he following is a listing of known Macintosh Virus's.   Thanks to John Norstad's excellent Disinfectant Program for some of the Virus Info used in this chapter.

MODM

Infects System file and application files.   May cause system crashes on infected computers. Also known as the zero virus.

HC

This virus infects only HyperCard stacks and can only spread through HyperCard stacks. When an infected stack is run the Macintosh may hum strangely and HyperCard painting tool symbols will appear at random parts of the screen.

The Scores Virus

The Scores virus was written by a disgruntled programmer.   It attacks only two applications which were under development at his former company.   Neither of the two applications were ever released to the general public.   Scores was first discovered in the Spring of 1988

Scores is also sometimes referred to as the "Eric," "Vult," "NASA," and "San Jose Flu" virus.

There is an easy way to see if you have a Scores infection.   Open your System folder and check the icons (View by Icon under the Views menu) for the Note Pad and Scrapbook files. They should have distinctive icons under System 7, or look like little Macintoshes under System 6.   If instead the look like blank sheets of paper with turned-down corners, there is a good chance your software may have been infected by scores.

t is possible to be only partially infected by the Scores virus and still have normal Note Pad and Scrapbook icons.   I still recommend that your run Disinfectant to make sure your Macintosh is not infected, even if you have normal icons.

Scores infects your System, Note Pad, and Scrapbook system files.   It also creates two invisible files in your System folder named "Scores" and Desktop".   You cannot see invisible files without the aid of ResEdit (Available from most online services).   Do not confuse Score's invisible Desktop file with the Finder's invisible Desktop file; they have nothing to do with each other.   The Finder's Desktop files lives at the root level on your disk, outside the system folder.   On the other hand, Score's Desktop file lives inside the System folder.   Also, Score's Desktop file has an extra space character at the end of its name.

Scores cannot and does not infect or modify document files, only applications and system files.

Scores gets its name from the invisible "Scores" document it creates.

Two days after your system becomes infected, Scores begins to spread to each application you run.   The infection occurs between two and three minutes after you begin the application.   The Finder and DA Handler usually also become infected.   For technical reasons, some applications are immune to infection.

Scores does not intentionally try to do any damage other than to spread itself and attack two specific applications (never released to the public).   It does occupy memory and disk space, however, and this can cause problems all by itself.   People have reported errors printing and using MacDraw and Excel.   There are also several errors in Scores which could cause system crashes or other erroneous behavior.

There is a serious conflict between Scores and Apple's System Software release 6.0.4 and later System 6 releases.   In System 6.0.4, Apple began using some resources with the same type ID as those used by Scores.   When Scores infects the System file, it replaces Apple's versions of these resources with the Scores viral versions of the resources.   Once the virus has been deleted you should immediately replace the System with an original 'clean' copy of the System file.

The nVIR Virus

The nVIR virus first appeared in Europe in 1987 and in the United states in early 1988.   At least one variation of the virus was written.   We know of two strains, which are called "nVIR A" and "nVIR B".   This virus is also known as Hpat, nFLU, AIDS, MEV#, nCAM, and prod.

There are reports of an earlier version of nVIR which was malicious.   It destroyed files in the System folder.   This earlier version appears to be extinct, and anti-virus programmers have been unable to obtain a copy.

nVIR is simpler than Scores.   It infects the System file, but it does not infect the Note Pad or Scrapbook files, and does not create any invisible files.   nVIR begins spreading to other applications immediately, without the two day delay of the Scores virus.   Whenever a new application is run, it becomes infected immediately.   As with Scores, some applications are immune to infection, the Finder and DA Handler usually become infected, and document files are not infected or modified.

At first nVIR A and B only replicate.   When the System file is first infected, a counter is initialized to 1000. The counter is decremented by one each time the system is started up and it is decremented by two each time an infected application is run.

When the counter reaches zero, nVIR A will sometimes either say "Don't panic" (if MacinTalk is installed in the System folder) or beep. This will happen on system startup with a probability of 1/16. It will also happen, with a probability of 15/128, when an infected application is run. In addition, when an infected application is run, nVIR A may say "Don't panic" or beep twice with a probability of 1/256.

When the counter reaches zero, nVIR B will sometimes beep. The beep will happen on a system startup with a probability of 1/8. A single beep will happen when an infected application is run with a probability of 7/32. A double beep will happen when an infected application is run with a probability of 1/64.

It is possible for nVIR A and nVIR B to mate and reproduce, resulting in new viruses combining parts of their parents.

Unlike Scores, there is no way to tell that you have an nVIR virus unless you run an anti-virus program.

The nVIR virus got its name because one of the viral resources added to infected files is resource type "nVIR."

The INIT 29 Virus

The INIT 29 virus first appeared in late 1988. We do not know much about its origin. A second minor variant appeared in March, 1994. There are no significant difference's between the two strains. The original strain is called "INIT 29 A". The variant is called "INIT 29B".

INIT 29 is extremely virulent. It spreads very rapidly. Unlike Scores and nVIR, you do not have to run an application for it to become infected. Also, unlike Scores and nVIR, INIT 29 can and will infect almost any file, including applications, system files, and document files. Document files are infected, but they are not contagious. The virus can only spread via system files and application files.

INIT 29 has one side effect which reveals its presence. If you try to insert a locked floppy disk on a system infected by INIT 29, you will get the following alert:

> The disk "xxxxx" needs minor repairs.
> Do you want to repair it?

If you see this alert whenever you insert a locked floppy, it is a good indication that your system might be infected by INIT 29.

As with Scores and nVIR, INIT 29 does not intentionally try to do any damage other than spread itself. Nevertheless, it can cause problems. In particular, some people have reported problems printing on systems infected with INIT 29. We have also experienced many system crashes, problems with MultiFinder under System 6, and incompatibilities with several startup documents on systems infected with INIT 29.

One of the viral resources added to infected files by INIT 29 has the resource type "INIT" and the resource ID 29, after which the virus was named.

The ANTI Virus

There are two known strains of the ANTI virus.   Both strains were first discovered in France. The ANTI A strain was discovered in February, 1989, followed by the ANTI B strain discovered in September, 1990.

ANTI does not infect the System file.   It only infects applications and other files which resemble applications (e.g., Finder).   ANTI does not infect document files.   It is less contagious than the INIT 29 virus, but more contagious than the Scores and nVIR viruses.   It is possible for an application to become infected even if it is never run.

Due to a technical quirk, ANTI does not spread at all under System 7 or under System 6 when MultiFinder is in use.   It only spreads when Finder is used under System 6.

There is an error in ANTI which causes it to slightly damage applications.   Usually Disinfectant or other anti-virus program can repair them, but not perfectly.   If you experience problems with the application it should be replaced with a clean copy of the application.

For the technically inclined, the error in ANTI is that it clears all the resource attributes of the CODE 1 resource.   Disinfectant has no way to know the values of the original attributes, so it leaves them cleared on the repaired application.   The only effect of this error is that the repaired application may use memory slightly less efficiently than the original version, especially on old Macintoshes with the 64K ROMs.

As with other viruses, ANTI does not intentionally attempt to do any damage other than spread itself.   As with all viruses, however, it can still cause problems.

The string "ANTI" appears within the virus giving its name.

Even though the B strain of ANTI was not discovered until about 19 months after the A strain, it appears that the B strain was actually written before the A strain.   The A strain of the virus contains special code which neutralizes any copies of the B strain which it encounters.   It is possible for an application to be infected by both the neutralized version of the B strain and by the A strain.

Other than the special code in the A strain which looks for and neutralizes the B strain, there are only minor technical differences between the two versions of the virus.

The MacMag Virus

The MacMag virus appeared in December, 1987.   This virus is also known as the "Drew," "Brandow," "Aldus," and "Peace" virus.   It was named after the Montreal offices of MacMag magazine, from where it originated.

Unlike the other viruses, MacMag does not infect applications, only System files.   It originated as a HyperCard stack named "New Apple Products."   The stack contained some exceptionally poorly digitized pictures of the then new Apple scanner.   When the stack was run, the virus spread to the currently active System file.   When other floppy disks containing System files were subsequently inserted in a floppy disk drive, the virus spread to the System files on the floppies.

Since applications are not infected by MacMag, it spreads much more slowly than the other viruses (people share System files much less frequently than they share applications). Even though the virus originated on a HyperCard stack, it does not spread to other stacks, only to System files.

MacMag was programmed to wait until March 2, 1988, the anniversary of the introduction of the Mac II. The first time the system was started up on March 2, 1988, the virus displayed a message of peace on the screen and then deleted itself from the System file.

Since MacMag was programmed to self-destruct, it is unlikely that your software is infected with the this virus.

There are two slightly different versions of MacMag. The differences were minor and both versions were programmed to behave identically.

The WDEF Virus

The WDEF virus was first discovered in December, 1989 in Belgium and in one of our labs at Northwestern University. Since the initial discovery, it has also been reported at many other locations, and we now know that it is very widespread. We know of two strains, which we call "WDEF A" and "WDEF B."

WDEF only infects the invisible "Desktop" files used by the Finder. With a few exceptions, every Macintosh disk contains one of these files. WDEF does not infect applications, document files, or other system files. Unlike the other viruses, it is not spread through the sharing of applications, but rather through the sharing and distribution of disks (usually floppy disks.)

WDEF spreads from disk to disk very rapidly. It is not necessary to run an application for the virus to spread.

Fortunately for all of you System 7 users, System 7 is completely immune to the WDEF virus.

The WDEF A and WDEF B strains are very similar. The only significant difference is that WDEF B beeps every time it infects a new Desktop file, whereas WDEF A does not beep.

Although the virus does not intentionally try to do any damage, WDEF contains errors which can cause very serious problems. In particular, the virus causes newer Mac models to crash almost immediately after insertion of an infected floppy (IIci and later computers). The virus also causes other Macs to crash more frequently than usual and it can damage disks. The virus also causes problems with the proper display of font styles. In particular, it often causes problems with the "outline" font style. Many other symptoms have also been reported and it appears that the errors in the virus can cause almost any kind of problem with the proper functioning of your Macintosh.

You can remove a WDEF infection from a disk by rebuilding the desktop. This is also the only way to get rid of a WDEF infection under System 7.

Even though AppleShare servers do not use the normal Finder Desktop file, many servers have an unused copy of this file. If the AppleShare administrator has granted the "make changes" privilege to the root directory on the server, then any infected user of the server can infect the Desktop file on the server. If a server Desktop file becomes infected, performance on the network will be very severely degraded. For this reason, administrators should never grant the "make changes" privilege on server root directories. We also recommend deleting the Desktop file if it exists. It does not appear that the virus can spread from an AppleShare server to other Macs on the network.

The WDEF virus can spread from a TOPS server to a TOPS client if a published volume's Desktop file is infected and the client mounts the infected volume. It does not appear, however, that the virus can spread from a TOPS client to a TOPS server.

If you use ResEdit to search for WDEF resources, do not be alarmed if you find them in files other than the Finder Desktop files. WDEF resources are a normal part of the Macintosh operating system. Any WDEF resource in a Finder Desktop file, however, is a reason for concern.

The ZUC Virus

There are three known strains of the ZUC virus. All of them were discovered in Italy. The virus is named after the reported discoverer of the first strain, Don Ernesto Zucchini. ZUC A was discovered in March 1990, ZUC B in November, 1990, and ZUC C in June, 1991.

ZUC only infects applications. It does not infect system files or document files. Applications do not have to be run to become infected.

ZUC A and B were timed to activate on March 2, 1990 or two weeks after an application becomes infected, whichever is later. Before that date, they only spread from application to application. After that date, approximately 90 seconds after an infected application is run, the cursor begins to behave unusually whenever the mouse button is held down. The cursor moves diagonally across the screen, changing direction and bouncing like a billiard ball whenever it reaches any of the four sides of the screen. The cursor stops moving when the mouse button is released.

ZUC C is very similar to ZUC A and B. The only significant differences are that ZUC C was timed to cause the unusual cursor behavior only during the period between 13 and 26 days after an application becomes infected, but not earlier than August 13, 1990, and ZUC C causes the cursor to begin to unusually approximately 67 seconds rather than 90 seconds after an infected application is run.

The behavior of the ZUC virus is similar to that of a desk accessory named "Bouncy." The virus and the desk accessory are different and they should not be confused. The desk accessory does not spread and it is not a virus. ZUC does spread and it is most definitely a virus.

ZUC has two noticeable side effects. On some Macintoshes, the A and B strains can cause the desktop pattern to change. All three strains can also sometimes cause long delays and an unusually large amount of disk activity when infected applications are opened. The virus also adds 1256 bytes of code to the end of the first executed CODE resource

ZUC can spread over a network from individual Macintoshes to servers and from servers to individual Macintoshes.

Except for the unusual cursor behavior, ZUC does not attempt to do any damage.

ZUC does not change the last modification date when it infects a file, so it is almost impossible to trace its source.

The MDEF Virus

There are four known strains of the MDEF virus. All of them were discovered in Ithaca, New York. The MDEF A strain was discovered in May, 1990 and is also sometimes called the "Garfield" virus. The MDEF B strain was discovered in August, 1990 and is also sometimes called the "Top Cat" virus. The C and D strains were discovered in October, 1990 and January, 1991, respectively.

Prompt action by computer security personnel and investigators of the New York State Police resulted in the identification of the author. The author, a juvenile, was released into the custody of his parents after consultation with the district attorney. The same person was responsible for writing the CDEF virus.

The A, B, and C strains of MDEF infect both applications and the System file. They can also infect document files, other system files, and Finder Desktop files. The finder and DA Handler also become infected. The System file is infected as soon as an infected application is run. Other applications become infected as soon as they are run on an infected system.

The D strain of MDEF only infects applications, not system files or document files. Applications can become infected even if they are never run. An application infected by MDEF D beeps every time it is run. We do not believe that the D strain of MDEF was ever released to the public.

The MDEF viruses do not intentionally attempt to do any damage, yet they can be harmful. They do not display any messages or pictures.

The MDEF B and C strains attempt to bypass some of the popular protection INITs.

The MDEF C strain contains a serious error which can cause crashes and other problems.

The MDEF D virus can damage some applications in such a way that it cannot be repaired. You should delete any infected applications you have and replace them with a clean copy.

The MDEF viruses are named after the type of resource they use to infect files. MDEF resources are a normal part of the Macintosh system, so you should not become alarmed if you see them with ResEdit.

The MDEF, WDEF, and CDEF viruses have similar names, but they are completely different and should not be confused with each other.

The Frankie Virus

The Frankie virus is very rare.

Frankie only affects some kinds of Macintosh emulators running on Atari computers. We have reports that it was targeted against pirated versions of the Aladdin emulator. It does not affect the Spectre emulator.

Frankie does not spread or cause any damage on any of the regular Apple Macintosh computers.

After a time delay, Frankie draws a bomb icon and the message "Frankie says: No more piracy!" at the top of the Atari screen, and the proceeds to crash the Atari.

Frankie only infects applications, not system files or document files. The Finder also usually becomes infected. Applications do not have to be run to become infected. For technical reasons, the virus only spreads under Finder, not MultiFinder.

The CDEF Virus

The CDEF virus was first discovered in Ithaca, New York, in August, 1990. The same person who wrote the MDEF virus also wrote the CDEF virus. See the description of the MDEF virus for details. The CDEF virus is quite widespread.

CDEF is very similar to the WDEF virus. It only infects the invisible "Desktop" files used by the Finder. It does not infect applications, document files, or other system files. It spreads from disk to disk very rapidly.

Fortunately, System 7 is completely immune to the CDEF virus.

Although the behavior of the CDEF virus is similar to that of the WDEF virus, it is not a clone of WDEF. it is a completely different virus.

The virus does not intentionally try to do any damage. AS with all viruses, however, the CDEF virus is still dangerous. We have had many reports of problems on CDEF-infected systems.

As with the WDEF virus, you can remove a CDEF infection from a disk by rebuilding the desktop.

The CDEF virus is named after the type of resource it uses to infect files. CDEF resources are a normal part of the Macintosh operating system, so you should not become alarmed if you see them with ResEdit or some other tool. Any CDEF resource in a Finder Desktop file is cause for concern.

A new version of the CDEF virus was discovered in February, 1993. There are only minor technical differences between the new version and the original virus.

The MBDF Virus

The MBDF virus was first discovered in Wales in February, 1992. Several popular Internet archive sites contained some infected games for a short period of time, so number of people around the world were affected. The games were named a "10 Tile Puzzle" and "Obnoxious Tetris."

In addition to these two games, a third game named "Tetricycle" or "tetris-rotating" was a Trojan horse which installed the virus.

Two undergraduate students at Cornell University were quickly apprehended shortly after the virus was discovered. They pleaded guilty to charges of second-degree computer tampering for writing and spreading the MBDF virus. They were sentenced to community service and restitution of damages. A third student at Cornell also pleaded guilty to a charge for helping to spread the virus, and was sentenced to community service.

The MBDF virus infects both applications and the System file. It also usually infects the Finder and several other system files. The System file is infected as soon as an infected application is run. Other applications become infected as soon as they are run on an infected system.

The MBDF virus is non-malicious, but it can cause damage. In particular, the virus takes quite a long time to infect they System file when it first attacks a system. The delay is so long that people often think that their Mac is hung, so they do a restart. Restarting the Mac while the virus is in the process of writing the System file very often results in a damaged System file which cannot be repaired. The only solution in this situation is to reinstall a new System file from scratch.

There are also reports that the MBDF virus causes problems with the "BeHierarchic" shareware program, and reports of other menu-related problems on infected systems.

The MBDF virus is named after the type of resource it uses to infect files. MBDF resources are a normal part of the Macintosh system, so you should not become alarmed if you see them with ResEdit.

Special thanks goes out to the people at Claris who included self-check code in their Macintosh software products. Their foresight resulted in an early detection of the virus, and has thus helped the entire Mac community. It is strongly encouraged that other vendors consider doing the same with their products.

There are two known strains of the MBDF virus, MBDF A and MBDF B. There are no significant differences between the two strains.

The INIT 1984 Virus

The INIT 1984 virus was discovered in the Netherlands and in several locations in the USA in March, 1992.

INIT 1984 is a malicious virus. It is designed to trigger if an infected system is restarted on any Friday the 13th in 1991 or later years. The virus damages a large number of folders and files. File and folder names are changed to random 1-8 character strings. File creators and file types are changed to random 4 character strings. This changes the icons associated with the files and destroys the relationships between programs and their documents. Creation and modification dates are changed to Jan. 1, 1904. In addition, the virus can delete a small percentage (<2%) of files.

The virus caused significant damage to the hard disks of several users on Friday, March 13, 1992. Because only a relatively small number of reports of damage were received, we hope that the virus is not widespread.

The virus only infects INITs (known as startup documents or system extensions). It does not infect they System file, desktop files, control panel files, applications, or document files. Because INIT files are shared less frequently than are programs, the INIT 1984 virus does not spread as rapidly as most other viruses.

The virus spreads from INIT to INIT at startup time.

The virus affects all types of Macintoshes.   It spreads and causes damage under both System 6 and System 7.   On very old Macintoshes (the Mac 128k, 512k, and XL), the virus will cause a crash at startup.

The CODE 252 Virus

The CODE 252 virus was discovered in California in April, 1992.

The virus is designed to trigger if an infected application is run or an infected system is started up between June 6 and December 31 of any year, inclusive.   When triggered, the virus displays the following message:

You have a virus

Ha Ha Ha Ha Ha Ha Ha

Now erasing all disks...

Ha Ha Ha Ha Ha Ha Ha

P.S. Have a nice day

Ha Ha Ha Ha Ha Ha Ha

(Click to continue...)

Despite this message, no files or directories are deleted by the virus.   However, a worried user might turn off or restart a Macintosh upon seeing this message, and this could corrupt the disk and lead to significant damage.

Between January 1 and June 5 of any year, inclusive, the virus simply spreads from applications to System files, and then on to other application files.

Due to errors in the virus, it only spreads to new applications under System 6 without MultiFinder.   The Finder also usually becomes infected.

Under System 6 with MultiFinder, the virus infects the System file and the "MultiFinder" file, but it does spread to new applications.

Under System 7, the virus infects the System file, but it does not spread to new applications. A bad error in the virus can cause crashes or damaged files under System 7.

Under any system, the virus infects the System file, and it can and will trigger the display of the message.

The virus contains a number of additional errors which could cause crashes, damage, or other problems on any system.

The T4 Virus

The T4 virus was discovered in several locations around the world in June, 1992.

The virus was included in versions 2.0 and 2.1 of the game GoMoku. Copies of this game were posted to the USENET newsgroup comp.binaries.mac and to a number of popular bulletin boards and anonymous FTP archive sites.

The games was distributed under a false name. The name used in the posting, and embedded in the game's about box, is that of a completely uninvolved person. Please do not use this person's name in reference to the virus. The actual virus author is unknown, and probably used this person's name as a form of harassment.

The virus spreads to other applications and to the Finder. It also attempts to alter the System file.

When the virus infects an application, it damages it in such a way that the application cannot be repaired.

The change to the System file results in alterations to the startup code under both Systems 6 and 7. Under system 6 and System 7.0, the change results in INIT files and system extensions not loading. Under System 7.0.1, the change may render the system unbootable or cause crashes in unpredictable circumstances. The System file cannot be repaired and has to be reinstalled with a clean System..

If your system suddenly stops loading INITs and system extensions for no good reason, it is a good indication that you may have been attacked by the T4 virus.

The virus masquerades as Disinfectant in an attempt to bypass general-purpose suspicious activity monitors like Gatekeeper. If you see an alert from such an anti-viral tool telling you that "Disinfectant" is trying to make some change to a file, and if Disinfectant is not running, it is a good indication that T4 is attacking your system. The virus also sometimes actually renames files "Disinfectant".

Once installed and active, the virus does not appear to perform any other overt damage. The virus may display the following message:

Application is infected with the T4 virus.

There are four known strains of the T4 virus: T4-A (contained in GoMoku 2.0), T4-B (contained in GoMoku 2.1), T4-C (discovered in February 1993), and a version which appears to have been used for testing which we call "T4-beta." The strains are very similar. The only significant difference is the trigger date. The trigger date for T4-A is August 15, 1992, while the trigger date for T4-B is June 26, 1992. The virus does not do anything before its trigger date. After the trigger date, the virus begins to spread to other files and attempts to alter the System file. The T4-C virus has no trigger date. T4-C begins spreading immediately.

The INIT 17 Virus

The INIT 17 virus was discovered in New Brunswick, Canada, in April, 1993.

The virus infects both the System file and application files. It does not infect document files.

The virus displays the message "From the depths of Cyberspace" the first time an infected Macintosh is restarted after 6:06:06 A.M. on October 31, 1993.   After this message has been displayed once, it is not displayed again.

The virus contains many errors which can cause crashes and other problems.   In particular, it causes crashes and other problems.   In particular, it causes crashes on Macintoshes with the 68000 processor like the Mac Plus, SE, and Classic.

For technical reasons, the virus does not infect some applications, and on some systems, it does not spread at all.   It does, however, spread under both System 6 and System 7.

Additional Macintosh Virus's are described in the next chapter.