disk, marking that sector as a bad spot on the disk so it will not be used in the future. Boot sector viruses can be very difficult to detect since the boot sector is the first thing loaded when a computer is starts. In effect, the virus takes full control of the infected computer.

About three out of every four virus infections reported are boot sector viruses. The only way that a system can become infected with a boot sector virus is to boot using an infected floppy disk. This is most commonly done when a user leaves a floppy disk in a drive and reboots the system (with the drive door closed). Good anti-virus software will look for an infected floppy disk when a user boots from the floppy drive and before the boot strap is loaded.

File infecting viruses

File infecting viruses are, unsurprisingly, viruses that infect files. Sometimes these viruses are memory resident. However, they will commonly infect most, if not all of the executable files (those with the extensions .COM, .EXE, .OVL and other overlay files) on a system. Some file infecting viruses will only attack operating system files (such as COMMAND.COM), while others will attack any file that is executable.

Some of these viruses act like boot sector infectors. They replace the “program load” instructions in an executable file with their own instructions, and move the original program load instructions to a different part of the file. Happily, this usually increases the file’s size, making detection a little easier. Other file infecting viruses work by using companion files. They rename all files with .COM extensions to .EXE, then write a file with the same name and a .COM extension. This new file will usually have the “hidden” attribute, making it difficult to detect with ordinary file handling commands. By default, MS-DOS executes the .COM file before the .EXE file so that the .COM file is executed first, loading the virus.

Polymorphic viruses

Polymorphic viruses change their appearance with each infection. Such encrypted viruses are usually difficult to detect because they are better at hiding themselves from anti-virus software. That is the purpose of the encryption.

Polymorphic viruses take encryption a step further by altering the encryption algorithm with each new infection. Some polymorphic viruses can assume over two billion different guises. This means anti-virus software products must perform algorithmic scanning, as opposed to standard string-based scanning techniques that can find simpler viruses.

An Introduction to Computer Viruses (cont.)

Stealth viruses

Stealth viruses attempt to hide from both the operating system and anti-virus software. To do this, they must stay in memory so they can intercept all attempts to use the operating system (system calls). The virus can hide changes it makes to file sizes, directory structures, and/or other operating system aspects. Since part of the virus is memory resident, there will be less memory available to users. The virus must hide this fact as well as from both users and anti-virus software. Stealth viruses must be detected while they are in memory. Once found, they must be disabled in memory before the disk-based components can be corrected.

Multi-partite viruses

Multi-partite viruses are those that infect both boot sectors and executable files. They are the worst viruses of all because they can combine some or all of the stealth techniques, along with polymorphism to prevent detection.

How Viruses Affect (and Infect) Your System

Before you can safeguard your system against viruses, it's important to understand how they spread and what they do to infected systems. The best virus protection program is consistent, ongoing education of computer users about the virus threat. Even with the proliferation of on-line services and communications, most viruses are still spread via infected floppy disks. The front line in the war against viruses must be fought by the user who is about to put a disk into the drive. Without an effective, ongoing education campaign, virus fighting efforts will be doomed to lighting backfires against infections already in place.

How Viruses Spread

Here are four common scenarios that spread viruses:

© A user brings a game to work that his child downloaded from a local computer BBS. Without thinking, the user runs the game on the company network to show fellow workers how cool it is. Unbeknownst to this user, the game program was infected with a virus. Now the entire company network is infected, too.

© Software purchased from a retailer in shrink wrap is infected because the store re-wrapped some returned software without checking the disks for viruses. Unfortunately, the original buyer had tried the software out on an infected machine.

© An instructor distributes disks to students so they can complete a class assignment. One student decides to do his homework in the office at night. Unfortunately, the instructor was not vigilant and distributed infected disks to the entire class.

© A friend gives you a disk so you can try out a new graphics program. The infection on your friends machine spreads to yours when you run the program for the first time. (The nifty graphics available don't quite compensate for the three weeks you spend reconstructing your lost data files.)

Viruses are designed to proliferate and propagate. This means each and every contact between your system and any other system is an opportunity for infection. That can include floppy disks and contacts via modem (or other network connection). Be especially careful of users who frequently use a number of different systems outside your company. Three notorious examples are:

© Field service technicians;

© Salespeople who run demonstration programs on your system; and

© Outside auditors who use their disks in your system (or, in some cases, connect their notebook computers directly to your network).

A common myth is that diskettes formatted as non-system disks cannot carry viruses. This is false since any disk can contain an executable file. Even more important, non-system disks can still carry boot sector viruses. Eternal vigilance is the only protection against infections!

Unauthorized users breaking into your system can easily wreak havoc by planting viruses directly in the most sensitive locations. One common path into a system is through a trapdoor.

Trapdoors

Viruses, worms, trojan horses, logic bombs and other hostile programs are no threat as long as they are kept out of a computer system. Unfortunately, lax computer security is the rule rather than the exception. Lack of security allows hackers to infiltrate systems with comparative ease.

A San Francisco consultant told us that she was given a password into the system of a leading telecommunications

How Viruses Affect (and Infect) Your System (cont.)

company so that she could carry out a project. She found that the same password still gave her access to the system over two years later. If a hacker discovered the password, it would have been the equivalent of owning the combination to the office safe. After the internet virus scare the company finally started using systematic, regular audits, including frequently changing passwords.

Unfortunately, passwords often are not even needed to get access to many systems. A worm or virus can be slipped in through a trapdoor. A trapdoor is a way of accessing a program or network without entering passwords or going through other security procedures. Trapdoors exist because programmers are lazy. When testing a piece of software, the programmer often doesn't want to bother going through the security procedure every time they start the program. Therefore, the programmer builds a trapdoor into the system so they can go directly into the software without entering bothersome passwords. The programmers usually intend to remove the trapdoors before the software is shipped. Sometimes, intentionally or not, they don't, giving free access to anyone who knows how to get through the trapdoor. The trapdoor can perform an invaluable role in its original guise as a set of coded instructions that permit easy direct access to a system's software or operating system. To be effective, it needs to bypass the security routines so that it can be used to fix problems, upgrade the system or run tests at any time.

Hackers have also created trapdoors after they have gained access to a system so that they can conveniently get back into it again. A typical hacker trapdoor gives access to a secret account that he leaves dormant as insurance to return if he is discovered and kicked off the system.

The most famous trapdoor was described in the movie War Games. The discovery of Joshua (the name used to access the trapdoor) set off a chain of incidents threatening a nuclear holocaust. Fortunately, most trapdoors don't have quite that much destructive capability! Real-life trapdoors are used both legitimately and illegally to get into hundreds of thousands of systems. Indeed, most large computers have had such doorways created in them as a routine when the systems were set up. They are very difficult (sometimes nearly impossible) to detect.

Joshua was left in a Defense Department computer used to simulate strategic crises. A young hacker (played by Matthew Broderick) discovered that he could access the system by typing the word Joshua to open the trap. When he tampered with data, the war game started to become a reality. Trapdoors are sometimes created by employees so they can see what their supervisors are doing. Discovering (or planting) a trapdoor in a high level user's activities can provide access to financial records, personnel information, or other very sensitive data. Valuable proprietary software was copied by a group of engineers in Detroit who found a trapdoor in a Florida system that they could open at will via a simple modem connection. Trapdoors are a powerful, secret tool of industrial espionage. Their presence in any system makes it particularly vulnerable to computer viruses and other destructive programs.

The internet virus got into networks in the U.S. through a trapdoor in a piece of common electronic mail software. The programmer had left the trapdoor so he could gain quick access to fine-tune his program code. He said he created the trapdoor because an administrator would not give him access to the program he had written.

The Real Value of Computers: Software and Data Files

The real value of computers is the software, the programming and the data created and processed with programs and mental skills. Some futurologists predict that we are approaching the situation where computer hardware will be virtually given away. If that day comes, our investment in computing will be entirely in software, especially data files. Even today the typical computer user has reached the point where the data captured on his system is far more valuable

How Viruses Affect (and Infect) Your System (cont.)

than the hardware that stores and processes it.

We need to remember this definition of value when considering the problems created by viruses. Insurance company actuaries have already done the calculations. They will gladly quote you rates to replace your hardware if it is lost, stolen or destroyed but will usually simply refuse to quote you any realistic premium for damage resulting from the loss of data caused by a virus infection.

Any competent technician can take an infected system and make the hardware functional; it's a trivial matter to clean viruses from disks. But this may be irrelevant to the real problem. Imagine a dead body brought back to life with its memory wiped clean. It's not much use to anyone. Similarly, the value of a computer system lies in its store of knowledge and its capacity to perform tasks. One can always buy a replacement machine, but there are no convenient retail stores that can sell you the data wiped out by a virus.

System Components That Can Be Affected

Any target for a virus infection must have two characteristics:

- It must be an executable file.
- It must be stored on a write-enabled disk.

The simple act of write-protecting floppy disks by covering the notch in 51/2" disks or opening the hole in 31/4" disks can prevent many virus infections. Unfortunately, if you copy executable files from this disk to a hard disk or network server, you will have undone all the good work you did by write-protecting the disk. Preventing software from writing to a disk is only the first step. Scanning the disk for viruses is the essential second step.

Viruses can hide in a number of places on a disk. If a virus simply attaches itself to an executable file stored on a hard or floppy disk, the file size will change, making it a straightforward matter to detect the virus. (Another file characteristic, the checksum, will also change. A checksum adds up various file characteristics to produce a hexadecimal number. If you know what this number should be, you can test to see if the file has changed. Unfortunately, smart viruses will record the original checksum and report it when you test your program, rendering this test null and void. Simply looking for infected files will only detect viruses that aren't smart enough to disguise themselves.

Viruses that locate in the logical drive boot strap program are somewhat more difficult to find. Another possible location is right next door on the first physical sector of the hard disk, commonly called the fixed disk partition table (or file allocation table, abbreviated FAT).

Finally, the virus may modify DOS directory entries and install a copy of itself in the directory that executes when other programs are run. These linked viruses change directory listings so the virus can hide itself from simple directory display commands.

The scope and variety of hiding places and infiltration methods means anti-virus software must be quite sophisticated. Simply scanning for executable files whose size has been changed since the last scan is not sufficient. Hidden files, system files and areas of the disk normally invisible to software must be explored. And anti-virus software alone will not do the job. Ongoing employee education and training must be an essential part of any program aimed at improving the safety of company data.

How Viruses Affect (and Infect) Your System (cont.)

The Real Virus Threat

Skepticism about viruses is natural. Many people have never seen any damage caused by a virus. Often even those who regularly use virus scanning software have never seen one. Is the virus threat real or is it just a hoax perpetrated by those who want to sell anti-virus software?

There are viruses out there and they are real threats. Professor Tony Lima (California State University, Hayward) routinely hands out floppy disks containing assignments in some of his courses. When these disks are returned, he always scans them for viruses. He estimates that between 3 and 5 percent of all returned disks contain a virus. In one case, he found the Michelangelo virus on a disk and warned the student who had used it. She suddenly looked very frightened because she had done the assignment on a computer attached to her company's network. The disk had been infected from the network. Fortunately, the problem was found in time to correct the potentially disastrous situation. The company has since implemented a virus protection system.

The University, however, was not immune. About six months after the incident reported above, Prof. Lima discovered that the network at the California State University, Hayward satellite campus in Concord, California was infected with the 'Stoned' virus.

The real problem is that once a virus is released into the computing world, it remains a threat as long as there is one copy remaining anywhere. The very nature of viruses (their ability to reproduce and spread) means one copy of a virus can turn into millions. By some estimates, there were about 4,000 viruses in existence at the end of 1994. Since the first document virus attack was in 1987 at the University of Delaware, the proliferation of viruses has been truly phenomenal; the figures in this paragraph imply a growth of 227% per year.

Where, then, are all the virus attack stories? Even though companies are (understandably) reluctant to discuss their experiences with viruses in public, one would still expect to read about several major incidents each year. The obvious answer is that the virus protection industry is its own worst enemy. By publicizing new viruses as they are discovered (but before they are widely spread), anti-virus software companies raise corporate awareness. Many businesses undoubtedly take action before the logic bomb date; there is no data whatsoever on the number of companies whose data has been saved by this publicity.

For example, in 1990 doom and destruction were forecast. The expected cause was the Michelangelo virus. The logic bomb date arrived and departed without much happening. The press declared the entire event a hoax. However, there is a second possible explanation: the volume of warnings motivated companies to take appropriate action in advance, eliminating the potential disaster by implementing preventive techniques.

In 1993, Information Week surveyed readers about viruses. Over half (58%) reported they had experienced some direct effect from a virus in the preceding 12 months. One in twenty respondents (5%) stated that viruses had infected over half their computers. Viruses are out there and ready to invade your system with no warning.

What Should You Do to Protect Your System?

Different organizations have different styles of operation. This fact extends to the ways they set up their computer networks and operating procedures. That makes it impossible for any document to set down a detailed set of procedures that can be used to cover each and every organization subject to virus attack. After all, you would not expect the same procedures to apply to the American Red Cross that work for General Electric. G.E.'s procedures are not appropriate for McAfee Associates either.

This white paper is intended to be a brief introduction to viruses. Entire books have been written on the subject. Here are two that contain detailed recommendations for setting up anti-virus procedures in different types of organizations:

Robert V. Jacobson, *Using McAfee Associates Software for Safe Computing* (1992), International Security Technology, Inc., 515 Madison Ave., New York, NY 10022. ISBN 0-9627374-1-0.)

John McAfee and Colin Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System* (1989 St. Martin's Press, New York, NY ISBN 0-312-02889-X).

Fortunately, there are some procedures that apply to any organization. Any good virus defense system must include:

- An ongoing training and education program for users
- Systematic use of anti-virus software
- A record-keeping system to identify ongoing weak points in the system.

The system you implement will depend strongly on the nature of your organization and its operating procedures, both for computers and people. If your computer operations consist of one or two personal computers used by five or fewer people, you probably will not need an elaborate defense system. But if your system is larger–up to and including the world-wide networks used by large corporations you need a detailed, systematic defense system.

Security Procedures

What factors should you consider when designing security appropriate to your operation? Jacobson suggests five areas of consideration:

1. The number and density of personal computers

If your company has many PCs or if there is a high ratio of computers to employees, your procedures should be more formal and extensive.

2. The extent to which computers are interconnected

Note that interconnection does not have to be via a network. If data is routinely moved from one computer to another via "sneaker net" (copying to a floppy disk and walking it across the room to the other computer), your computers are interconnected. The factor you must consider is the extent to which data is moved between computers, not the number of feet (or miles) of wire connecting them.

3. The number of locations where computers are used

To the extent that computers are physically located at a distance, more people will have to coordinate their security activities. In addition, they will have to agree on what procedures are appropriate. Remember, coordination problems increase in proportion to the square of the number of people involved.

4. The pace of operations

Some businesses simply operate at a faster pace than others. Examples include security brokerage houses, travel

What Should You Do to Protect Your System? (cont.)

agents and airline reservation operations. All other things being equal, a currency trading unit will work at a faster pace than a research laboratory. The faster the pace of operations the greater the degree of protection required because the rate at which new data is generated is proportional to the pace of operations. More data equals greater risk!

5. On-line real-time operations

If a PC-based network is used to support an on-line operation, the highest possible level of anti-virus security is necessary. For example, suppose the LAN is used to capture data recorded from a technical support operation. Telephone calls come in and the information from them is logged by technical support people typing much of the information into their computers. There is one (and only one) chance to capture the data. Even daily backup procedures are not sufficient to protect this irreplaceable database.

Naturally, this list is not exhaustive. Other questions to consider include:

-If there are a large number of PCs in the organization, are there some that should not be included in the anti-virus operation?

-What special procedures should be used for the company network?

-Exactly how will user reports of virus infections be recorded and processed? In very large organizations, it may be necessary to establish a help desk to handle these reports.

-What records of virus infections and anti-virus procedures should be maintained? Who should keep them? (Itís important to log the routine anti-virus scans as well as the infections themselves.)

-Who will create and maintain the virus control policy and procedures manual?

-What schedule should be adopted for initial implementation of the virus control program?

-Who will provide the funding for staff, development and software?

Here are some simple prevention rules that everyone who uses personal computers should know and understand:

1. Any floppy disk should be write-protected before it is inserted in a disk drive. Cover the notch in 51/4” disks with a write protection tab. Slide open the write-protect window on 31/2” disks.

2. Once the disk is write-protected, scan it for viruses before doing anything else.

3. If people routinely work on their computers at home, insist that they follow the same procedures there that they do in the office. However, disks brought from their home computer should still be treated as foreign disks, following steps 1 and 2.

4. Report any suspicious behavior. If routine tasks suddenly cause unexpected results, a scan for viruses should be one of the follow-up procedures.

5. If files are routinely downloaded from computers outside the company, they should be downloaded directly to floppy disks if possible. If the files are too large or downloads too frequent to make that feasible, an isolated computer (one not connected to the company network in any way) should be used to store downloaded files. Those files should be off-limits to the rest of the organization until they have been thoroughly scanned for viruses.

What Should You Do to Protect Your System?(cont.)

(If compressed files are downloaded, they should be decompressed before scanning.)

6. Establish and maintain a virus-free environment. Only when you are certain that your current computing environment has no viruses can you begin to control future infections.

7. If possible, dedicate a computer to virus control. This computer is designated as the one that will be used to handle all incoming data. (Ironically, this means the virus control computer is most likely to be infected from time to time.)

8. Develop an and use consistent routines for backing up data.

Note that if a virus is included with other files on a back-up tape, that tape is effectively useless. Therefore, the practice of rotating tapes for backup purposes may simply cause clean data to be replaced by infected data. Make an archive copy at least once a month, more often if the nature of your data indicates that is appropriate. That archive copy should be kept forever–or at least until after the next anti-virus sweep is performed.

Anti-Virus Software

Software is only one piece of the war against viruses. However, it is an essential component.

Anti-virus software must be able to perform three tasks:

-Test files and directories for the presence of viruses.
-Clean infected files
-Provide ongoing real-time protection against memory resident viruses.

McAfee makes software available to handle each of these jobs. VirusScan will scan one (or many) logical disk drives as well as the current memory for viruses. Currently, VirusScan 2.1 catches 97% of all known viruses, as well as providing advanced protection against those viruses that have not yet been cataloged. By using the /CLEAN switch, most viruses can be eliminated from infected systems; no additional software is necessary to clean up. And Vshield provides ongoing, continuous protection because it remains memory resident, examining files before they are run and preventing virus infections from spreading. VirusScan is distributed as shareware and is available for downloading from many computer BBS systems, directly from McAfee's own BBS, on CompuServe and most other commercial providers and via internet ftp. Specific addresses and telephone numbers are included at the end of this document.

McAfee also publishes more advanced anti-virus hardware and software. RomShield provides hardware level protection against boot sector viruses. It replaces the boot ROM chip found on most Ethernet adapters. This means RomShield is loaded before the boot sector of any disk is accessed, providing the most advanced protection against boot sector viruses that is possible. NetShield protects Novell networks. Since NetShield is installed and runs entirely from network servers, it is the ideal tool for network administrators who must manage local (or wide) area networks. No installation on local workstations is required, allowing administrators to enable virus protection from their offices.

What Are The Implications For System Administrators?

Implementing a virus defense procedure is an integral part of any system administrator's job. These procedures should be integrated with other routine chores such as backing up the network server(s). Scans for viruses should be performed regularly using good anti-virus software. Since new viruses appear at unpredictable intervals and old viruses mutate, it is important to update your software regularly. VirusScan 2.1 includes optional software that will automatically call the McAfee computer, download updated software and install it in your system.

Sources of Information and Software

Patricia Hoffman's VSUM

Patricia Hoffman's VSUM is a database and catalog of over 2,500 known viruses and variants. It contains detailed information on viruses, where they were first encountered, what effect the virus might have on a system, as well as the size and any specific characteristics this virus might contain. VSUM can be downloaded from several on-line services, or from her BBS at (408) 244-0813.

The National Computer Security Association (NCSA)

The National Computer Security Association (NCSA) is the leading membership organization providing educational materials, training, testing and consulting to help users improve computer and information security, reliability and ethics.

The NCSA also maintains an extensive library of viruses which it will make available to qualified reviewers and virus researchers. Please contact Robert Bales, Executive Director of the NCSA for additional information regarding this library. The NCSA can be reached at:

National Computer Security Association
10 South Courthouse Avenue
Carlisle, PA 17013
Phone: (717) 258-1816
Fax: (717) 243-8642

Email: 75300.2557@compuserve.com
CompuServe: GO NCSAFORUM

McAfee

VirusScan is available for downloading from many computer bulletin boards. However, if a BBS sysop is not diligent, one or more of the files in the VirusScan package may be infected. Only download anti-virus software from well-maintained BBS systems. If you have any doubts about a BBS, you can obtain the shareware version of VirusScan directly from McAfee at one of the following locations:

BBS: (408) 988-4004

8 data bits, 1 stop bit, no parity (8N1). Up to 14,400 baud. Log on as first name guest, last name user

CompuServe: GO MCAFEE

Internet file transfer protocol (ftp): ftp to mcafee.com, log in using anonymous or ftp as your user ID, and use your e-mail address as the password. Programs are located in the pub\antivirus directory.

Questions (including information about other ftp sites) should be directed to support@mcafee.com.