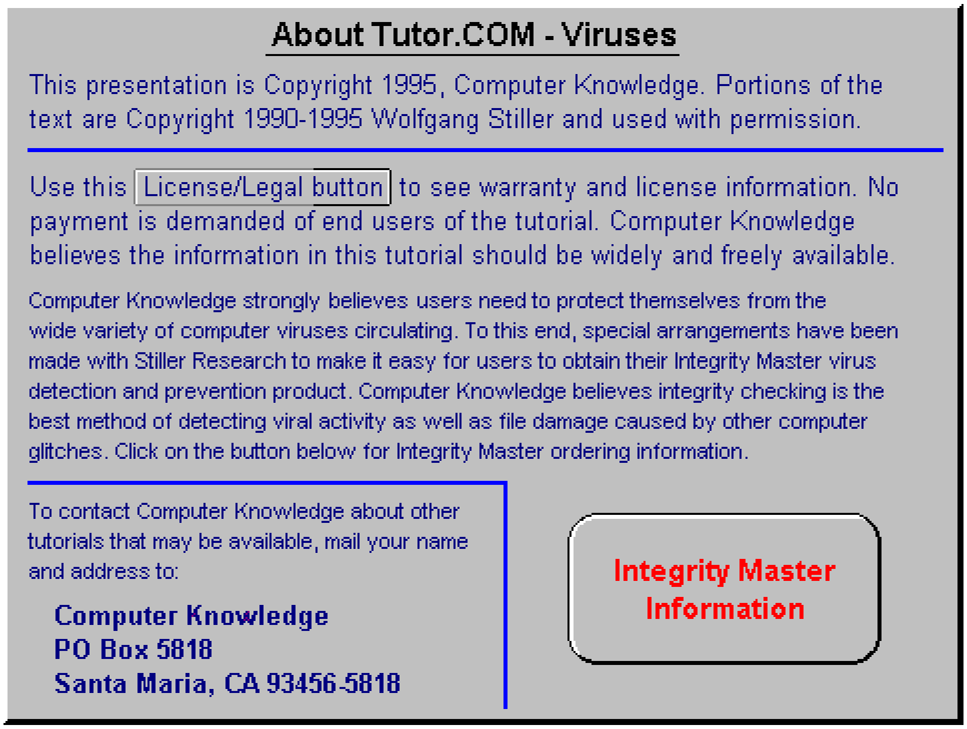
Contents

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

For Help on navigating, Press F1

Close



About Tutor.COM - Viruses

Use this License/Legal button to see warranty and license information. No payment is demanded of end users of the tutorial. Computer Knowledge believes the information in this tutorial should be widely and freely available.

Computer Knowledge strongly believes users need to protect themselves from the wide variety of computer viruses circulating. To this end, special arrangements have been made with Stiller Research to make it easy for users to obtain their Integrity Master virus detection and prevention product. Computer Knowledge believes integrity checking is the best method of detecting viral activity as well as file damage caused by other computer glitches. Click on the button below for Integrity Master ordering information.

To contact Computer Knowledge about other tutorials that may be available, mail your name and address to:

Computer Knowledge
PO Box 5818
Santa Maria, CA 93456-5818

Version 1.0 — October 1995

Summary

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

The material below is a quick and dirty summary. There are a number of pop-up links for items you may not completely understand. To fully understand the topics in the tutorial, however, you really need to go completely through the Full Tutorial section of this file.

What is a virus?

Basically, a virus is a computer program that is able, with your help and by attaching itself to other programs, to move from computer to computer. Typically, these programs are often harmful and not beneficial (although technically they could be).

A virus is not the only way you can experience problems with your computer; indeed, for most people, hardware or software problems are far more common. The Full Tutorial section of this file contains a detailed discussion of some of these.

There are several classes of code often grouped under the name "virus." Not all are viruses in the classic meaning of the term. Some of these are: worm, Trojan Horse, logic bomb, and others. The thing to remember is that a virus moves from computer to computer by attaching itself to a program, including the small program that exists in the boot sector of every floppy or hard disk, bootable or not.

For most viruses, when the program with the virus is run, the viral code goes into memory and stays there for as long as the computer is turned on; even if you warm boot the computer with Ctrl-Alt-Del. To spread itself, it first attaches itself to other programs or other disks as they are accessed. Then, if the circumstances are correct for the particular virus, it activates and does whatever damage it was programmed to do. This may range from a simple message to complete erasure of your disk.

Anti-Viral Steps

Since new viruses are being developed every day with different ways of hiding themselves and working there is no way to absolutely guarantee you will never see one. There are, however, several easy steps you can take to minimize your exposure.

- Test your system with a new version of an anti-virus program. Start the computer with a known-clean boot floppy disk so you know there are no viruses in memory.

- Use the anti-virus program to clean your system if found to be infected.

- Don't forget to check all disks you use in your computer (floppy, hard, and removable).

Now that you have a clean system. . .

- Every time you start your computer run the DOS CHKDSK program (put it in your AUTOEXEC.BAT file) and note if anything has changed, particularly the amount of available memory.

- When you put a new floppy disk into your computer's drive, use an anti-virus program to scan the disk; even if it's a data disk with no programs on it. If you don't plan to write to the disk, make certain it is write-protected.

- If connected to a network and receive electronic mail with executable programs attached never run one of the programs without first checking it for viruses using an up-to-date scanner.

These steps will help assure the computer stays clean. Again, no guarantees, but reasonable precautions will go a long way to help.

Absolute Protection

Nothing is absolute but if you want to go one step beyond the above steps you can do so with integrity checking. Applied properly this method gives you excellent protection.

Integrity checking starts with a clean system. This is important. The program that controls the checking then examines each file on your hard disk vulnerable to infection (some check all files) and uses sophisticated mathematical techniques to generate one or more checksums unique to each file. These checksums are stored as a record of the file's signature when it was known to be clean from viruses. Signatures also extend to the important areas of the disk (e.g., boot sector). On checking, the system is powered up and the integrity program is run. It again computes checksums for each file and then compares these with the checksums previously recorded. Any changes are noted and reported. The program then helps you determine if the changes are expected or possibly due to infection. This method will find even unknown and new viruses.

Next ▷

Full Tutorial

Full Tutorial

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

This tutorial covers the basics of both hardware and software threats, with a concentration on viruses. You can navigate to major section headers via the links below:

About...
Computer Threats

Computer Threats

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Do you have data or programs on your PC which you can't afford to have unexpectedly damaged? How can you make sure that your data is safe? To protect the integrity of your data, you must first understand the nature of the threats against it. You might be surprised to find there are more than you might imagine.

The most publicized threats to your computer are software-based attacks often lumped together as "viruses" by the media. Although viruses are often over-sensationalized by media coverage, they do present a very real menace to your data (discussed in Virus Threats). Even if a virus never attacks your PC, it is almost inevitable that system glitches will someday corrupt data or programs on your PC. Considering that viruses are but one threat to your data, and not the most likely threat by far, it's ironic that so many people have anti-virus software but so few people take steps to protect the integrity of their programs and data from other hazards. Can anyone afford ***not*** to know that each and every byte on their disk is undamaged?

So what's the explanation? Why do so few people take steps to assure the integrity of the data on their PC? The main reason is that data integrity gets almost no media coverage, (even in the trade journals), while a virus story may make the local evening news. The result is that people just don't give data integrity a second thought. It's all too easy to take the reliability of our modern PCs for granted—and, as you'll see, all too dangerous!

You may be reading this primarily because you're interested in viruses. If that's true, then, for you, the media attention to viruses will have had a very beneficial effect. You will learn about other threats and how to protect your PC against much more than just viruses! Data integrity is not a very glamorous subject, yet it's both crucial and fundamental to using any computer. Without positive assurance of data integrity, computers cannot be depended upon to process any type of important data. How would you respond if someone were going to change a byte of data somewhere at random on your disk? You'd be pretty upset right? Well, the odds are, it has already happened but you were not aware of it. Perhaps the result was that a program quit working or CHKDSK found lost or cross-linked clusters. Or perhaps, if you're lucky, the damage was to some inconsequential part of your disk.

Let's explore the different threats to your files and programs. . .

- **Hardware Threats**
- **Software Threats**
- **Virus Threats**

Go Back

Full Tutorial

About...

Ways to Combat Threats

Hardware Threats

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Hardware problems are all too common. We all know that when a PC or disk get old, it might start acting erratically and damage some data before it totally dies. Unfortunately, hardware errors frequently damage data on even young PCs and disks.

◆ **Power Faults**

Your PC is busy writing data to the disk and the lights go out! "Arghhhh!" Is everything OK? Maybe so, maybe not; it's vital to know for sure if anything was damaged.

Other power problems of a similar nature would include brownouts, voltage spikes, and frequency shifts. All can cause data problems, particularly if they occur when data is being written to disk (data in memory generally does not get corrupted by power problems; it just gets erased if the problems are serious enough).

◆ **Age**

It's not magic, as computers age they tend to fail more often. Electronic components are stressed over time as they heat up and cool down. Mechanical components simply wear out. Some of these failures will be dramatic; something will just stop working. Some, however, can be slow and not obvious. Regrettably, it's not a question of "if", but "when" in regard to equipment failure.

◆ **Incompatibilities**

You can have hardware problems on a perfectly healthy PC if you have devices installed that do not properly share interrupts. This problem is getting more and more frequent as we see multiple adapters installed in a PC that use the same interrupt (IRQ). Sometimes problems are immediately obvious, other times they are subtle and depend upon certain events to happen at just the wrong time, then suddenly strange things happen!

◆ **Finger Checks** (*Typos and "OOPS! I Didn't mean to do that!"*)

These are an all too frequent cause of data corruption. This commonly happens when you are intending to delete or replace one file but actually get another. By using wild cards, you may experience a really "wild" time. "Hmmm I thought I deleted all the *.BAK files—but they're still here—something was deleted—what was it?—or was I in the other directory?" Of course if you're a programmer or if you use sophisticated tools like a sector editor, then your fingers can really get you into trouble!

◆ **Malicious or Careless Damage**

Someone may accidentally or deliberately delete or change a file on your PC when you're not around. If you don't keep your PC locked in a safe, then this is a risk. Who knows what was changed or deleted? Wouldn't it be nice to know if anything changed over the weekend? Most of such damage is done unintentionally by someone whom you probably know. This person didn't mean to cause trouble; they simply didn't know what they were doing when they used your PC.

- **Typhoid Mary**

One major source for computer infections is the Customer Engineer (CE), or repairman. When a CE comes for a service call, they will almost always run a diagnostic program from diskette. It's very easy for these diskettes to become infected and spread the infection to your computer. Sales representatives showing demonstrations via floppy disks are also possibly spreading viruses. Always check your system after other people have placed their floppy disk into it.

- **Magnetic Zaps**

Computer data is generally stored as a series of magnetic changes on disks. While hard disks are generally safe from most magnetic threats because they are encased within the computer compartment, floppy disks are highly vulnerable to magnets. The obvious threat would be to post a floppy disk to the referigerator with a magnet; but there are many other, more subtle, threats.

More Info

Bottom line: There are tools to assist in recovery from disk problems, but how do you know all the data is OK? These tools do not always recover good copies of the original files. Active action on your part ***before*** disaster strikes is your best defense.

About... Computer Threats

About... Software Threats

Magnetic Threats

About...

Some of the more subtle sources of magnetism include:

- **Computer Monitor**
  Don't put floppy disks anywhere near the monitor as it generates a magnetic field.

- **Telephone**
  When ringing, telephones (particularly older phones with a bell) generate a magnetic field.

- **Bottom Desk Drawer**
  While the desk drawer does not generate a magnetic field, the vacuum cleaner that the maintenance people slide under the desk to clean the floor does.

- **Bottom Bookcase Shelf and File Cabinet Drawer**
  Same comment as the desk drawer just above.

- **Pets**
  Pet fur generates a strong electrostatic charge which, if discharged through a disk, can affect files on the disk. Instead of "The dog ate my homework," today it could just as easily be: "The cat sat on my homework."

Software Threats

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Software threats can be general problems or an attack by one or more types of malicious programs.

- **Software Problems**

This category accounts for more damage to programs and data than any other. We're talking about non-malicious software problems here, not viruses. Software conflicts, by themselves, are much more likely threats to your PC than virus attacks.

We run our PCs today in a complex environment. There are many resident programs (TSRs such as a Mouse driver) running simultaneously with various versions of DOS, BIOS and device drivers. All these programs execute at the same time, share data and are vulnerable to unforeseen interactions between each other. Naturally, this means that there may be some subtle bugs waiting to "byte" us. Anytime a program goes haywire, there's the risk it may damage information on disk.

There's the further problem that not all programs do what we hope they will. If you have just undeleted a file, you don't really know if all the correct clusters were placed back in the right order. When CHKDSK "fixes" your disk for you, you have no way of knowing exactly what files it changed to do its job.

Software problems happen and can be very serious if you have not taken appropriate action ***in advance*** of the problem.

- **Software Attacks**

These are programs written deliberately to vandalize someone's computer or to use that computer in an unauthorized way. There are many forms of malicious software; sometimes the media refers to all malicious software as viruses. It's important to understand the distinction between the various types.

- Logic Bombs
  Just like a real bomb, a logic bomb will lie dormant until triggered by some event.

- Trojans
  These are named after the Trojan horse, which delivered soldiers into the city of Troy.

- Worms
  A worm is a self-reproducing program that does not infect other programs as a virus will, but instead creates copies of itself, that create even more copies.

- Viruses
  An entire topic has been dedicated to this threat.

About...
Computer Threats

About...
Virus Threats

Virus Threats

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Viruses are a cause of much confusion and a target of considerable misinformation even from some virus "experts." Let's define what we mean by virus:

> A virus is a program that reproduces its own code by attaching itself to other programs in such a way that the virus code is executed when the infected program is executed.

You could probably also say that the virus must do this without the permission or knowledge of the user, but that's not a vital distinction for purposes of our discussion here.

Most viruses do their "job" by placing self-replicating code in other programs, so that when those other programs are executed, even more programs are "infected" with the self-replicating code. This self-replicating code, when triggered by some event, may do a potentially harmful act to your computer. Viruses are initially distributed in the form of a trojan. In other words, the virus code has been planted in some useful program. Since the virus infects other useful programs, absolutely any piece of executable code will suddenly become a trojan delivery vehicle for the virus.

Another way of looking at viruses is to consider them to be programs written to create copies of themselves. These programs attach these copies onto other programs (infecting these programs). When one of these other programs is executed, the virus code (which was attached to that program) executes, and links copies of itself to even more programs.

General Virus Behavior

Viruses come in a great many different forms, but they all potentially have two phases to their execution, the infection phase and the attack phase:

Infection Phase: When the virus executes it will infect other programs. What's often not clearly understood is precisely ***when*** it will infect the other programs. Some viruses infect other programs each time they are executed; other viruses infect only upon a certain trigger. This trigger could be anything; a day or time, an external event on your PC, a counter within the virus, etc. This brings up an important point which bears repeating:

> **It is a serious mistake to execute a program a few times - find nothing infected and presume there are no viruses in the program. You can never be sure the virus simply hasn't yet triggered its infection phase!**

More Info

Attack Phase: Many viruses do unpleasant things such as deleting files or changing random data on your disk, simulating typos or merely slowing your PC down; some viruses do less harmful things such as playing music or creating messages or animation on your screen. Just as the virus's infection phase can be triggered by some event, the attack phase also has its own

trigger.
About...

There are several categories of viruses:

- **System Sector Viruses**
- **File Viruses**
- **"Data" File Viruses**
- **Companion Viruses**
- **Cluster Viruses**
- **Polymorphic Viruses**
- **Stealth Viruses**
- **Fast and Slow Infectors**
- **Sparse Infectors**
- **Armored Virus**

Finally, we'll end the initial discussion with some general comments.

- **Number of Viruses**
- **How Serious Are Viruses?**

About...
Computer Threats

About...
Ways to Combat Threats

Infection Phase

About...

Modern viruses have become more selective about when they infect programs. Being selective improves the virus' chance to spread; if they infect too often, they will tend to be detected before they have enough time to spread widely. Virus writers want their programs to spread as far as possible before anyone notices them.

Many viruses go resident in the memory of your PC in the same way as terminate and stay resident (TSR) programs. This means the virus can wait for some external event before it infects additional programs. The virus may silently lurk in memory waiting for you to insert a diskette, copy a file, or execute a program, before it infects any other programs. This makes these viruses more difficult to analyze since it's hard to guess what trigger condition they use for their infection. Resident viruses frequently corrupt the system software on the PC to hide their existence. This technique is called stealth.

Attack Phase

About...

Viruses usually delay revealing their presence by launching their attack only after they have had ample opportunity to spread. This means the attack may be delayed for years after the initial infection. The attack phase is optional, many viruses simply reproduce and have no trigger for an attack phase. Does this mean that these are "good" viruses? No, unfortunately not! Anything that writes itself to your disk without your permission is stealing storage and CPU cycles. This is made worse since viruses that "just infect", with no attack phase, damage the programs or disks they infect. This is not an intentional act of the virus, but simply a result of the fact that many viruses contain extremely poor quality code. One of the most common viruses, the Stoned virus is not intentionally harmful. Unfortunately, the author did not anticipate the use of anything other than 360K floppy disks. The virus will try to hide its own code in an area of 1.2MB diskettes that results in corruption of the entire diskette.

System Sector Viruses

About...

System sectors are special areas on your disk containing programs that are executed when you boot your PC. Sectors are not files but simply small areas on your disk that your hardware reads in single chunks. Under DOS, sectors are most commonly 512 bytes in length. These sectors are invisible to normal programs but are vital for correct operation of your PC. They are a common target for viruses. There are two types of system sectors found on DOS PCs:

- **DOS Boot Sectors**
- **Partition Sectors**

System sector viruses modify the program in either the DOS boot sector or the partition sector. Since there isn't much room in the system sector (only 512 bytes), these viruses usually have to hide their code somewhere else on the disk. These viruses sometimes cause problems when this spot already contains data that is then overwritten. Some viruses, such as the Pakistani Brain virus, mark the spot where they hide their code as bad clusters. This is one reason to be alarmed if CHKDSK suddenly reports additional bad sectors on your disk. These viruses usually go resident in memory on your PC, and infect any floppy disk that you access. Simply doing a DIR on a floppy disk may cause it to be infected. Some viruses will infect your diskette immediately when you close the drive door. Since they are active in memory (resident), they can hide their presence. If Brain is active on your PC, and you use a sector editor to look at the boot sector of an infected diskette, the virus will intercept the attempt to read the infected boot sector and return instead a saved image of the original boot sector. You will see the normal boot sector instead of the infected version. Viruses that do this are known as stealth viruses.

In addition to infecting diskettes, some system sector viruses spread by also infecting files. Viruses of this type are called "multipartite" (multiple part) viruses. Since they can infect both files and sectors have more avenues to spread and are more difficult to remove.

File Viruses

About...

In terms of sheer number of viruses, these are the most common. The simplest file viruses work by locating a type of file that they know how to infect (usually a file name ending in ".COM" or ".EXE") and overwriting part of the program they are infecting. When this program is executed, the virus code executes and infects more files. These overwriting viruses do not tend to be very successful since the overwritten program rarely continues to function correctly and the virus is almost immediately discovered. The more sophisticated file viruses save (rather than overwrite) the original instructions when they insert their code into the program. This allows them to execute the original program after the virus finishes so that everything appears normal. Just as system sector viruses can remain resident in memory and use "stealth" techniques to hide their presence, file viruses can hide this way also. If you do a directory listing, you will not see any increase in the length of the file and if you attempt to read the file, the virus will intercept the request and return your original uninfected program to you. This can sometimes be used to your advantage. If you have a "stealth" virus (such as 4096 or Dir-2), you can copy your program files (*.EXE and *.COM files) to files with other extensions and allow the virus to automatically disinfect them! If you "COPY *.COM *.CON", and then cold boot your PC from a known good copy of DOS and "REN *.CON *.COM", this will disinfect the renamed files.

Some file viruses (such as 4096) also infect overlay files as well as the more usual *.COM and *.EXE files. Overlay files have various extensions, but ".OVR" and ".OVL" are common.

"Data" File Viruses

About...

As indicated throughout this tutorial, in order for a virus to do anything, first a program of some type must execute. A virus, not matter what type, is still a program and it must load into memory ***and*** run in order to do anything. Simply loading it into memory is not sufficient. Pure data files are not viruses simply because, by their nature, they do not execute.

The problem, however, is that some modern programs now contain some form of macro language; in some cases a very powerful macro language with commands that include opening, manipulating, and closing files. More and more, these programs allow a user to extend their capabilities by writing powerful macros and then attaching these to data files produced by that program. In many cases, in order to make things easy for users, the macros are set up to run automatically whenever the data file is loaded. It's in cases like this where the line between a data file and program start to blur.

Note: There are many triggers (other than loading the document) that viral code can exploit and, once running, various elements of the programs macro language can be exploited so that all future data files produced by that program version could contain the viral macro code.

Most scanners can be set to check every file instead of just files that normally execute; but most do not do this by default—that would make the scanning process too long for most people.

In order to know when to turn full scanning on you need to know something about the software you use. In particular, you need to make yourself aware of any software that uses the sort of "automatic macro" feature described here. Never use a piece of software until you've explored its manual for some time just to see what its full capabilities are. If these include some sort of "programming" (macro) language, be aware that there is an opportunity for problems there.

To protect yourself best you can also use integrity checking. While you may not be suspicious of detected changes to a file you just edited, you certainly should become suspicious if other files, not associated with the one you are editing, suddenly start to exhibit changes.

Stealth Viruses

About...

A virus, by its nature, has to modify something executable in order to become active when that executable is run. This might be a file, the boot sector, or partition sector (master boot record); but whatever it is, it has to change. Unless the virus takes over portions of the system in order to manage accesses to the changes it made, these changes will become visible and the virus will be exposed.

A stealth virus hides the modifications it makes. It does this by taking over the system functions which read files or system sectors and, when some other program requests information from portions of the disk the virus has changed, the virus reports back the correct (unchanged) information instead of what's really there (the virus). Of course, the virus must be resident in memory and active to do this.

Use of stealth is the major reason why most anti-virus programs operate best when the system is started (booted) from a known-clean floppy disk. When this happens, the virus does not gain control over the system and it is immediately available to be seen and dealt with.

Important Note: Some viruses, when they infect, encrypt and hide the original information in the sector they infect. If you are infected, some people may advise you to use generic DOS commands (e.g., SYS and/or FDISK /MBR) to correct the problem. If you do this you run the risk of making matters much worse. Monkey, for example, encrypts the partition information and moves it. If you overwrite the virus with FDISK /MBR then you will no longer be able to see your hard disk as DOS will not recognize what's in the partition table and can't access the encrypted version without Monkey helping.

> **Never use undocumented commands (e.g., FDISK /MBR) to fix virus contamination.** Always use an anti-virus package that can deal with the particular virus in question. Undocumented commands are undocumented for a reason!

Fast and Slow Infectors

About...

The term "fast" or "slow" when dealing with viruses pertains to how often and under what circumstances they spread the infection.

Typically, a virus will load itself into memory when an infected program is run. It sits there and waits for other programs to be run and infects them at that time.

A **fast** infector. on the other hand, infects programs not just when they are run, but also when they are simply accessed. The purpose of this type of infection is to ride on the back of anti-virus software to infect files as they are being checked. By its nature, anti-virus software (a scanner, in particular) opens each file on a disk being checked in order to determine if a virus is present. A fast infector that has not been found in memory before the scanning starts will spread itself quickly throughout the disk.

A **slow** infector does just the opposite. A slow infector will only infect files when they are created or modified. It's purpose is to attempt to defeat integrity checking software by piggybacking on top of the process which legitimately changes a file. As the user knows the file is being changed, they will be less likely to suspect the changes also represent an infection. By its nature (and because executable code is not usually changed) a slow infector does not spread rapidly and if the integrity checker has a scanning component it will likely be caught.

Companion Viruses

About...

Would you believe that a virus can infect your files without changing a single byte in the file? Well, it's true! The more common of two kinds is called the companion or spawning type virus. This virus infects your files by locating a file name ending in ".EXE". The virus then creates a matching file name ending in ".COM" that contains the viral code.

Here's what happens; let's say a companion virus is executing (resident) on your PC and decides it's time to infect a file. It looks around and happens to find a file called "WP.EXE". It now creates a file called "WP.COM" containing the virus. The virus usually plants this file in the current directory although it could place it in any directory on your DOS path. If you type "WP" and hit enter, DOS will execute "WP.COM" instead of "WP.EXE". The virus executes, possibly infecting more files and then loads and executes "WP.EXE". The user probably won't notice anything wrong. This type of virus is fortunately easy to detect by the presence of the extra ".COM" files. There are some instances where it is normal to have both ".COM" and ".EXE" files of the same name (such as DOS 5's DOSSHELL) but this is relatively rare.

Cluster Viruses

About...

There is a new type of virus known as a "cluster" virus that infects your files not by changing the file or planting extra files but by changing the DOS directory information so that directory entries point to the virus code instead of the actual program. When you type the name of the program, DOS loads and executes the virus code, the virus then locates the actual program and executes it. Dir-2 is an example of this type of virus.

This type of virus can cause serious problems if you don't know it's there. While the virus is in memory, it controls access to the directory structure on the disk. If you boot from a clean floppy disk, however, and then run a utility such as CHKDSK the utility will report serious problems with cross-linked files on your disk. Most such utilities will offer to correct the problem and users, not knowing any better, often accept the offer. Unfortunately, in the case of this virus type, if you accept the offer you will end up with all your executable files the same length and each one will be the virus code. Your original programs will be lost.

Polymorphic Viruses

About...

To confound virus scanning programs, virus writers created polymorphic viruses. These viruses are more difficult to detect by scanning because each copy of the virus looks different than the other copies. One virus author even created a tool kit for other virus writers to use called the "Dark Avenger's Mutation Engine" (also known as MTE or DAME). This allows someone who has a normal virus to use the mutation engine with their virus code. If they use the mutation engine, each file infected by their virus will have what appears to be totally different virus code attached to it. Fortunately, the code isn't totally different and now anyone foolish enough to use the mutation engine with their virus will be creating a virus that will be immediately detected by most of the existing scanners. The existing viruses (such as Pogue, Dedicated, CoffeeShop, CryptLab, and Groove) which use the mutation engine pose little threat since they are all simple minded and rather buggy.

Virus Tool Kits

Besides the mutation engine, there are now several tool kits available to help people create viruses. Several of these programs allow someone who has no knowledge of viruses to create their own "brand new" virus. One of these tool kits, known as the Virus Creation Laboratory (VCL), has a very slick user interface with pull down menus and on-line help. You just pick your choices from the various menus and in a flash you've created your very own virus. While this sounds like a pretty ominous development for scanning technology, it's not as bad as it sounds. All the existing tool kits (such as VCS, VCL and MPC) create viruses that can be detected easily with existing scanner technology. The danger with these tool kits lies in the fact that it's possible to create such a tool kit that could create viruses that really are unique. Fortunately, this hasn't been done yet, but it's only a matter of time before such a tool kit will be created. This will make scanning-based products useless; the only reliable way to detect these viruses will be with an integrity check product.

Number of Viruses

About...

There are more PC viruses than all other types of viruses combined (by a large margin). Estimates of exactly how many there are vary widely and the number is constantly growing. In 1990, estimates ranged from 200 to 500; then in 1991 estimates ranged from 600 to 1,000 different viruses. In late 1992, estimates were ranging from 1,000 to 2,300 viruses. In mid 1994, the numbers vary from 4,500 to over 7,500 viruses. The confusion exists partly because it's difficult to agree on how to count viruses. New viruses frequently arise from someone taking an existing virus that does something like put a message out on your screen saying: "Your PC is now stoned" and changing it to say something like "Donald Duck is a lie". Is this a new virus? Most "experts" say "yes." This is a trivial change that can be done in less than two minutes resulting in yet another "new" virus.

Another problem comes from viruses that try to conceal themselves from scanners by mutating. In other words, every time the virus infects another file, it will try to use a different version of itself. These viruses are known as polymorphic viruses. One example, the Whale (a huge clumsy 10,000 byte virus) creates 33 different versions of itself when it infects files. At least one person counts this as 33 different viruses on their list. Many of the large number of viruses known to exist have not been detected in the wild but probably exist only in someone's virus collection.

David M. Chess of IBM's High Integrity Computing Laboratory reported in the November 1991 Virus Bulletin that "about 30 different viruses and variants account for nearly all of the actual infections that we see in day-to-day operation." Now, about 38 different viruses account for all the viruses that actually spread in the wild. How can there be only 38 viruses active when some "experts" report such high numbers? This is probably because most viruses are poorly written and cannot spread at all or cannot spread without betraying their presence. Although the actual number of viruses will probably continue to be hotly debated, what is clear is that the total number of viruses is increasing rapidly, although perhaps not quite as rapidly as the numbers might suggest.

How Serious are Viruses?

About...

It's important to keep viruses in perspective. There are many other threats to your programs and data that are ***much*** more likely to harm you than viruses. A well known anti-virus researcher once said that you have more to fear from a cup of coffee (which may spill) than from viruses. While the growth in number of viruses now puts this statement into question, it's still clear that there are many more occurrences of data corruption from other causes than from viruses.

So, does this mean that viruses are nothing to worry about? Emphatically, no! It just means that it's foolish to spend much money and time on addressing the threat of viruses if you've done nothing about the other more likely threats to your files. Because viruses are deliberately written to invade and possibly damage your PC, they are the most difficult threat to guard against. It's pretty easy to understand the threat that disk failure represents and what to do about it (although surprisingly few people even address this threat). The threat of viruses is much more difficult to deal with. There are no "cures" for the virus problem. Why is this so? We'll explore this in the next section on Ways to Combat Threats.

Ways to Combat Threats

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

There are a number of ways to combat the various threats to your data. The tutorial discusses them in the order you would typically use them: problem detection, data protection, and recovery (assuming a problem has been found). You need to go through each of these to understand how they tie together. In some cases, you may not be able to recover damaged data if you have not first installed and used some of the protection techniques. Once data is overwritten, for example, there is no way to recover it unless you have a backup of some kind.

- **Detection Techniques**
- **Protection Techniques**
- **Recovery Techniques**

About... Computer Threats

About... Detection Techniques

Detection Techniques

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

A virus may or may not present itself. Viruses attempt to spread before activating whatever malicious activity they may have been programmed to deliver; but often there are symptoms that can be observed by a trained casual observer who knows what to look for. There are even DOS tools that can be a big help.

Virus authors usually place a wide variety of indicators into their viruses (e.g., messages, music, graphic displays). These, however, typically only show up when the virus payload activates. The unaccounted reduction of the amount of RAM known to be in the computer is an important indicator resident viruses have a hard time getting around. This can be detected by DOS tools.

Your first defense in detecting problems is to use the tools DOS has provided; not to fix the problems, just to detect them. CHKDSK, for example, is a good tool for detecting problems on your disk (and even some viruses) but not an extremely good tool for fixing them.

- **DOS Tools for Problem Detection**

Your second defense is aimed at detecting and identifying virus attacks to your computer. There are three mothods in general use. Each has pros and cons and are discussed via these links.

- **Scanning**
- **Interception**
- **Integrity Checking**
- **Guidelines for Using Anti-Virus Products**

Another line of defense is continuing education. Click below to see some sources of on-going information.

- **On-going Virus Infomation**

About...
Ways to Combat Threats

About...
Protection Techniques

DOS Tools for Problem Detection

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Probably the best general-purpose DOS utility you can run is CHKDSK. CHKDSK is a utility that checks the status of your disk drive(s) and memory in your computer. The report that CHKDSK produces (see below) is a good summary and contains information that can be used to make a fairly accurate quick diagnosis of both hardware/software error-caused damage and viral activity.

Run CHKDSK (or some equivalent program) regularly on each PC, and pay attention to the results. If you are seeing problems, be sure you understand what's causing the problems. If you are experiencing cross-linked or lost clusters, something is being damaged. Run an integrity checker to find out exactly what is being damaged. Also pay attention to the amount of available memory. If this suddenly changes with no new resident (TSR) software installed, you may have a virus. In particular, pay attention to the line that reports total memory in the system. This should almost never change.

A CHKDSK report looks something like that shown below. Pay close attention to the information in the lines marked as **bold red** text. It is the most likely to change under the influence of a virus.

```
        Volume VOL_LABEL    created Jun 5, 1994   7:14p
        Volume Serial Number is 0D35-1BEA

85,391,360   bytes total disk space          Total disk space
   139,264   bytes in 3 hidden files         Hidden file info
    22,528   bytes in 9 directories          Directory status info
11,409,408   bytes in 257 user files         User file info
73,820,160   bytes available on disk         Free space on disk

     2,048   bytes in each allocation unit   Size of each storage unit on
disk
    41,695   total allocation units on disk  Number of units on the disk
    36,045   available allocation units on disk      Number of units
available

   655,360   bytes total memory              Total RAM (only rarely
changes)
   549,152   bytes free                      Free RAM
```

In particular, when using CHKDSK, pay attention to the total RAM figure. On most machines it will show up as 655,360 bytes (640K). There are legitimate reasons for it to be otherwise. Some examples include:

- An IBM PS/2 computer typically reserves 1K of RAM for use as an extended BIOS area.

- Some computers with an American Megatrends, Inc. (AMI) BIOS can be set up to reserve 1K for internal variables.

- Sometimes a SCSI controller will reserve memory.

- A variety of other situations, too numerous to mention.

The point here is to use several up-to-date anti-virus programs to make certain your computer is free of viruses. Then run CHKDSK and see what it reports as total memory. Make note of that number. If that number changes, then become very suspicious.

Note: Do not run CHKDSK in a DOS box in Windows or other such program that controls the computer's environment. You can never tell if the results are due to outside influences or the environment program. You can solve this problem by simply putting CHKDSK early in your AUTOEXEC.BAT program so it runs as the starts up and before Windows (or other such program) starts.

About...
Detection
Techniques

CHKDSK

About...

CHKDSK is a transient DOS command first introduced in DOS 1.0. CHKDSK checks a disk and displays a status report for the current drive or on the specified drive (if no optional parameters are specified). For testing a disk it is always best to use CHKDSK without any parameters. That way, the command will tell you what it would do, but not make any changes to your disk.

The command format is:

CHKDSK [<d:><path>] [/F /V]

where

/V Option to display all checked files

/F Option to "fix" any errors that might be found

IMPORTANT: Do NOT use any version of CHKDSK from a version of DOS lower than that used to format the disk. Data may be damaged.

See your DOS manual for descriptions of the many possible error conditions CHKDSK may report. The most common will be lost clusters from files which have become damaged. The following error message indicates the problem:

```
#### lost clusters found in ### chains
Convert lost chains to files (Y/N)?
```

You are asked if you want the lost clusters converted to files. If you did not specify /F, "yes" or "no" will do nothing; if you did include /F CHKDSK will create file(s) in your root directory with the name FILE####.CHK, where #### starts at 0000 and increments. In most cases these files are worthless and can be deleted, freeing the disk space. At times a useful file (program or data) may be affected by this process; you may have to restore from backup.

Again, to repeat, it's best to use CHKDSK without any parameters and other programs to fix problems found, if any. CHKDSK has limited abilities to fix extensive damage as might be caused by a virus.

The DOS commands JOIN, SUBST, & ASSIGN affect CHKDSK. In addition, you should never use CHKDSK when in a DOS box with Windows running. Windows creates and keeps open temporary files that will report as errors in the CHKDSK display. If you attempt to fix these errors damage can be done to your disk.

A CHKDSK report looks something like:

```
Volume VOL_LABEL    created Jun 5, 1994   7:14p
Volume Serial Number is 0D35-1BEA
```

85,391,360	bytes total disk space	Total disk space
139,264	bytes in 3 hidden files	Hidden file info
22,528	bytes in 9 directories	Directory status info
11,409,408	bytes in 257 user files	User file info
73,820,160	bytes available on disk	Free space on disk
2,048	bytes in each allocation unit	Size of each storage unit on disk
41,695	total allocation units on disk	Number of units on the disk
36,045	available allocation units on disk	Number of units available
655,360	bytes total memory	Total RAM
549,152	bytes free	Free RAM

Note: In DOS 6.2 separators are used for numbers over 999 to make the output easier to read.

CHKDSK also reports bytes in bad sectors.

DOS 6.2 introduced the command SCANDISK which performs many of the same functions as CHKDSK. It is, however, more complete and gives better error messages. Use it instead of CHKDSK if you must use a DOS utility to fix disk problems.

Scanning

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Once a virus has been detected, it is possible to write programs that look for telltale code (signature strings) characteristic of the virus. The writers of the scanner then extract identifying strings from the virus. The scanner uses these signature strings to search memory, files, and system sectors. If the scanner finds a match, it announces that it has found a virus. This obviously detects only known, pre-existing, viruses. Many so-called "virus writers" create "new" viruses by modifying existing viruses. This takes only a few minutes but creates what appears to be a new virus. It happens all too often that these changes are simply to fool the scanners.

The major advantage of scanners is that they allow you to check programs before they are executed. Scanners provide the easiest way to check for new software for old (known) viruses. Since they have been aggressively marketed and since they provide what appears to be a simple painless solution to viruses, scanners are the most widely used anti-virus technique.

Too many people seem to regard "anti-virus product" and "scanner" as synonymous terms. The peril here is that if too many people depend solely upon scanners, newly created viruses will spread totally unhindered causing considerable damage before the scanners catch up with the viruses. An example of this was the attack by the Maltese Amoeba (Irish) virus in the UK. This virus was not detected prior to its destructive activation on November 1, 1991. Prior to its attack, it had managed to spread quite widely and none of the existing (mostly scanner-based) products detected this virus.

According to the December 1991 Virus Bulletin:

> *Prior to November 2nd, 1991, no commercial or shareware scanner (of which VB has copies) detected the Maltese Amoeba virus. Tests showed that not ONE of the major commercial scanners in use ... detected this virus.*

This indicates the hazard of depending upon scanner technology or active monitor technology for virus protection.

Another major drawback to scanners is that it's dangerous to depend upon an old scanner. With the dramatic increase in the number of viruses appearing, it's risky to depend upon anything other than the most current scanner. Even that scanner is necessarily a step behind the latest crop of viruses since there's a lot that has to happen before the scanner is ready:

- The virus has to be detected somehow to begin with. Since the existing scanners won't detect the new virus, it will have some time to spread before someone detects it by other means.

- The newly discovered virus must be sent to programmers to analyze and extract a suitable signature string or detection algorithm. The string must then be tested for false positives on legitimate programs.

- The string must then be incorporated into the next release of the virus scanner.

- The virus scanner must be distributed to the customer.
- In the case of retail software, the software must be sent to be packaged, to the distributors, and then on to the retail outlets. Commercial retail software takes so long to get to the shelves, that it is almost certainly out of date. Yet, many retail products depend upon their scanner for most of their effectiveness.

If you depend upon a scanner, be sure to get the latest version directly from the author. Also, be sure that you boot from a clean write-protected copy of DOS before running the scanner; there's a good chance that the scanner can detect a resident virus in memory, but if it misses the virus in memory, the scanner will wind up spreading the virus rather than detecting it. Every susceptible program on your disk could be infected in a matter of minutes this way! (See Fast and Slow Infectors.)

Ghost Positives

Scanners may also give you what can be termed "ghost" positives.

When DOS reads from a disk it does not read exactly what is requested; it also reads a bit ahead so that when the next read request comes in DOS may just have the material needed in a memory buffer and it can be provided much faster. Likewise, when a scanner reads files it has to compare each with scan strings. These are stored in memory.

If, after scanning, the scanner does not clear its buffers in memory and you immediately run a second scanner (which is common practice) then the second scanner may see the first scanner's strings in memory and if it uses the same string(s) could identify that virus as being in memory.

This is why it's important to run your scanner (or other anti-virus product) after a cold boot. One of the features of a cold boot is a complete memory check and this check overwrites all of memory, clearing out all false traces of viruses.

About...

Detection
Techniques

Interception

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Interceptors (also known as resident monitors) are particularly useful for deflecting logic bombs and trojans. The interceptor monitors operating system requests that write to disk or do other things that the program considers threatening (such as installing itself as a resident program). If it finds such a request, the interceptor generally pops up and asks you if you want to allow the request to continue. There is, however, no reliable way to intercept direct branches into low level code or to intercept direct input and output instructions done by the virus itself. Some viruses even manage to disable the monitoring program itself.

It is important to realize that monitoring is a risky technique. Some products that use this technique are so annoying to use (due to their frequent messages popping up) that some users consider the cure worse than the disease! An interception (monitoring) product would be a useful adjunct to a data integrity program, as protection against some the more simple minded logic bombs.

About...

Detection
Techniques

Integrity Checking

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Integrity check based products work by reading your entire disk and recording integrity data that acts as a signature for the files and system sectors. An integrity check program is the only solution that can handle all the threats to your data along with viruses. Integrity checkers also provide the only reliable way to discover what damage a virus has done. A well-written integrity checker should be able to detect any virus, not just known viruses.

So, why isn't everyone using an integrity checker? In fact, many anti-virus products now incorporate integrity checking techniques. One problem with many products is that they don't use these techniques in a comprehensive way. There are still too many things not being checked. Some older integrity checkers were simply too slow or hard to use to be truly effective. A disadvantage of a bare-bones integrity checker is that it can't differentiate file corruption caused by a bug from corruption caused by a virus. Only recently have advanced integrity checkers become available that incorporate the capability to analyze the nature of the changes and recognize changes caused by a virus. Some integrity checkers now use other anti-virus techniques along with integrity checking to improve their intelligence and ease of use.

If you choose an integrity checker, be sure it has all these features:

- It's easy to use with clear, unambiguous reports and built-in help.
- It hides complexity, so that complicated details of system file or system sector changes are only presented if they contain information the user must act upon.
- The product recognizes the various files on the PC so it can alert the user with special warnings if vital files have changed.
- It's fast. An integrity checker is of no use if it's too slow to run.
- It recognizes known viruses, so the user doesn't have to do all the work to determine if a change is due to a software conflict, or if it's due to a virus.
- It's important that the integrity computation be more sophisticated than a mere checksum. Two sectors may get reversed in a file or other damage may occur that otherwise rearranges data in a file. A simple checksum will not detect these changes.
- It's comprehensive. Some integrity checkers, in order to improve their speed, don't read each file in its entirety. They read only portions of larger files. They just spot check. This is unacceptable—it's important to know the file hasn't changed, not just that some of the file hasn't changed.
- It checks and restores both boot and partition sectors. Some programs check only files.

(Computer Knowledge recommends using the integrity checking technique for the most complete and effective method of detecting problems. Click on the About button above for specific product information.)

Detection Techniques

Guidelines for Using Anti-Virus Products

About...

Most modern anti-virus products use a combination of techniques. Most products still get almost all of their protection from their scanner component. It's vital to understand exactly how your product works so that you understand what type of protection you really have. Here are some rules that will help you make sure that you get maximum protection out of whatever product you already have:

- Be sure to cold boot your PC from a write-protected diskette before virus checking. Most anti-virus products make this recommendation, but this rarely gets done because the recommendation is often buried in some obscure location in the documentation. If your PC is infected with a virus that your scanner does not recognize, you could infect all the programs on your disk. Don't take this chance; boot from a write-protected diskette before you scan.

- If you are using a product which depends mostly on its scanner component, make sure that you always have the latest version. Scanners are often updated every 30 days.

- Before you execute or install any new software, check it first. If it comes with an install program, check again after you install the software; an install program will frequently change or decompress executable programs. After you first execute brand new software do an additional check of your system to make sure everything is as it should be.

- If your product contains a scanner component, consider checking the boot sector on all diskettes brought in from another location—***even data diskettes***! Inevitably someone will leave these diskettes in their A drive, potentially spreading a boot sector virus.

Protection Techniques

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

There are several levels of protection you can apply to help prevent disasters. They include physical/hardware and software techniques.

Click on each topic to bring up a discussion.

- **Physical/Hardware Protection**
- **Gadgets**
- **Virus Disinfectors**
- **Inoculators**
- **Network Protection**
- **Backup Strategy**

Summary

Hardware techniques, such as placing all your programs in read only memory (ROM), can, in theory, provide virus prevention, but nothing even comes close to doing this yet (when all software actually runs from a CD-ROM instead of just loading from one we'll be closer since a CD-ROM can only be infected by its producer). Pure software techniques can probably not prevent all viruses. There are all sorts of schemes that make it more difficult for a virus to penetrate your system, but none totally eliminate the threat of a virus. For each software-based technique, there is a way a virus could circumvent it. Software helps a lot, but isn't absolute protection. While prevention of viruses may not be possible, detection is. Detection, if applied carefully, can detect all viruses, no matter how tricky. If viruses are detected before they spread, the most serious aspect of the virus threat is eliminated. If integrity checking is practiced widely, the threat of a virus spreading to millions of PCs and then years later doing a destructive act can be eliminated.

About...
Detection
Techniques

About...
Recovery
Techniques

Physical/Hardware Protection

About...

This may not be an issue if you keep your PC locked in a vault when you're not using it, but otherwise you can never be sure that an intruder hasn't changed something on your PC. The intruder may be your spouse or offspring. They probably have no intention of changing anything but may be confused on how to use one of the programs on your PC, with the result that they inadvertently change the wrong file. On the other hand, you may work in an environment where someone may want to deliberately do you harm or perhaps just "play a little joke" on you.

There are add-in boards available that modify the partition sector on your PC so that the hard disk is unavailable unless someone provides a password. Some PCs come with a power-up password. You can lock the case to your PC to make it more difficult to open. You may wish to consider any of these options depending upon how much risk you face, but please realize that they can all be bypassed in less than ten minutes by a knowledgeable user.

Gadgets

About...

There are currently some gadgets (hardware devices) that are sold as virus protection. So far, there seems to be nothing that provides protection beyond what is offered by software-only products. Beyond putting some of the anti-virus code in read only memory (ROM), there has been little eles that can be accomplished by existing hardware. In one product, the hardware was used to store some integrity data; a floppy disk can do the same thing and it's actually more secure.

Virus Disinfectors

About...

Most vendors that sell scanners also sell a disinfector (sometimes it's the same program). A disinfector has the same limitations that a scanner has, in that it must be current to be safe to use and it's always one step behind the latest crop of viruses. The disinfector, however, has an even bigger disadvantage: Many viruses simply cannot be removed without damaging the infected file. There have also been numerous reports that files are still damaged even when the program claims to have disinfected the file. A disinfector, like a scanner, can be a very handy tool in your anti-virus arsenal, but it must be used with care. If you use a disinfector, be sure you have the latest version direct from the producer (and use an integrity check to verify that all files and system sectors are correctly restored).

To take but one example of the above caveat, currently, one of the oldest and most common infectors of files is the Jerusalem (1813) virus. Disinfectors generally claim to be able to remove this virus. Yet the Jerusalem virus frequently overwrites part of the original file (due mostly to its many bugs) making it impossible to restore the infected program. In spite of this, most (if not all) disinfectors claim to disinfect Jerusalem-infected files. A very dangerous situation!

Bottom line: You ***should not depend on disinfectors*** as the sole method of recovering from virus infections.

Inoculators

About...

There are two types of inoculators or so-called "immunizers." One modifies files or system sectors in an attempt to fool viruses into thinking that you are already infected. The inoculator does this by making the same changes that the viruses use to identify the file or sector as infected. Presumably, the virus will not infect anything because it thinks everything is already infected. This works only for a very small number of viruses.

The second technique is actually an attempt to make your programs self-checking by attaching a small section of check code onto your programs. When your program executes, the check code first computes the check data and compares it with the stored data. It will warn you if it finds any changes to the program. Not only can this be circumvented by existing stealth viruses, but the self-checking code and check data can be modified or disabled as well. Another problem arises because some programs refuse to run if they have been modified in this way. This also creates alarms from other anti-virus programs since the attached self-check code changes the original program in the same way a virus would. Some products use this technique to substantiate their claim to detect unknown viruses.

Network Protection

About...

Networks have the potential to spread viruses far and wide, very quickly. Fortunately, network administrators have some powers that, if used properly, can go a long way toward limiting this spread.

First, make sure that any shared executable files allow only execute or read access. Execute only is best, but it's essential not to allow write access.

Most network compatible programs allow you to store the files they write to on separate disks from the programs themselves. Install programs so that all items unique to a user is stored on the user's system so that when the files are open for write access the network is not involved.

Be sure to limit write access with access rights not with file attributes (Netware FLAG or FLAGDIR). A virus can easily bypass file attributes, but access rights can thwart the attempts of a virus to write to the shared disk.

The person who supervises the LAN needs to have two accounts—one privileged and one not. For normal use, they should use the less privileged account. The privileged account should be used only when the job requires supervisor rights. It's critical that any user with supervisory rights log off as soon as possible and be very careful when executing any programs, especially those on a workstation.

Run regular integrity checks on the file server. This is important on the workstations too, but is critical on the file server since an infected file here could quickly infect all the workstations on the network.

Never access the network from an unchecked workstation with network administrator (supervisor) authority!

Backup Strategy

About...

Too many people wait for a virus to attack their PC before they take any action. Once a virus reveals its presence on your PC, it may be too late to recover damaged files. There are many viruses that cannot be successfully removed due to the way the virus infects the program. It's absolutely vital to have protection before the virus strikes. If you wait until you notice that your hard disk is losing data, you may already have hundreds of damaged files.

It's essential to carefully protect all your software and regularly back up the data on all your disks. Do you have a single disk that you can afford ***not*** to regularly backup? It's rare to find any PC that does not have some type of important data stored on it.

Suggested Policy

- All original software (program) diskettes should immediately be write-protected, copied and stored in two secure, separate, locations after installation. If you are using an integrity check program, immediately record (initialize) the integrity data for the new programs after installing.

- Determine a schedule for full backups by considering how frequently your data changes. It is an excellent idea to have three full sets of backup tapes or diskettes and to store one set at another location to protect against fire, theft, or some other disaster. If your data is critical, you may wish to have a separate cycle of backups (e.g., quarterly or yearly) that can be used to recover when someone damages (or deletes) a vital file, but the deletion isn't discovered until months later.

- The full backups should be coordinated with periodic incremental backups. The incremental backup, which copies just the files that have changed, normally runs very quickly and takes just a minute or so. Many people find that an incremental backup run at the end of each day works quite well. This way their data is protected should anything happen overnight. One rule of thumb for incremental backups is to do them when it would become difficult or not cost effective to re-enter the data.

- Make sure you use reliable backup hardware and software. Periodically test by restoring from a backup. Too many people have discovered that their backup program couldn't recover their files when it was too late. If you use an integrity check program you can verify that the restored files are correct.

- Be certain you store the recovery program for your backups ***with*** your backups. Some people have regularly backed up their data only to find that the only version of the recovery program was on their backups and not available to actually run.

Recovery Techniques

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

There are many different ways to recover from problems with your data; but most of them only work well if you've taken some precautions in advance. There are no guarantees if you do not take precautions.

Information in your computer is generally divided into two broad categories: programs and data.

In the event of disaster, programs can usually be reinstalled from their original master disks; data, however, is a different story. Since you create data and it changes on a day-to-day basis you need to make periodic backups of that data and store them in a safe place. If you have not done so and the portion of the disk that the data resides on gets somehow garbaged, you are just out of luck. There is no magic bullet that will recover data that has been overwritten.

Your first step in recovering is to determine the threat and what happened.

- First gather as much information as possible. Did you do anything unusual? Did you install any new software? Did you execute any programs that you don't normally use? Have you seen any signs of hardware problems?

- Run CHKDSK to see if your directories and other areas are OK.

- Run a full integrity check to see exactly what has changed.

- If you suspect hardware problems as the culprit, then run any diagnostic programs you have. If the diagnostics don't turn anything up, but you still suspect a hardware problem, then run your integrity check in full check mode daily for a while. This should help track down exactly what's happening on your PC. Be more than ever careful about keeping a current backup.

- If you suspect software problems, run the software in question and then run your integrity check to see if anything is being corrupted. When doing this, it's very helpful to duplicate the original situation of the problem as closely as possible. Make sure the hardware is the same and that you have exactly the same resident programs and device drivers loaded as when the problem first occurred. (Again, backup, backup, and backup again into different backup sets.)

- Could the problem be a virus? If you think so, have you seen any of the signs of virus activity? Are only executable files (such as files ending in .EXE, .COM, .OVR, .OVL .BIN, or .SYS) affected? If so, how many? If more than one or two unrelated program files have mysteriously changed, it could be a virus. Remember that some programs (such as the DOS program SETVER) modify themselves as part of normal execution. If the programs have changed but the DOS time and date stamps haven't, this is further reason to suspect either a serious problem or a virus. If you are not using an advanced integrity checker that recognizes known viruses, you may wish to get a virus scanner at this point to see if you have a known virus. If this turns up nothing, then it's time to play detective—you may have discovered a brand new virus (lucky you!).

Once you have discovered the threat, you are in a position to do something about it. It is beyond the scope of this tutorial to describe each and every possible recovery technique. If in doubt, present your data to a more experienced computer user and ask for help. Basically, you should have:

- **Data integrity software**
- **Current backups**
- **Utility tools**

There are some general techniques that can be applied when you come up against a virus attack. These are covered in the topic below:

- **Handling a Virus Attack**

Below are some specific problems people come up against. They are listed here as they are fairly common.

- **Infinite Subdirectory Loop**

- **Stoned/Michelangelo Interaction**

About...
Protection Techniques

About...
Hoaxes and Myths

Handling a Virus Attack

About...

Following is a general plan of attack should you find a virus on your computer.

1) Don't Panic

Don't do anything rash if you suspect a virus attack. Be skeptical, there are quite a few practical joke programs that behave exactly like viruses. There's even a virus simulator that simulates the Ping Pong (bouncing ball), Jerusalem (black hole), Cascade (falling letters on the screen), Yankee Doodle (music) and a few other viruses. It's perfectly harmless, but it has alarmed many people. Don't do anything drastic until you confirm that it really is a virus.

Use an up-to-date version of a good anti-virus product to verify the virus and determine which one it is. If you just suspect a virus, be certain to contact your anti-virus product supplier to get instructions on how to "capture" the beast and send it to them for analysis.

2) Report the Attack

Report the virus attack to a virus researcher or anti-virus developer. We need to stop sweeping this under the rug. If we can track where viruses first get started, then maybe we can work toward eliminating these beasts.

3) Play Detective

It is very important that you try to track down how you got the virus. If you got it from someone's software, it's vital they be notified. The sooner these viruses are detected and others who might have them notified, the less damage they can do.

Suppose you have indications of a virus, but your software doesn't identify it as a known virus. What do you do? Make a note of all circumstances that lead you to believe you have a virus (e.g., changed total memory reading in CHKDSK, integrity check variations, etc.) and then notify your anti-virus software producer. There are special techniques for capturing file versus boot sector viruses and the technical support people can tell you exactly what to do to capture the beast and send it to them.

If you want to experiment some to pin the virus down, here is one technique you can use (after a good backup of your important data files at least!).

> First, cold boot (hit the hardware reset button or power off and back on) from a known good write-protected copy of DOS on a diskette. Run a full integrity check. Run CHKDSK and print the results. Now execute any suspect programs. Execute them several times. Viruses may wait for some trigger event to begin infection. Run CHKDSK again to see if the amount of free (or total) memory has been reduced. This is a sign of a virus going resident in memory. Now cold boot again and rerun an integrity check. Repeat this cycle with the various suspect programs. This should track down the guilty program if you've got a file infector. Keep in mind that if it's a virus, it will modify other programs and those programs should themselves further modify other programs. By

executing the modified programs, it's possible to tell whether you really have a virus or you just have a buggy program that is accidentally writing to other programs.

For a suspected boot sector virus, first boot normally, run CHKDSK and make a note of the total and free memory. Then, as above, perform a cold boot from a known-clean write-protected floppy disk and again run CHKDSK. If the total and/or free memory has changed you may have a boot virus. This is particularly true if the memory values differ from those you should have on record for CHKDSK on your system.

4) Clean House

Follow these steps when removing a virus from your PCs:

- Cold boot (power off and on or hit the hardware reset button) from a known-good write-protected copy of DOS.

- Delete all infected files.

- Reload any infected system sectors. You should use a good utility program to do this or use images of your system sectors stored by your anti-virus software. You can use the DOS "SYS" command to reload the DOS boot sector if you have no such utilities. Unfortunately, the SYS command will only remove a small number of boot sector viruses. Most of these infect the Master Boot Record (or partition table) and SYS has no effect on that. If you use a DOS utility to rebuild the Master Boot Record (e.g., FDISK) you will then have to reformat and completely restore your hard drive from backups. It's much better to use a utility program designed for this purpose.

- Rerun a full integrity check, or at least a scan if you don't have an integrity checker.

- Check any floppies that may have been infected. Remember, if you have a system sector virus such as Stoned, Joshi or Brain, even empty data diskettes can be infected. Check them all.

- Notify any other PC user you have contact with to check their PCs.

5) Guard the House

Virus infections return in a very high number of cases. This is usually because somewhere there is an infected file or diskette that was missed in the first cleaning. Run your integrity checker or anti-virus program daily, for the next month, to catch a possible repeat infection.

Infinite Subdirectory Loop

About...

Now and again you may look at a subdirectory and notice that it looks just like the root directory. If you then change to that directory again you will see the same thing. Indeed, you can continue this process for a significant number of iterations and continue to see the same files as you go deeper and deeper into the directory tree.

Is this a virus?

Likely not. This can happen easily if an errant piece of software sets the cluster pointer of a subdirectory to the same value as an upper-level directory (most often the root directory). Every time you change to the so-marked directory, you will actually be seeing the upper level directory entries; over and over and over again.

Most DOS utilities (e.g., SCANDISK) can fix this problem by deleting the mis-pointed directory (everything in that directory will be effectively deleted from the disk). You can then restore the offending subdirectory from your backup.

Important: If this situation arises, do ***not*** erase files or remove directories before the disk is repaired. If, for example, you command DEL *.* in the offending directory to just erase it you are actually erasing all the files in the pointed-to directory (usually the root). This can cause much more serious problems.

Stoned/Michelangelo Interaction

About...

It's possible for a computer to be infected with two different viruses at the same time. Sometimes this happens in a way both viruses can be removed without problem; other times there are significant problems. The latter happens when both Stoned and Michelangelo appear on the same computer. The computer becomes unbootable and anti-virus programs have problems removing the viruses; when one is removed, the other appears and vice versa.

The problem is that both of these viruses infect the Master Boot Record and, while they store the virus code in different locations on the hard disk, they store the original copy of the MBR in the same place. Thus, when the second of the two infects the computer it does not check for the other and simply stores what is in the MBR sector in the storage location. Unfortunately, this is a copy of the other virus, not the original MBR. Since this is what the second virus attempts to run when the computer is next booted and it's not the original MBR, the computer hangs.

Anti-virus software checking this disk will see the second infection and remove it, replacing the MBR with what's in the storage location (again, usually without checking the contents). This effectively reinstalls the first virus and makes it possible for the overwriting cycle to start anew.

Again, anti-virus software is used and sees the first virus and "fixes" it the same way, reinstalling the second virus. The cycle can continue as often as the anti-virus software is run and the computer rebooted.

The solution to this problem is to use a special utility to replace the Master Boot Record with a stored copy of the original MBR and thus erase pointers to either virus. A good anti-virus utility will have this capability.

Hoaxes and Myths

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Viruses, by their nature, tend to mystify the average user. They operate in the background under rules that are little understood by most users. As such, a mythology has developed where stories are passed from person to person as true; yet few are based in fact.

Here you'll find a discussion of the more common myths (and the "real" story) along with hoaxes, silly tricks, and poor policies.

- **Myths**
- **Hoaxes**
- **Silly Tricks**
- **Poor Policies**

About...
Ways to Combat Threats

About...
Myths

Myths

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

A few of the more common mythical virus sources are presented here along with the "real" story.

- **Attachment to a Network or BBS**
  Myth: Simply being attached to a network (such as CompuServe, or Internet), a bulletin board system (BBS), or even a local area network (LAN) will make you susceptible to viruses.

About...

- **From Data**
  Myth: You can obtain a virus by looking at some data.

About...

- **From CMOS Memory**
  Myth: A virus can hide in your CMOS (setup) memory instead of on your hard disk.

About...

About...	About...
Hoaxes and Myths	Hoaxes

Attachment to a network or BBS

About...

Myth: Simply being attached to a network (such as CompuServe, or Internet), a bulletin board system (BBS), or even a local area network (LAN) will make you susceptible to viruses.

Truth: The only way you can get a virus is to execute a program on your PC that you obtained over the network. The mere act of downloading the program is harmless; it's only by downloading and then executing an infected program that your PC can become infected. The same is true for electronic mail; the mere act of reading electronic mail cannot infect your PC (see the Good Times hoax description).

Caveat: There is one thing that can happen when connected to another computer. If you have the device driver ANSI.SYS (or an equivalent) loaded (in your CONFIG.SYS file), someone could send a sequence of characters to your screen that assigns a set of keystrokes to a key on your keyboard. These keystrokes could easily be something harmful like "DELTREE /Y C:\". When you hit the key that was reassigned, the command would execute just as if you had typed it yourself. This "practical joke" could cause some trouble, but it certainly can't reproduce and isn't a virus. Further, most modern communications programs that emulate the ANSI driver have built-in safeguards that disable keyboard remapping.

From Data

About...

Myth: You can obtain a virus by looking at some data.

Truth: Since data is not executed, you cannot become infected from data. If someone sent you a data file that contained a virus, you would have to "execute" it to become infected.

Caveat: You can become infected from a diskette that is not bootable and contains no visible executable programs. All diskettes have a boot sector that contains a program which can become infected by a boot sector virus. If you leave such an infected diskette in your floppy drive when you power up or boot, your PC can become infected!

Please also see the More Information link. Click on the button. About...

From CMOS Memory

About...

Myth: A virus can hide in your CMOS (setup) memory instead of on your hard disk.

Truth: Most computers (except early PC/XT models) contain a small amount of battery-backed CMOS memory to store the configuration and to maintain the time and date. This memory is never executed so you can't become infected from CMOS memory.

Caveat: A virus can change information in the CMOS. You may have set the CMOS values so that the computer tries to boot from the hard disk first to avoid boot sector viruses on floppy disks. A virus could, in theory, change that so the computer tries to boot from the floppy first instead. In practice, since CMOS data is not standardized, this would only affect a small number of computers and is therefore considered unlikely.

Hoaxes

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Most hoaxes, while deliberately posted, die a quick death because of their outragous content. Some make it into the wild and get out of hand.

A lot of hoaxes spout some pretty good technobabble, so unless you are a real expert, it's quite easy to get caught. Look for specific technical details, particularly how to identify and get rid of the beast. If you don't recognize the name of the person posting the warning, check to see who they say they have sent copies to for study. Independently verify the report with secondary sources.

Some of the more "popular" hoaxes are listed here along with some comment.

◆ **The "Mike RoChenle" Modem Virus**

Identified with IBM's then new Microchannel architecture, this virus supposedly used a "secret carrier wave" kept hidden by modem manufacturers for testing. In fact, modems do not use a "carrier" frequency.

◆ **Proto-T**

This was announced as a super-virus which no anti-virus product could detect. It is not, of course, possible to write a virus which cannot be detected. Showing how a hoax can get out of hand, once it had been determined that there was no Proto-T virus, the virus community wrote one. Several, actually.

◆ **Desert Storm Virus**

This virus, supposedly hidden in printers sent to Iraq, was clearly based on an April Fools joke in InfoWorld magazine. But Pentagon spokespersons vouched for its authenticity, completely taken in by the rumour.

◆ **Good Times and XX-1**

Both of these were reported at about the same time. Both seem to have been sincere warnings by totally unsophisticated people. Both reported mail messages which could somehow wipe out your hard disk.

About...

◆ **Paul Revere**

A few years back, one of the PC magazines published a list of joke viral programs, usually with some pun on the name. One was Paul Revere (returns 1 if infected by LAN and 2 if by C). Some time later, a local sysop calling the OS/2 support line with an oddity and was told he might have the Paul Revere virus. This was not widespread, but shows how even a joke can get out of hand.

◆ **The Porno GIF Virus**

A pornographic GIF graphics file uuencoded and posted on one of the alt.binaries.* graphics groups had some very weird text in it, somewhat indicative of a virus or trojan. Analysis indicated that it wouldn't do anything.

- **The JPEG Virus**

A recent variation on the GIF virus discussed just above.

- **FCC Modem Tax**

Every so often someone posts a dire warning that the FCC is considering a tax on modems and online services. The warning encourages you to tell your friends so they can take political action. It's a hoax. It's been going on for at least five years, and probably much longer. Look for congressional bill number (and double-check it if you see one).

- **Make Money Fast**

If you haven't seen a Make Money Fast message, just wait. An electronic version of a chain letter pyramid scheme will soon show up in your mailbox or your favorite newsgroup. You're supposed to send money to the ten people on the list, then add your name to the list and repost the chain letter, committing fraud in the process.

- **Craig Shergold Needs Your Get Well Cards**

Craig Shergold is a UK resident who was dying of cancer. He wanted to get in the Guinness Book of World Records for having received the most get well cards. When people heard of the poor boy's wish, they began sending him postcards. And, they kept sending him postcards, and never stopped. He was listed in the Guinness Book of World Records in ***1991***. He really does not want your postcards any more, and neither does his hometown post office.

Certainly there are more hoaxes out there and, as night follows day, there will be more. Before jumping into the deep end of the pool and believing everything that comes across the net, check it out:

- Look at the location of the posting. If the posting is in an inappropriate newsgroup be suspicious.
- Look at the poster. Is it someone who is clearly identified and is a known expert on the subject of the posting?
- Look closely at the details:
    - If it involves government action there should be some reference to an easily-obtained bill or federal regulation.
    - If it involves something technical look for obvious technobabble (e.g., Nth complexity infinite binary loop).
- Double check it anyhow!

About...

About... Hoaxes and Myths

About... Silly Tricks

Detailed Analysis: Good Times Hoax

About...

The "Good Times" message usually begins with some sort of warning. The warnings vary, but may be similar to that shown here:

> Thought you might like to know...
>
> Apparently , a new computer virus has been engineered by a user of America Online that is unparalleled in its destructive capability. Other, more well-known viruses such as Stoned, Airwolf, and Michaelangelo pale in comparison to the prospects of this newest creation by a warped mentality.
>
> What makes this virus so terrifying is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing e-mail systems of the InterNet.
>
> Luckily, there is one sure means of detecting what is now known as the "Good Times" virus. It always travels to new computers the same way - in a text e-mail message with the subject line reading simply "Good Times". Avoiding infection is easy once the file has been received - not reading it. The act of loading the file into the mail server's ASCII buffer causes the "Good Times" mainline program to initialize and execute.
>
> The program is highly intelligent - it will send copies of itself to everyone whose e-mail address is contained in a received-mail file or a sent-mail file, if it can find one. It will then proceed to trash the computer it is running on.
>
> The bottom line here is - if you receive a file with the subject line "Good TImes", delete it immediately! Do not read it! Rest assured that whoever's name was on the "From:" line was surely struck by the virus. Warn your friends and local system users of this newest threat to the InterNet!   It could save them a lot of time and money.

Added text often accompanies or modifies the initial warning. Here is where the technobabble tends to trip up the writer as the fantasy gets deeper. Examples are shown here.

> The FCC released a warning last Wednesday concerning a matter of major importance to any regular user of the InterNet. Apparently, a new computer virus has been engineered by a user of America Online that is unparalleled in its destructive capability. Other, more well-known viruses such as Stoned, Airwolf, and Michaelangelo pale in comparison to the prospects of this newest creation by a warped mentality.
>
> What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing e-mail systems of the InterNet. Once a computer is infected, one of several things can happen.   If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop - which can severely damage the processor if left running that way too long.   Unfortunately, most novice computer users will not realize what is happening

until it is far too late.

On December 6, 1994, the U.S. Department of Energy's CIAC (Computer Incident Advisory Capability) issued a bulletin declaring the Good Times virus a hoax and an urban legend. The bulletin was widely quoted as an antidote to the hoax.

About...

Is An E-mail Virus Possible?

About...

No. There is no way for a virus to spread simply by ***reading*** email.

A few people have gone through mental gymnastics trying to dream up a way such a thing could be done. The closest anyone has come is to infect a program with a virus, encode the program into text with uuencode, binhex, etc., and email the encoded program. The person receiving the email would have to download the mail to their hard drive, decode it, and run the infected program. That's not even close to the claims made for the spread of Good Times.

You should, of course, be wary of any file attachments a stranger sends you. At the least, you should check such file attachments for viruses before running them.

Important note: Some E-mail readers, when they detect a particular type of document attached to an E-mail message, will automatically start the appropriate program and display the document; or, will start executable attachments for you. These have options to set that disable such behavior; always set the options to ***not*** load and/or run attachments automatically.

Silly Tricks

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

There have been many articles and books written that propose all kinds of things to virus-proof your PC. Here are some of the most useless:

- **Write-protecting Your Files**

You can use the DOS ATTRIB command to set files to a read-only status. This is very easy for a virus to bypass and simply causes far more problems than it cures.

- **Hiding or renaming COMMAND.COM**

COMMAND.COM is a program that executes each time you boot your PC. There was an early virus that only infected COMMAND.COM, so the idea of hiding or renaming this file began. Today, many viruses actually go out of their way to avoid infecting this file, since some anti-virus products single it out (and a few others) for special scrutiny. With today's viruses, hiding COMMAND.COM is utterly futile.

- **Checking Time and Date Stamps**

While it's helpful to check the time and date stamps of your executable files for unexpected changes, this is not a reliable way to catch viruses. Many viruses are smart enough not to change the time and date stamps when they infect a file. Some viruses even hide the change to a file's size when they infect a file.

- **Write-protecting Your Hard Disk**

There are several programs that claim to write-protect your hard disk. Since this is done in software, it can be bypassed by a virus. The technique may stop a few viruses and will protect your disk from someone inadvertently writing to it; but can become a serious problem since much software needs to write to the hard disk in order to operate. These programs are generally less effective than virus interception products.

It is possible to write-protect a disk using hardware; but, again, is likely to only result in problems for you when running software.

About... Hoaxes and Myths

About... Poor Policies

Poor Policies

Click to learn how to protect your computer and obtain other tutorials of interest.

Many companies and agencies have developed policies that are supposed to help control and combat virus spread within that company or agency. While they may have helped some, most of these policies cannot be shown to be cost effective when the cost of implementation and control are factored into the equation.

Here are some that you need to look carefully at before implementing.

- **Central Certification**

It's the policy in some companies to have a certification desk where all software executed on PCs must be checked out. The person at the certification desk usually runs the software through an anti-virus product to check for known viruses and then sets the date ahead on the PC and checks for anything strange. If all looks OK, the software is certified clean. This is a reasonable idea. The danger comes from the "certified clean" label. Simply setting the date ahead is not a reliable way to set off most virus triggers and the anti-virus product used may not recognize a virus, if it's not known to the anti-virus software writer. It's just not possible to know for sure that any piece of software doesn't contain a virus. An unknown virus could be lurking that simply hasn't triggered yet. If the virus screening desk should get such a virus, they could easily spread the virus to all other disks that they are certifying clean! Central certification is not a substitute for individual protection policies.

- **Purchase Retail Software Only**

Several "virus experts" have suggested that users avoid downloading software and avoid shareware. There are no facts to support this viewpoint. The most common viruses are boot sector viruses such as Stoned and Michelangelo that spread when someone boots from an infected disk. To spread these viruses, a physical disk must be passed around and then booted. Michelangelo spread widely because software distribution disks were infected with this virus. There was no reported incident of this virus spreading via shareware.

It is, of course, wise to make sure that you download your software from a source that screens each program for known viruses.

You are actually more likely to be infected from software purchased at a retail outlet than from shareware. Quite a few viruses have been shipped directly from the software manufacturer in the shrink wrapped packages. One major software company has on at least two separate occasions shipped a virus with their product.

Buying shrink wrapped retail software is much more dangerous than many people think it is, since many retailers accept returned software and then simply rewrap the software and sell it again. This software could have easily been infected by the first user who tried it and then returned it.

Again, only individual protection methods will protect you; not policies.

Quick and Easy Cures

The simple point to make here is: there are none. Any product that advertises itself as a "quick and easy cure" for "all viruses past, present, and future" is more likely than not exercising its advertising imagination. Everyone would like to just buy product X, run it, and be rid of viruses forever. Unfortunately there is no such easy cure.

About... Hoaxes and Myths

About... Specific Virus Descriptions

Specific Virus Descriptions

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

As of the middle of 1995 the following viruses were among the most commonly reported in the world. This is not to say you will not see any of the other several thousand viruses; it's just that these seem to be "popular." In general, the higher up in the list a virus is, the more it is seen in the wild.

We've included brief descriptions of the viruses in the list. Please keep in mind that there are many variants for most viruses. Each may have a different payload and/or activation mechanism. It is beyond the scope of this tutorial to describe each of these in detail.

Virus (Aliases)

- Form
- Stoned.Empire.Monkey.B (Monkey-2)
- V-Sign (Cansu, Sigalet)
- Parity_Boot.B (Generic-1, Parity)
- AntiEXE (D3, Newbug, New Bug)
- Stoned.Standard.A (New Zealand, Stoned 1)
- Joshi.A
- Stealth_Boot.B (Nops, STB, stelboo, Stealth.B)
- Stoned.No_Int.A (NoInt, Stoned)
- AntiCMOS.A (Lenart)
- Stoned.Michelangelo.A (Michelangelo)
- Stoned.Empire.Monkey.A (Monkey-1)
- Jumper (2kb, French Boot)
- Ripper (Jack the Ripper)
- NYB (B1)
- Natas
- Boot-437
- Tequila.A
- Kampana.A (Anti-Tel, Campana, Telecom, Telephonica)
- Cascade.1701 (1701)
- Athens (Trojector)
- Qrry (Query, Quarry)
- Jerusalem.1808.Standard (1813, Jeru-1808)
- Flip.2153.A (Omicron)
- Junkie (Junkie-1027)

About...

Hoaxes and Myths

Form

The Form virus infects the DOS boot sector on hard drives and the boot sector on floppy disks. It stores itself at the end of the hard disk and in sectors marked as bad on floppies.

Form infects through leaving an infected disk in the boot floppy drive.

Form's payload activates on the 18th of any month when the PCs speaker clicks on each keypress. There is a bug that causes this keyclick to not happen when a keyboard driver is loaded.

Form is relatively easy to remove.

Monkey

The Monkey virus infects hard disk Master Boot Records and the boot sector on floppy disks. The virus replaces the entire MBR with its code and encrypts the original. On a clean boot (or if generic removal techniques are used) the message "Invalid drive specification" will be seen for any access to the hard drive.

Monkey infects through leaving an infected disk in the boot floppy drive.

Monkey has no payload at the time of this writing. It does have a bug that causes it to overwrite a portion of the FAT on 2.88MB floppy disks.

Use an anti-virus program to remove Monkey.

V-Sign

The V-Sign virus infects hard disk Master Boot Records and the boot sector on floppy disks. V-Sign does not save the original boot sector when infecting. V-Sign detects disks infected with Stoned and removes it in favor of infecting with itself.

V-Sign infects through leaving an infected disk in the boot floppy drive.

V-Sign displays a large ASC letter V after 64 disks are infected and then hangs the computer.

V-Sign is relatively easy to remove.

Parity Boot

The Parity Boot virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Parity Boot infects through leaving an infected disk in the boot floppy drive.

Parity Boot's payload activates after about an hour of inactivity on its part, when it displays "PARITY CHECK" on the monitor and simulates a genuine hardware problem by hanging the computer.

Parity Boot is relatively easy to remove.

AntiExe

The AntiExe virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

AntiExe infects through leaving an infected disk in the boot floppy drive.

AntiExe's payload targets a particular (unknown) EXE file with a specific string in its header. If that file is ever found, it's contents will be corrupted.

AntiExe is relatively easy to remove.

Stoned

The Stoned virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Stoned infects through leaving an infected disk in the boot floppy drive.

Stoned's payload sometimes activates to display "Your computer is now stoned" in some of its variants. Stoned has many variants; some are more virulent and damage boot sectors at defined times (e.g., one variant displays flames on the monitor and activates when the month changes).

Stoned is relatively easy to remove.

Joshi

The Joshi virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Joshi infects through leaving an infected disk in the boot floppy drive.

Joshi's payload activates on 5 January each year when it displays the message: "type Happy Birthday Joshi." If that phrase is typed the boot continues; if not the computer is stopped.

Joshi is relatively easy to remove.

Stealth_Boot.B

The Stealth_Boot.B virus infects the hard disk Master Boot Record and the boot sector on floppy disks. The virus is based on code published in a book about computer viruses.

Stealth_Boot.B infects through leaving an infected disk in the boot floppy drive.

Stealth_Boot.B has no intentional payload but may corrupt some files when infecting a floppy disk.

Stealth_Boot.B is relatively easy to remove.

AntiCMOS

The AntiCMOS virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

AntiCMOS infects through leaving an infected disk in the boot floppy drive.

AntiCMOS' payload clears setup information from CMOS.

AntiCMOS is relatively easy to remove.

Michelangelo

The Michelangelo virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Michelangelo infects through leaving an infected disk in the boot floppy drive.

Michelangelo's payload activates on each 6 March to "celebrate" the birthday of Michelangelo Buonarroti (6 March 1475). On boot that date the virus overwrites the first 17 sectors of the first 256 tracks of the hard disk using heads 0 to 3. Material overwritten cannot be recovered.

Michelangelo is relatively easy to remove.

Jumper

The Jumper virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Jumper infects through leaving an infected disk in the boot floppy drive.

Jumper has no payload.

Jumper is relatively easy to remove.

Ripper

The Ripper virus infects the hard disk Master Boot Record and the boot sector on floppy disks. It encrypts itself randomly.

Ripper infects through leaving an infected disk in the boot floppy drive.

Ripper's payload activates randomly, approximately every 1,000 disk writes. The virus will swap information being written to disk which causes (data usually) to become slowly corrupted. This corruption, because it is in data and occurs slowly, is difficult to notice (although it could be very dangerous if it happens to just the wrong set of data).

Ripper is relatively easy to remove.

NYB

The NYB virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

NYB infects through leaving an infected disk in the boot floppy drive.

NYB's has no payload, but will seriously corrupt some floppy disks.

NYB is relatively easy to remove.

Natas

The Natas virus infects the hard disk Master Boot Record, the boot sector on floppy disks, and COM, EXE, and overlay files. It is polymorphic.

Natas infects through leaving an infected disk in the boot floppy drive as well as running any infected executable files.

Natas' payload activates randomly, approximately every 512th time an infected file is run. The virus will, at that time, overwrite drive C: and other hard disks in the system. This virus is very dangerous.

Natas is relatively easy to remove, however the nature of its infection makes it necessary to closely check **everything**. Missing a single instance of this virus could be very dangerous.

Boot-437

The Boot-437 virus infects the DOS boot sector on hard drives and the boot sector on floppy disks.

Boot-437 infects through leaving an infected disk in the boot floppy drive.

Boot-437 has no payload.

Boot-437 is relatively easy to remove.

Tequila

The Tequila virus infects the hard disk Master Boot Record, and EXE files. When in infected EXE file is run the Master Boot Record is infected. The next time the computer is started, the virus goes resident and infects EXE files as they are run. (*Note: There are multiple varieties of Tequila. Some act differently.*)

Tequila infects through running any infected executable files.

Tequila's payload displays a text fractal image on the display. In some versions this happens four months after initial infection and then monthly. Under some circumstances a text message may also be displayed.

Tequila is relatively easy to remove.

Kampana

The Kampana virus infects the hard disk Master Boot Record, the boot sector on floppy disks, and COM files. (*Note: The virus is actually a family of viruses, some of which are boot sector infectors and some file infectors.*)

Kampana infects through running any infected executable files (or leaving an infected floppy disk in the drive when booting for that variant).

Kampana's payload overwrites your hard disk while displaying an anti-Spanish-telephone-company message after 400 boots.

Kampana is relatively easy to remove.

Cascade

The Cascade virus infects COM files.

Cascade infects through running any infected executable files.

Cascade's payload, if it executes (not all versions execute a payload), causes text characters on the screen to "fall down" and be left in a pile at the bottom of the screen.

Cascade is relatively easy to remove.

Athens

The Athens virus infects COM and EXE files.

Athens infects through running any infected executable files.

Athens does little more than just infect files. File length is increased but stealth techniques make this increase hard to detect if Athens is in memory. System errors may be noted when the virus is in memory.

Infected files may have to be deleted and an uninfected version reinstalled from original disks or a clean backup.

Qrry

The Qrry virus infects the hard disk Master Boot Record and the boot sector on floppy disks.

Qrry infects through leaving an infected disk in the boot floppy drive.

Qrry's payload activates in December and overwrites parts of the hard disk. Material overwritten cannot be recovered.

Qrry is relatively easy to remove.

Jerusalem

The Jerusalem virus infects both COM and EXE files.

Jerusalem infects any program that is run when it is active in memory.

Jerusalem's payload activates on Friday the 13th. The virus will delete any file run on that date. (Some variants activate on each Sunday with a simple message.)

Some Jerusalem variants can be removed; others damage the file they infect.

Flip

The Flip virus infects the hard disk Master Boot Record, and COM (if smaller than 62,857 bytes) and EXE files.

Flip infects through running any infected executable files.

Flip's payload causes EGA or VGA displays to "flip" the screen and reverse each character between 4pm and 4:59pm, the second day of each month. (The date/time varies with different varients of this virus.)

Flip is relatively easy to remove.

Junkie

The Junkie virus infects the hard disk Master Boot Record, the boot sector on floppy disks, and COM files (it also infects files named COM but with EXE headers).

Junkie infects through leaving an infected disk in the boot floppy drive as well as running any infected executable files. Junkie is usually termed a fast infector, although it does not infect every file opened. Also, Junkie does not infect the boot sectors of 360K or 2.88MB floppies.

Junkie's has no payload.

Junkie is relatively easy to remove.

Integrity Master Information

Click to go to an order form.

Computer Knowledge strongly recommends each user establish a strong anti-tampering routine for their computer(s). We feel that integrity checking is an excellent part of such a routine and have found the a particular product, Integrity Master by Stiller Research, is an excellent integrity checker. We recommend it and through this page make all ordering information for it available to you for consideration.

Read each item below in turn for more information. . .

- What is Integrity Master?
- What do I get when I order?
- Order Form
- Quantity/Site License Information

What is Integrity Master?

Order Click to go to an order form.

(From the Integrity Master documentation. Use the File|Print Topic menu item to print this page.)

Integrity Master is a powerful anti-virus and PC data integrity system that also provides security and change logging. This high performance assembly language program provides fastest integrity checking available for the PC. Integrity Master provides function and performance far beyond any other anti-viral or data integrity software, yet is easy enough for novice users. Integrity Master is the recommended anti-virus program in the "1995 PC Magazine Buyer's Guide" and is NCSA (National Computer Security Association) certified as an anti-virus product. Integrity Master features:

- Integrity Master recognizes known viruses by name and will describe their characteristics and then guide you through their removal.

- It can detect not only existing viruses, but also as yet unknown viruses. Unlike other programs, which you must constantly update to keep ahead of the current crop of viruses, Integrity Master continues to protect you.

- Unlike other programs, it detects sectors and files which were damaged by a virus not just those that were infected.

- Integrity Master checks your CMOS configuration memory and provides an intelligent display of any important changes. If needed, it can restore your CMOS memory (the full CMOS, not just the old 64 byte PC/AT CMOS). This also allows your quick recovery when you need to replace your CMOS battery.

- Integrity Master understands which files and areas on your disk are special and provides special specific diagnosis and recovery if these areas have changed.

- Integrity Master can reload system sectors on disks which are so badly damaged that DOS can no longer recognize them.

- Integrity Master detects any form of file or program corruption, not just that caused by viruses. This makes Integrity Master a useful tool to provide PC security, change management and hardware error detection. Why spend your time merely checking for viruses when you can give your PC a complete check out with Integrity Master?

- Integrity Master provides easy to use menus with built in help and the experience of a PC integrity expert through its Integrity Advisor(TM) feature.

- Integrity Master is useful as an aid to PC security. If someone changes, adds or deletes any of your files you will know.

- Integrity Master is useful with disk diagnostics. You can run your normal test programs to check if your disk drive is working OK right now, but was it working correctly at 3 PM yesterday? Integrity Master will detect if a disk error damaged some data yesterday.

- You just restored your files from a backup. Are all the files really OK? Integrity Master will tell you.
- IM is NCSA (National Computer Security Association) certified as a virus scanner.
- You just deleted *.BAT rather than *.BAK. Integrity Master will tell you exactly which files you need to restore.
- Your hard disk is having problems. Now DOS will not even recognize it as a disk. IM can diagnose and then reload your partition and boot sectors to "fix" your disk.

Author/Publisher Information:

Stiller Research is a company specializing in operating systems related software owned and operated by Wolfgang Stiller. This expertise in operating systems makes Stiller Research uniquely capable in the areas of data integrity and viruses. Wolfgang Stiller is the author of PC Magazine's PCdata integrity toolkit and the accompanying article, published in the February 13, 1990 issue of PC Magazine.

Stiller Research has been producing top quality computer software at reasonable prices, continuously, since 1985.

What do I get when I order?

About... Click to go to an order form.

(From the Integrity Master documentation. Use the File|Print Topic menu item to print this page.)

You will be ordering directly from the author when you purchase Integrity Master. You will receive:

- The latest licensed version of Integrity Master direct from Stiller Research with availability of automatic updates.

- The 128 page professionally printed book: "Defeating Viruses and Other Threats to Data Integrity." This is a complete guide and reference manual for IM as well as a guide on data integrity and viruses. It now includes expanded information on: details of common viruses, how viruses mutate and spread, the virus underground, how to use advanced anti-virus tools, guidelines for consultants, stealth viruses, and why people write viruses.

- A guide to installing and safely using DOS 6, DoubleSpace, SmartDrive (also applies to other compression and cache programs). It contains the tips and step-by-step directions gained from helping hundreds of users.

- Special offers, including a ***free*** introductory CompuServe subscription ($39 value) with up to 2.5 hours of connect time. (This may be a time-limited offer so order today.)

- Exclusive three year virus updates. (Please read the link attached to the "More Info" button here for the caveats.)
  About...

- Twelve month free technical support for IM, which includes direct assistance (from Stiller Research) with virus attacks (if needed).

- Add on utilities to supplement the capabilities of Integrity Master:

  - Stiller Research's own high speed automatic run utility. This program will allow you run IM (or any other program) at specific intervals. This allows you to place IM in your AUTOEXEC.BAT file and have it run only once a day, once every X days, or even only on specific days of the week or month.

  - For a limited time, we're including free PC hardware and configuration analysis software. It analyzes your PC's configuration (base memory, extended/expanded memory, ports, CPU, BIOS, video and drives). This is great for tracking down hardware and configuration problems.

Three Year Anti-Virus Support

About...

(From the Integrity Master documentation.)

For three years from the date you purchase your copy of Integrity Master, Stiller Research will provide the following support at our expense:

- If we discover a virus which can infect your PC and not be detected by Integrity Master, we will notify you as soon as we confirm this threat.

    This refers to Integrity Master's ability to detect unknown viruses by detecting changes to affected files or system areas on your PC. ***This does not refer to notification each time a virus appears which we do not recognize by name as a known virus.*** Since new viruses appear daily, this would be too costly.

    Please read the chapter on integrity checking for details on how Integrity Master detects (new) unknown viruses. Clearly, Integrity Master can't name and otherwise identify a newly created virus. This virus won't even have a name until it is analyzed and a name is agreed upon. (In many cases, new viruses still can be identified by name, since most new viruses are not really new but are modifications of existing viruses. Integrity Master works by detecting certain core virus characteristics which are often still present in a modified virus.)

- We will provide instructions on what precautions to take and deliver a version of Integrity Master designed to handle this virus as soon as it's available.

- This offer applies only to the hardware upon which you originally installed Integrity Master and the DOS operating environment.

Order Form

(Use the File|Print Topic menu item to print this page.)
If you require multiple copies or a site license, Click Here.

Integrity Master(tm) ordering information: To order quickly, call Advanced Support Group at **(800) 788-0787** (toll free) or **(314) 256-3130** or **fax to (314) 966-1833** with VISA or MasterCard. Ask for **Integrity Master, CK Special Offer**.

For mail orders, please fill out the following and mail to:
Stiller Research, **Dept CK**
2625 Ridgeway Street
Tallahassee, FL 32310 USA

Name:___________________________________ Title:____________________

Company:____

Address:__________________________________ City:____________________

State:______________ Zip:________________ Country:_________________

Date:____/____/____ Type of PC: ____________________ DOS Version:___

Disk: 5-1/4" ___ 3-1/2" ___ Telephone: ________________________________

Description	Qty	Price	Each	Total
CK Integrity Master Package (1st copy) Shipping & Handling (this copy)	1	$35.00 $ 4.50	$39.50	$39.50
Outside U.S./Canada extra charge ($5 per copy)		$ 5.00	$_____	
Add $6 for non-prepaid purchase orders	—>	———>	———>	
Subtotal (Use current exchange rate if non-US currency)	—>	———>	———>	
Florida residents add local tax (6-7%)	—>	———>	———>	
Total enclosed. (Checks accepted in currency from Australia, Belgium, Canada, England, France, Germany, Ireland, Japan, or Switzerland.) No US$ checks from non-US banks please.	—>	———>	———>	$_____

Reminder: If you are outside of the U.S. or Canada, did you include the extra $5.00 for overseas shipping as well as the $4.50 (basic shipping)?

If you send cash, please register your letter to confirm delivery; we can not be responsible for cash lost in the mail. Please do **not** sent currency other than US dollars in the form of cash.

Release date for this tutorial is on the About page; if quite old, please call to check prices.

Thank you for your order!

Full Order Form

(Use the File|Print Topic menu item to print this page.)

Integrity Master(tm) ordering information: To order quickly, call Advanced Support Group at **(800) 788-0787** (toll free) or **(314) 256-3130** or **fax to (314) 966-1833** with VISA or MasterCard. Ask for **Integrity Master, CK Special Offer**.

For mail orders, please fill out the following and mail to:

Stiller Research, **Dept CK**
2625 Ridgeway Street
Tallahassee, FL 32310   USA

Name:___________________________________ Title:____________________

Company:____

Address:__________________________________ City:____________________

State:______________ Zip:________________ Country:________________

Date:____/____/____ Type of PC: ____________________ DOS Version:___

Disk: 5-1/4" ___ 3-1/2" ___ Telephone: ________________________________

Description	Qty	Price	Each	Total
CK Integrity Master Package (1st copy) Shipping & Handling (this copy)	1	$35.00 $ 4.50	$39.50	$39.50
Added full copies (includes book/disk) (See table for amount per copy) Shipping & Handling (per copy)		$_____ $ 4.50	$_____	
Added seats (site license) ...(See table for amount per copy)		$_____	$_____	
Extra book/disk sets (site license only) Shipping & Handling (per copy)		$10.00 $ 4.50	$12.00	
Outside U.S./Canada extra charge ($5 per copy)		$ 5.00	$_____	
Add $6 for non-prepaid purchase orders	—>	———>	———>	
Subtotal (Use current exchange rate				

if non-US currency)	—>	———>	———>	
Florida residents add local tax (6-7%)	—>	———>	———>	
Total enclosed. (Checks accepted in currency from Australia, Belgium, Canada, England, France, Germany, Ireland, Japan, or Switzerland.) No US$ checks from non-US banks please.	—>	———>	———>	$_____

Reminder: Did you include $4.50 shipping/handling for each copy of IM that includes a book and disk? If you are outside of the U.S. or Canada, did you include the extra $5.00 for overseas shipping as well as the $4.50 (basic shipping) for each copy?

If you send cash, please register your letter to confirm delivery; we can not be responsible for cash lost in the mail. Please do **not** sent currency other than US dollars in the form of cash.

Release date for this tutorial is on the About page; if quite old, please call to check prices.

Thank you for your order!

Quantity/Site License Information

About... Click to go to an order form.

(From the Integrity Master documentation. Use the File|Print Topic menu item to print this page.)

If you wish to use Integrity Master on more than one PC, you must license multiple copies. There are two ways to do this.

- One way is to simply purchase more than one copy; you will get a price reduction on multiple copies. In this case, you will get complete packages including the book and disk.

- The other way is to purchase a site license for the extra copies. In this case, you do not get extra copies of the book and diskettes unless you specifically order them, but you pay a lower price than if you had ordered the complete package.

(Note: site licenses are generally less expensive than quantity orders unless you need complete copies of the manual and disk with each licenesed copy)

Quantity Orders:

Please use this table if you want to use Integrity Master on multiple PCs, with the complete Integrity Master package including book and disk for each PC. To order from this table, select the number of ***additional*** copies you wish to order. You must order the first copy at full price and then select the number of additional copies from the table below. If you have already licensed your first copy (on an earlier order), you can cross out that price on the order form and pay only the price for the additional copies.

The following prices apply to Integrity Master packages after the first copy:

#***Additional*** copies	Price per additional copy
1 to 5	$30.00 (US) ea + S&H
6 to 10	$27.00 (US) ea + S&H
11 to 15	$25.00 (US) ea + S&H
16 to 20	$24.00 (US) ea + S&H
21 to 25	$23.00 (US) ea + S&H
26 to 30	$22.25 (US) ea + S&H
31 to 35	$21.60 (US) ea + S&H
36 to 40	$21.00 (US) ea + S&H
41 to 45	$20.50 (US) ea + S&H
46 to 50	$20.10 (US) ea + S&H
51 to 55	$19.80 (US) ea + S&H
56 to 60	$19.50 (US) ea + S&H
61 to 65	$19.25 (US) ea + S&H
66 to 70	$19.00 (US) ea + S&H
71 to 80	$18.75 (US) ea + S&H
81 to 100	$18.50 (US) ea + S&H
101 +	$18.25 (US) ea + S&H

Example of ordering multiple copies:

To order 12 copies, you would pay $39.50 for the first copy which includes $4.50 for domestic shipping. You now want to order 11 additional copies. Looking in the table, you see that 11 copies are $25.00 each. $25 plus $4.50 shipping brings the unit cost to 29.50. The total on the order would be $364 which is $39.50 plus 11 times 29.50. If you live outside the US or Canada you would need to include $5 *for each copy* to cover the additional shipping and support expenses.

Site License:

Please use this table if you want to use Integrity Master on multiple PCs, and you do ***not*** need the complete package including book and disk for each PC. ***Note, that site licenses do not include books or disks***. You can order additional copies of the book and disk for $7.50 each with your site license.

To order from this table, select the number of ***additional*** PCs you wish to license to use Integrity Master. You must order the first copy at full price and then select the number of additional licensed copies. This way each site license has at least one copy of the book and disk. If you have already licensed your first copy (on an earlier order), you can cross out that price on the order form and pay only the price for the additional copies.

To qualify for a site license:

- You must purchase at least one book/disk set and then select the number of additional PCs which may use Integrity Master.

- You must designate a single point of contact. This need not be a particular person, but should be a single address with a single telephone number to coordinate all purchasing and support activity. Any requests for technical support or license upgrades must go through that person or office before contacting Stiller Research.

- Site licenses may ***not*** be transferred to another organization or person.

These licenses can be upgraded at any time for only an incremental payment:

#***Additional*** PCs	Price per additional license
1 to 5	$20.00 (US) each
6 to 10	$18.00 (US) each
11 to 15	$16.00 (US) each
16 to 20	$15.00 (US) each
21 to 25	$14.30 (US) each
26 to 30	$13.75 (US) each
31 to 35	$12.95 (US) each
36 to 40	$12.60 (US) each
41 to 45	$12.30 (US) each
46 to 49	$12.05 (US) each
50 to 60*	$11.95 (US) each
61 to 70	$11.70 (US) each
71 to 80	$11.55 (US) each
81 to 90	$11.40 (US) each

91 to 100	$11.30 (US) each
101 to 120	$11.20 (US) each
121 to 140	$11.11 (US) each
141 to 160	$11.05 (US) each
160 to 180	$11.00 (US) each
180 to 200	$10.95 (US) each
201 +	$10.90 (US) each

*Site licenses for 50 or more PCs include automatic mailing of the new releases of Integrity Master at no extra charge for twelve months.

Additional copies of the book and disk are available for $10.00 each (plus $4.50 S&H each) to site license customers.

Example of ordering a site license:

To use IM on 161 PCs, you would pay $39.50 for the first copy which includes $4.50 for domestic shipping. You now want to order 160 additional licenses. Looking in the table, you see that 160 licenses are $11 each. No shipping is needed for the additional licenses. The total on the order would be $1799.50 which is $39.50 plus 160 times $11. If you live outside the US or Canada you would need to include $5 for the book and disk to cover the additional shipping and support expenses.

Special Site License

If you are a large organization and have your own help desk, we offer special low-support license rates of only $6.00 per license, for licenses between 100 and 500 copies. For over 500 licenses, we offer a $5.00 rate. Under this special license, all users must report and document any problems to the central help desk (or one of our authorized agents if prior arrangements are made with that agent). Problem reports may still be sent directly to Stiller Research.

Dealer inquiries are welcome. We also offer special educational discounts to public educational institutions. Please contact us for details.

Tutorial Map

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

Electronic Mail

Electronic mail is the computer equivalent of mail delivered by the local post office. Via networks, information can be easily moved from computer to computer. Certain computers on a network can be set up as "post offices" such that they accept mail you send to another person and then deliver that mail when the person attaches to the network. Electronic mail can be constrained to local connections or be delivered throughout the world. As networks become more widespread electronic mail (often called E-mail) is becoming more popular.

Cleaning

Not all anti-virus programs will clean your system. Not all viruses can be cleaned; some damage files or sections of the disk.

If the program has found a virus it's usually best to do a complete backup or at least a backup of your most important files before attempting to clean your disk. Not all viruses can be cleaned without damage to either files or a disk.

Why All Disks?

Viruses are capable of hiding anywhere and everywhere. Any floppy disk can have one and without checking you never know. Probably the biggest source of reinfection is missing a virus on a floppy disk you've stored away and then use later.

Write Protected?

If, by chance, your system has a boot sector virus the only way it can move from machine to machine is via a floppy disk. If every floppy that can be is write protected before putting it in a disk drive then when an active virus attempts to write to the disk it will not be able to do so.

Of course, there are disks you must write to and can't have write protected. Make certain you check the disks after writing to them and write protect them as soon as possible.

Boot Sector

When a disk is formatted (it doesn't matter if it's a system or data disk) the very first portion of the disk is set aside for two main purposes: storing information about the disk and storing a short program that either puts a message on the screen saying the disk cannot be used to start the computer if it's a data disk or starts to load the operating system if it's a system disk which can start the computer. This special sector is numbered 0,0 and is called the Boot Sector.

Checksum

A unique value obtained by applying a special formula to a stream of characters (e.g., a simple checksum would add each character in the stream to the results of adding every prior character). If the proper formula is used the checksum process can produce a unique value that will be a telltale to determine if the file has changed since the last checksum was computed.

If you consider simply adding all characters as your checksum you can see how easy that is to defeat: you would not be able to detect the reversal of every other character in the entire file. This is why such advanced functions as cyclic-redundancy checks (CRCs) and, in even more secure systems, cryptographic check values are used.

Worm

A worm is a self-reproducing program that does not infect other programs as a virus will, but instead creates copies of itself, that create even more copies. These are usually seen on networks and on multi-processing operating systems, where the worm will create copies of itself that are also executed. Each new copy will create more copies quickly clogging the system. The so-called ARPANET/INTERNET "virus" was actually a worm. It created copies of itself through the network, eventually bringing the network to its knees. It did not infect other programs as a virus would, but simply kept creating copies of itself that would then execute and try to spread to other machines.

Trojan Horse

These are named after the Trojan horse, which delivered soldiers into the city of Troy. Likewise, a trojan program is a delivery vehicle; a program that does something undocumented which the programmer intended, but that the user would not approve of if she knew about it. The trojan program appears to be a useful program of some type, but when a certain event occurs, it does something nasty and often destructive to the system.

Some researchers consider a virus a particular case of a Trojan horse; others believe that if a virus does not do any deliberate damage it cannot be classed as a Trojan. In common use, most people use Trojan to refer to a non-replicating malicious program.

Logic Bomb

Just like a real bomb, a logic bomb will lie dormant until triggered by some event. The trigger can be a specific date, the number of times executed, a random number, or even a specific event such as deletion of an employee's payroll record. When the logic bomb is triggered, it will usually do something unpleasant. This can range from changing a random byte of data somewhere on your disk to making the entire disk unreadable. Changing random data may be the most insidious attack since it generally causes substantial damage before anyone notices that something is wrong. It's vital to have software in place that quickly detects such damage. Although you can detect it after the fact, there is unfortunately no way to prevent a well written logic bomb from damaging your system.

AUTOEXEC.BAT

This batch file runs automatically when DOS starts if it's found. You can use it to perform standard functions during the time the computer is starting.

AUTOEXEC.BAT is optional.

Brownouts

Brownouts are lower voltages at the outlets. Usually they are caused by an extraordinary drain on the power system. Frequently you will see a brownout during a heatwave when more people than normal have their air conditioners on full. Sometimes these power shortages will be "rolling" across the area giving everyone a temporary brownout. Maybe you'll get yours just as that important file is being written to disk.

Voltage Spikes

Spikes are far more common than most people realize.

- Industrial processes on the same power grid can often cause spikes when large motors or circuit breakers turn on and off.

- If a driver hits a power pole and the power grid has to adapt to the loss of that single section, there will likely be a spike on the rest of the grid.

- Even your refrigerator or air conditioner cycling on and off can cause local spikes that can affect your computer.

- Lightning in your area often places a spike on the power lines.

Frequency Shifts

While very infrequent, if the line frequency varies from the normal 60 Hz (or 50 Hz in some countries), the power supply on the computer can be affected and this, in turn, can reflect back into the computer causing data loss.

Proper Plural

The correct English plural of "virus" is "viruses." The Latin word is a mass noun (like "air"), and there is no correct Latin plural.

DOS Boot Sectors

The very first sector on disk or diskette that DOS is aware of is the boot sector. From a DOS perspective, this is the first sector on the disk. This sector usually contains an executable program whether the disk is bootable or not. Since this program is executed every time you power on or boot your PC, it is very vulnerable to virus attack. Damage to this sector can make your disk appear to be unreadable. This sector is rewritten whenever you do a "SYS" or a "FORMAT /S" to a disk.

Warning: Even a non-bootable floppy can contain a virus in the boot sector. If you leave the floppy in your PC when you power on or boot, you will be infected even though the PC won't successfully boot from that floppy.

Partition Sectors

On hard (fixed) disk drives, the very first sector is the partition sector (also known as the master boot record or partition table). Each physical hard disk drive has one of these sectors. A single physical disk can be partitioned into one or more logical disks. For example, you may have a physical drive partitioned into C: and D: logical disks so that your single physical disk appears (to DOS) to be two logical disks. The single partition sector contains the information that describes both logical disks. If the partition sector is damaged, then DOS may not even recognize that your disk exists.

The partition sector also contains a program that is executed every time you power up or boot your PC. This program executes and reads the DOS boot sector that also contains a program. Many viruses plant their code in the partition sector.

Sparse Infector

A virus might use techniques to minimize the probability of its being discovered. It might, for example, only infect every 20th time a file is executed; it might only infect files whose lengths are within narrowly defined ranges or whose names begin with letters in a certain range of the alphabet.

A virus which uses such techniques is often termed a sparse infector.

Armored Viruses

Armored is a class that overlaps many other classes of viruses.

Basically, an armored virus uses special "tricks" which are designed to foil anti-virus researchers. An anti-virus researcher who wants to find out how a virus works must follow the instruction codes in the virus. By using a variety of methods, virus writers can make this disassembly task quite a bit more difficult. Such a virus can be said to be armored.

An early virus, Whale, made extensive use of these techniques.

Detection Algorithm

Not all new viruses can be detected via a string search. Those that randomly encrypt themselves and/or change their configuration (polymorphic viruses) present a different face, often with each infection, to any scanner. For this reason, scanners must now also look at the start of programs and follow the code to determine if it appears "normal" or has the characteristics of a virus (e.g., uses the various DOS calls that allow the virus to install itself into memory).

Data Integrity Software

Data integrity software can be very helpful in determining exactly what has been affected by whatever problem has come up (hardware, software, virus, or whatever).

If you accidently delete files, integrity software will tell you exactly what was deleted; no more guessing when you run your undelete utility.

If files are modified by a virus, you can tell which have been so affected and replace them.

If you have to restore backed up files, integrity software can tell you if the restore operation actually restored the latest file and/or did so correctly.

Having reliable integrity checking available to you can help in multiple ways.

Current Backups

Current backups are very important to correct recovery from problems. You can have all the data recovery utilities in the world, but if the Michelangelo virus activates on your system they will be worthless without a good backup to restore from. Viruses are not the only problem a good backup helps with; the simple fact is: **hard disks fail**. It can't be said often enough or loud enough. If you don't have a good backup, everything is gone in this situation.

A good backup does not mean you have to back up everything on the disk every day (or hour, or whatever). Many things on the disk don't change very often. But, if you value your data, you should make a backup of that data every time you've changed it enough so that you would not want to re-enter it should something fail. Only you can say if this is once an hour, day, week, or year.

Whatever the period, however: just **do it!**

Utility Tools

Utility tools (there are many) are optional but can be handy for those times where they can help. The problem is that if you don't know what you are doing there is some chance that using a utility tool can actually make matters worse. As an example, if you boot from a clean floppy disk on a system infected with the Monkey virus, you will not be able to access the hard disk. You may be tempted at this point to use FDISK, FORMAT, and restore from backup to rebuild the disk from scratch. This is totally unnecessary as any good anti-virus utility can remove this virus without problems. Indeed, using some 3rd party DOS tools can also recover by rebuilding the partition information without the need for reformatting the disk.

If you have and use powerful utility tools, please understand the tools and what their effects are before using them. Education is important.

On-going Hoax Info

Follow the alt.folklore.urban newsgroup for on-going information. The alt.folklore.urban FAQ is available via FTP from cathouse.org in the pub/cathouse/urban.legends/AFU.faq directory. It is also available on the World Wide Web at http://cathouse.org/UrbanLegends/AFUFAQ/

For CIAC offical information FTP to ciac.llnl.gov and look in the /pub/ciac/sectools/unix directory. The URL is ftp://ciac.llnl.gov/pub/ciac/sectools/unix/. The URL for the CIAC home page on the World Wide Web is: http://ciac.llnl.gov/ciac/

Regarding the Good Times Virus hoax:

For America Online's official statement keyword "virus2" on America Online.

For the Good Times Virus Hoax FAQ FTP to usit.net and look in the pub/lesjones directory. The URL is: ftp://usit.net/pub/lesjones/GoodTimes-HoaxFAQ.txt

On-going Virus Info

Follow on-going discussions in the newsgropu comp.virus and, to a lesser extent, in comp.security.misc. The comp.virus discussions are summarized and sent to a mailing list.

To subscribe to the Virus-L list send E-mail to listserv@lehigh.edu and in the body of the message include the line:

```
sub virus-l <your address>
```

(Replace <your address> with your E-mail address.)

A companion list distributes computer security alerts (Valert-L). Send E-mail to the above address with the following in the body of the message (again, substitute your E-mail address):

```
sub valert-l <your address>
```

Nth-Complexity Infinite Binary Loop

There is no such thing. Also, since a processor runs at a defined internal speed regardless of what it is doing, the idea that it will burn out if accessing the same internal location is a fabrication.

Quantity Discount Table

#***Additional*** copies	Price per additional copy
1 to 5	$30.00 (US) ea + S&H
6 to 10	$27.00 (US) ea + S&H
11 to 15	$25.00 (US) ea + S&H
16 to 20	$24.00 (US) ea + S&H
21 to 25	$23.00 (US) ea + S&H
26 to 30	$22.25 (US) ea + S&H
31 to 35	$21.60 (US) ea + S&H
36 to 40	$21.00 (US) ea + S&H
41 to 45	$20.50 (US) ea + S&H
46 to 50	$20.10 (US) ea + S&H
51 to 55	$19.80 (US) ea + S&H
56 to 60	$19.50 (US) ea + S&H
61 to 65	$19.25 (US) ea + S&H
66 to 70	$19.00 (US) ea + S&H
71 to 80	$18.75 (US) ea + S&H
81 to 100	$18.50 (US) ea + S&H
101 +	$18.25 (US) ea + S&H

Site License Table

#***Additional*** PCs	Price per additional license
1 to 5	$20.00 (US) each
6 to 10	$18.00 (US) each
11 to 15	$16.00 (US) each
16 to 20	$15.00 (US) each
21 to 25	$14.30 (US) each
26 to 30	$13.75 (US) each
31 to 35	$12.95 (US) each
36 to 40	$12.60 (US) each
41 to 45	$12.30 (US) each
46 to 49	$12.05 (US) each
50 to 60*	$11.95 (US) each
61 to 70	$11.70 (US) each
71 to 80	$11.55 (US) each
81 to 90	$11.40 (US) each
91 to 100	$11.30 (US) each
101 to 120	$11.20 (US) each
121 to 140	$11.11 (US) each
141 to 160	$11.05 (US) each
160 to 180	$11.00 (US) each
180 to 200	$10.95 (US) each
201 +	$10.90 (US) each

Educational Discount

There is a $2 per PC discount for educational institutions. This applies over and above the quantity/site license price tables. Further, educational institutions will be sent free mailed upgrades if 25 or more Pcs are licensed (versus 50 Pcs for non-educational purchases).

For example, if there is a site license ordered for 100 copies the tables indicate the normal price would be $11.30 per seat. An educational institution would pay $9.30. Shipping and handling charges remain the same.

License & Legal Information

About...

Click to learn how to protect your computer and obtain other tutorials of interest.

License for Use and Distribution

Tutor.COM - Viruses a freeware program. It is ***NOT*** a public domain program. It is copyrighted by Computer Knowledge and it and all accompanying materials are protected by United States copyright law and also by international treaty provisions.

Tutor.COM - Viruses requires no payment of license fees for its individual use as an educational tool. No royalties are required for distribution so long as distribution charges only cover the costs of such distribution (plus a nominal profit if the distribution channel is a profit-making channel). **Under no circumstances is payment of such fees to be represented or understood to constitute legal ownership of this tutorial or any of its associated files.**

Any distribution for profit beyond that described just above requires written permission from Computer Knowledge and payment of negotiated royalties.

You may not use, copy, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program except as provided in this agreement. Any such unauthorized use shall result in immediate and automatic termination of this license.

In no case may this product be bundled with hardware or other non-shareware software without written permission from Computer Knowledge (PO Box 5818, Santa Maria, CA 93456).

All distribution of Tutor.COM - Viruses is further restricted with regard to sources which also distribute virus source code and related virus construction/creation materials. **The tutorial may not be made available on any site, CD-ROM, or with any package which makes available or contains viruses, virus source code, virus construction programs, or virus creation material.**

Consult the VENDINFO.DIZ data record in the original distribution files for all distribution requirements. It is hereby incorporated by reference. Any distribution satisfying all the distribution requirements expressed in that text and data record is hereby authorized. In no case will this program be distributed without its VENDINFO.DIZ file.

Permission to distribute the Tutor.COM-Viruses program is not transferable, assignable, saleable, or franchisable. Each entity wishing to distribute the package must independently satisfy the terms of this limited distribution license.

U.S. Government Information: Use, duplication, or disclosure by the U.S. Government of the computer software and documentation in this package shall be subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013 (Oct 1988) and FAR 52.227-19 (Jun 1987). The Contractor is Computer Knowledge, PO Box 5818, Santa Maria, CA 93456-5818.

Computer Knowledge may revoke any permissions granted here, by notifying you in writing.

All rights not expressly granted here are reserved to Computer Knowledge.

Warranty

Limited warranty: This software is provided on an "as is" basis. Computer Knowledge disclaims all warranties relating to this software, whether expressed or implied, including but not limited to any implied warranties of merchantability or fitness for a particular purpose. Neither Computer Knowledge nor anyone else who has been involved in the creation, production, or delivery of this software shall be liable for any indirect, consequential, or incidental damages arising out of the use or inability to use such software, even if Computer Knowledge has been advised of the possibility of such damages or claims. The person using the software bears all risk as to the quality and performance of the software.

Some jurisdictions do not allow limitation or exclusion of incidental or consequential damages, so the above limitations or exclusion may not apply to you to the extent that liability is by law incapable of exclusion or restriction.

In no event shall any theory of liability exceed the license fee paid to Computer Knowledge or any distributor of this tutorial.

This agreement shall be governed by the laws of the State of California excluding the application of its conflicts of law rules and shall inure to the benefit of Computer Knowledge and any successors, administrators, heirs and assigns. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be brought only in a STATE or FEDERAL COURT of competent jurisdiction located in Santa Barbara County, California. The parties hereby consent to in personam jurisdiction of said courts.

Any suit or other legal action, claim or any arbitration relating in any way to this agreement or software covered by it must be officially filed or officially commenced no later than three months (90 days) after your first use the software.

This agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

If any part of this agreement is found void and unenforceable, it will not affect the validity of the balance of the agreement, which shall remain valid and enforceable according to its terms.

You agree that the software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations.

Using this tutorial means that you agree to these terms and conditions. This agreement may only be modified in writing signed by an authorized officer of Computer Knowledge.

About...
Contents