Disinfectant 3.7.1

July 9, 1997

Table of Contents

Disclaimer and Copyright Notice

Disinfectant may help you detect and remove some Macintosh viruses. It may fail to locate and repair some infected files. Use it at your own risk.

NORTHWESTERN UNIVERSITY PROVIDES DISINFECTANT AS IS, WITHOUT ANY WARRANTY OR PROMISE OF TECHNICAL SUPPORT. NORTHWESTERN UNIVERSITY DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF DISINFECTANT, INCLUDING, WITHOUT LIMITATION, INCIDENTAL, CONSEQUENTIAL, INDIRECT OR SPECIAL DAMAGES OF ANY KIND, EVEN IF NORTHWESTERN UNIVERSITY IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. NORTHWESTERN UNIVERSITY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PROGRAM, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

We also grant permission to extract and reproduce all or part of the Disinfectant document in other publications, provided it is not for profit and provided you give appropriate credit to both John Norstad and Northwestern University.

Disinfectant is free. There is no shareware fee.

There are no site license fees for the use of Disinfectant within an organization. We encourage you to make and distribute as many copies of the program as you wish, for whomever you wish, as long as it is not for profit.

Introduction

Viruses and other kinds of destructive computer software have become an increasingly serious problem in the computing world. In the Macintosh community, although the problem is not as serious as it was several years ago, viruses continue to spread rapidly and widely. Viruses will continue to cause problems for some time.

A virus is a piece of software which attaches itself to other programs or files. Viruses quickly propagate to other files and disks as you use your computer. Viruses spread from one Macintosh to another via the sharing and distribution of infected software or infected disks.

Viruses may be malicious or non-malicious. Non-malicious viruses replicate, but they do not attempt to do anything destructive. For example, they may beep, display messages on the screen, or do something else innocuous, but they do not intentionally try to do any damage. On the other hand, malicious viruses, in addition to replicating, do attempt to damage something. For example, malicious viruses often intentionally damage or delete files or destroy the contents of hard drives.

We are very fortunate that to date most of the known Macintosh viruses are non-malicious. It is very important to realize, however, that even non-malicious viruses are always damaging, even if the damage is unintentional. Many people who have experienced infections have reported problems with the normal operation of their Macintosh. Viruses occupy memory and disk space and this is enough to cause problems all by itself. They also live at very low levels in the operating system and can interfere in unexpected ways with other parts of the system. We have also discovered errors in most viruses which can cause unexplained crashes and strange behavior.

Disinfectant recognizes all of the currently known Macintosh system viruses. It also recognizes all the known variations and clones of these viruses. Furthermore, Disinfectant also recognizes many possible unknown variations and clones. It will both detect the viruses and, when possible, repair files which have been infected by the viruses.

Disinfectant will not recognize all possible viruses: only the ones it has been configured and programmed to recognize. If a new virus or strain appears, we will have to modify the program to recognize it, and you will have to get a new copy of the program.

Disinfectant does not recognize application-specific scripting or macro language viruses. These include the “Dukakis,” “Three Tunes,” and “MerryXMas” HyperCard viruses and the many cross-platform Microsoft Word 6 and Excel 5 macro viruses.

The Microsoft macro viruses are currently a major problem, especially for Word 6 users. If you need protection against these viruses, we recommend a commercial Macintosh anti-viral program. You do not need to worry about these viruses if you do not use Word 6 or Excel 5.

Unfortunately, because there are so many Microsoft macro viruses, and so many new ones keep appearing, we do not have the resources at Northwestern University to attempt to combat them in Disinfectant.

Disinfectant also includes a virus protection extension (INIT). When properly installed, the Disinfectant INIT will protect an uninfected system against infection by any of the known Mac system viruses.

Viruses should not be confused with other types of destructive software such as “worms” and “Trojan horses.”

A “worm” is a program which replicates and spreads, but does not attach itself to other programs. Unlike a virus, it does not require a host to survive and replicate. Worms usually propagate over a network of computers. They are not spread through the sharing of software or disks. The most well-known example is the Fall 1988 Internet worm, which infected and disabled several thousand government and university UNIX computers in a single day.

A “Trojan horse” is a program which appears to do something useful, yet additionally does something destructive behind your back. An example would be game or other program which quietly erased your hard drive in the background while you used the program. Trojan horses do not replicate.

Disinfectant does not attempt to address the problems of worms and Trojan horses.

There is no need to panic over the current virus situation. However, you should take the problem seriously. Using Disinfectant, it only takes a few minutes per week to effectively protect your Macintosh against the known viruses. See the section titled “Recommendations” for a short list of the simple things we suggest you do to protect your Mac.

There is a misconception that you can protect your Macintosh against viruses by merely avoiding shareware and freeware software. This is far from the truth. There have been many reported cases of (inadvertently) infected commercial software, while most of the major national sources of freeware and shareware software are remarkably virus-free.

The virus problem is serious, but even more serious is the tendency to overreact to the threat. Organizations which impose severe restrictions on the use of personal computers and personal computer software are doing more harm than good. For example, some companies keep computers in locked rooms and do not permit their employees to use unapproved software. Some companies have even gone so far as to prohibit their employees from joining bulletin boards or user groups! These restrictions are completely unnecessary and are, in fact, very dangerous. The heart of the personal computer revolution (especially the Macintosh revolution) is the empowerment of the individual. At their best, personal computers are extensions of each individual’s imagination, unfettered by arbitrary rules and regulations imposed by the corporate MIS priesthood. We cannot let the virus problem and other security concerns endanger this revolution.

The analogy between biological viruses and computer viruses is striking. Both of them replicate and they both require the assistance of a host to survive. In both cases, the infected system is sometimes severely damaged. With both kinds of viruses, it is sometimes possible to remove the infection without damaging the system and it is sometimes possible to inoculate or vaccinate the system to protect it against future infection.

As with all analogies, however, it is possible to carry the analogy between biological and computer viruses too far. Computers are not living organisms. Biological viruses usually occur naturally and are almost never created by people. Computer viruses are always created by people; they never occur naturally. Most importantly, it is not possible to compare the enormous suffering caused by biological viruses such as HIV to the comparatively meaningless damage caused by computer viruses.

Disinfectant is distributed electronically. When a new virus is discovered, we usually release a new version of Disinfectant to recognize the virus within a few days. The official anonymous FTP site is:

ftp://ftp.nwu.edu/pub/disinfectant/

Disinfectant is not a commercial product. We cannot offer typical commercial services such as telephone support, mailing lists, or upgrade services.

Macintosh users who do not have access to electronic sources of free and shareware software may obtain a copy of Disinfectant by sending a self-addressed stamped envelope and a floppy disk (800K or 1440K) to the author at the address given at the end of this manual. People outside the U.S. may send an international postal reply coupon instead of US stamps (available from any post office). Please use sturdy envelopes, preferably cardboard disk mailers.

Quick Start

This section describes how to use Disinfectant for the first time to check your system for viruses, remove any viruses which you may have on your system, and protect your system against future infections. We also discuss a few very important rules and restrictions which you should follow when using Disinfectant.

The first step below is different depending on whether you use System 7 or later or System 6. This first step is very important. Do not skip it!

• Step 1 (for System 7 or later users). Make a backup copy of Disinfectant on a floppy disk. Lock the floppy disk and label it “Disinfectant Backup.” To lock the floppy, slide the plastic tab on the back of the floppy up so that you can see through the hole.

The backup copy of Disinfectant is very important. During normal operations, you will run Disinfectant from your hard drive. However, if Disinfectant becomes damaged in any way, or if it becomes infected by a virus, it will refuse to run! In this case, you will need the backup copy.

It is impossible for a virus to infect a file on a locked floppy disk, provided the disk is always kept locked. Never unlock your backup Disinfectant floppy.

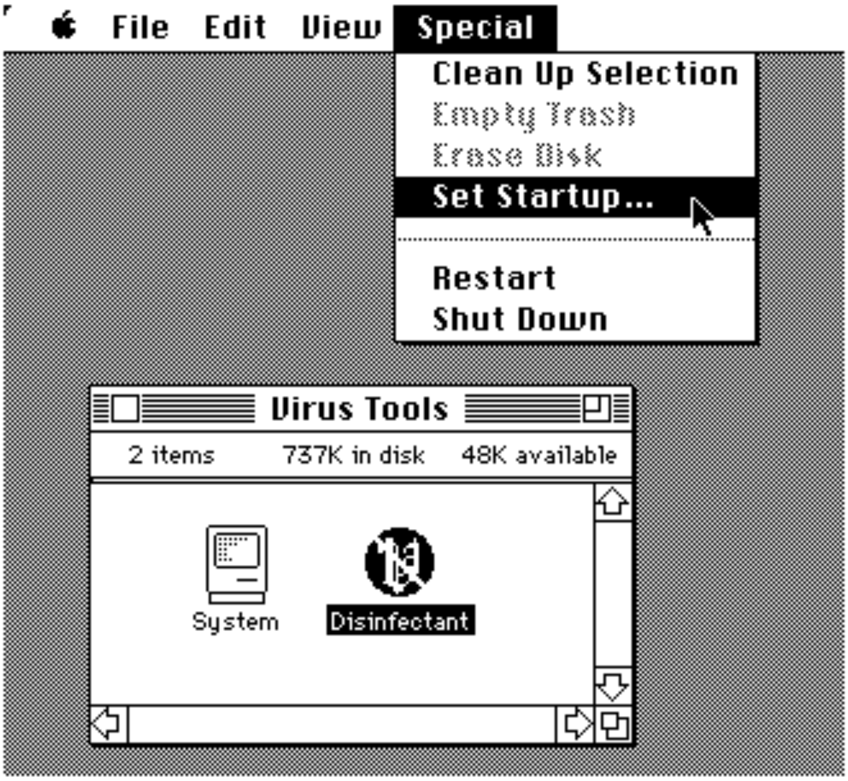
Also identify and locate your Apple emergency startup disk. This might be a bootable floppy disk named “Disk Tools” or some other name, or it might be a bootable CD-ROM disk. This disk is part of the standard Apple System release. Some kind of bootable emergency startup disk is included with every Macintosh sold. Keep this disk locked (if it is a floppy) and in a safe place. You may need to start up from this disk to remove viruses from some kinds of files.

Keep both your Disinfectant backup floppy and your emergency startup disk in a safe place.

• Step 1 (for System 6 users). Make a “Virus Tools” floppy containing a copy of the System file and a copy of Disinfectant.

Use an original locked System 6 Apple “System Tools” disk for your copy of the System file. Do not use the System file from your hard drive or some other System file because it may be too big to fit on the floppy along with Disinfectant.

After copying the two files to the floppy, click the Disinfectant icon in the floppy’s window to select it, then use the “Set Startup” command in the System 6 “Special” menu to set Disinfectant as the startup program.



Making Disinfectant the Startup Program

Eject the Virus Tools floppy. Lock it and label it "Virus Tools." To lock the floppy, slide the plastic tab on the back of the floppy up so that you can see through the hole.

Test your Virus Tools disk. Restart your Macintosh from the Virus Tools disk (shut down your Mac, insert your Virus Tools disk in the floppy drive, and then start up your Mac again). Disinfectant should run automatically. When the main Disinfectant window appears, click the Quit button to quit the program. An alert should appear telling you that the Finder is "busy or damaged." This is normal. The alert appears because there is no Finder on the Virus Tools disk. Click the Restart button in this alert to restart your Mac.

The Virus Tools disk is very important. During normal operations, you will run Disinfectant from your hard drive (if you have one). However, if Disinfectant becomes damaged in any way, or if it becomes infected by a virus, it will refuse to run! In this case, you will need your Virus Tools disk. You may also need to start up from your Virus Tools disk to remove viruses from some kinds of files.

It is impossible for a virus to infect a file on a locked floppy disk, provided the disk is always kept locked. Never unlock your Virus Tools floppy.

Keep your Virus Tools floppy in a safe place.

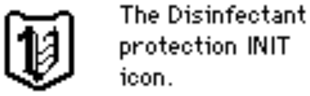
If you wish, you may try to put a copy of the Finder on your Virus Tools disk. This is not necessary, however, if you follow the instructions above. In some cases there is not even enough room on the floppy to add the Finder. (For example, there is not enough room on an 800K floppy for the System 6.0.7 System and Finder files and Disinfectant.)

• Step 2. Run Disinfectant from your hard drive, if you have one. If you do not have a hard drive, start up your Mac using your Virus Tools disk. Disinfectant will run automatically.

• Step 3. Disinfect all of your hard disks. (Skip this step if you do not have a hard disk.) Select the "All Local Unlocked Disks" command from the "Disinfect" menu. Disinfectant will scan all of your hard disks and will remove any viruses which it discovers.

• Step 4. Disinfect all of your floppy disks. Select the "Floppies" command from the "Disinfect" menu. Disinfectant will prompt you to insert floppies one at a time to be scanned and repaired. Unlock each disk before inserting it. (Disinfectant cannot repair a disk if it is locked.) You can lock the disk again after Disinfectant has ejected it.

• Step 5. Install the protection INIT on your hard drive. (Skip this step if you do not have a hard drive.) Select the "Install Protection INIT" command from the "Protect" menu. Disinfectant will place a copy of the protection INIT inside the currently active System folder on your hard drive. (On System 7 or later, the INIT is placed inside the Extensions folder.) An alert will appear asking if you want to restart your Macintosh to activate the INIT. Click the Restart button. You should see the protection INIT icon appear at the bottom of your screen during startup.



The Disinfectant protection INIT icon.

• Step 6. Install the protection INIT on each of your startup floppy disks. Run any copy of Disinfectant. Select the "Save Protection INIT" command from the "Protect" menu. A standard file dialog will appear. Use the standard file dialog to save a copy of the protection INIT. Quit Disinfectant. Drag copies of the protection INIT into the System folder on each of your startup floppy disks.

There are only a few rules and restrictions when running Disinfectant, but they are important.

Disinfectant requires System 6.0 or later.

Disinfect all your disks at one time. Do not do some of them, then run some other programs, and finally disinfect the rest of your disks. If you run other programs before making certain that you have completely eradicated the virus, you run the risk of reinfecting your system.

You can and should run Disinfectant from your hard drive using your normal system. It is not necessary to run it from your backup locked floppy disk or Virus Tools disk for everyday use. If you encounter problems running it using your normal system, however, we suggest that you try restarting your Mac using either your emergency startup disk (for System 7 or later) or your Virus Tools disk (for System 6). Try running Disinfectant again. This avoids INIT conflicts and other possible causes of problems.

When repairing (disinfecting) files, Disinfectant may be unable to repair a file or files because they are "busy." In this case, an error message is issued advising you what to do. In many cases, the solution recommended by the error message is to restart using either your emergency startup disk (for System 7 or later) or your Virus Tools disk (for System 6), as described above.

Disinfectant runs much faster if you set your monitor to black and white and use a RAM cache. (A 32K RAM cache seems to work well.) Some virus protection INITs can make Disinfectant run slower than normal. (The Disinfectant INIT, however, has no noticeable effect on the performance of Disinfectant.)

For even greater safety, if you have locked original copies of applications and system files, you can delete the files that Disinfectant says are infected and reinstall uninfected copies from the original floppies. If you do this, use Disinfectant to rescan the replaced files to make certain your originals were not infected.

Disinfectant creates a file named "Disinfectant Prefs" in your Preferences folder (System 7 or later) or in your System folder (System 6). This file is used to save preferences, window positions, and page setup information between Disinfectant sessions.

You should now be ready to use Disinfectant for the first time. The remainder of this manual gives more information about Macintosh viruses and Disinfectant. You may read it now if you wish, or return to read it later.

Known Problems

This section lists some known problems with Disinfectant. Many of these problems involve incompatibilities with older versions of other software.

If you have a Rodime Cobra disk drive, make certain that you are using version 1.1.3 or later of the Cobra disk driver. Earlier versions of the Cobra driver contained an error which caused problems with Disinfectant.

Both the Disinfectant program and the Disinfectant INIT are incompatible with versions of "Greg's Buttons" earlier than 1.5. The incompatibility can cause crashes and other problems. If you use Greg's Buttons, make certain you have version 1.5 or later.

The Disinfectant INIT is incompatible with versions of Robert Mathew's "Speed Beep" earlier than version 2.0.6. The incompatibility causes Speed Beep to refuse to work. If you use Speed Beep, make certain you have version 2.0.6 or later.

The Disinfectant INIT is incompatible with versions of Microseed's INITPicker earlier than version 2.0. The earlier versions of INITPicker did not properly deal with INITs whose names begin with a special character. If you use INITPicker, check to make certain that you have version 2.0 or later.

The Disinfectant about box plays a tune. On some Mac models with some versions of the Apple system software, the tune is not played correctly (the timing between notes is not correct). There is nothing we can do about this problem.

Disinfectant will not detect infected files if they are part of a StuffIt, Compact Pro, or other kind of archive, if they have been converted to a text file with BinHex, if they have been compressed with PackIt, or if they have been compressed, converted or archived by some similar utility. If you have such files and want to make certain they do not contain infections, you must unpack them and check the unpacked files.

Disinfectant does, however, work properly with automatic disk compression utilities like Disk Doubler and AutoDoubler. With these kind of utilities, files are automatically decompressed when programs access them.

Disinfectant cannot be used to check the backup floppy disks or tapes produced by most of the various hard disk backup utility programs. These programs usually write their backups in a special format which is not recognized by Disinfectant. If you suspect that your backups are infected, we recommend that you first disinfect all of your other disks (hard drives and floppies), then do a new full backup, and finally erase (reformat) all of your remaining suspect backup floppies.

System 7 Notes

Disinfectant is fully compatible with System 7 and Mac OS 8, including virtual memory, 32 bit addressing, and file sharing.

Disinfectant is also compatible with the Power Macintosh.

Leave the Disinfectant INIT in the Extensions folder. Do not move the INIT to the System Folder. The “Install Protection INIT” command installs the INIT in the proper location in the Extensions folder. Do not move it.

If you try to repair an infected file, Disinfectant may tell you that the file is busy and recommend that you either restart using your “Virus Tools” or emergency startup disk and try again or “rebuild the desktop.” Restarting using your “Virus Tools” or emergency startup disk was discussed in the “Quick Start” section above. Rebuilding the desktop is discussed in the “Problem Clinic” section below.

You should also be aware that System 7 is completely immune to the “Desktop file” viruses (WDEF and CDEF). These viruses never activate, spread, or cause any damage under System 7. Both hard disks and floppy disks are immune to these viruses under System 7. Since the Disinfectant INIT detects and blocks viruses when they first try to attack your system, and since the Desktop file viruses never attack under System 7, the Disinfectant INIT will not detect them under System 7.

System 7 hard drives, however, often contain an old System 6 format Desktop file. If you restart using an infected System 6 startup floppy, this file can and will become infected by WDEF or CDEF. The virus will only be active, however, when you start up your Mac with System 6. The proper way to protect against this problem is to install a copy of the Disinfectant protection INIT in your System 6 System folder.

You should also be aware of a problem with System 7’s file sharing feature. If you share a folder and permit write access to it by granting the “make changes” privilege with the “Sharing” command, it is possible for files in the shared folder to become infected by a virus over the network, even if you have the Disinfectant INIT installed on your Mac. The INIT will, however, prevent the virus from spreading to your non-shared folders. It will also completely block any attempt by the virus to execute its viral code on your Mac or cause any damage to your Mac.

We have always had the problem of viruses spreading over a network to files in writable folders on dedicated AppleShare file servers. With System 7’s file sharing, this has now also become a problem on personal Macs.

Virus infection over the network is only one of many serious security problems with writable shared folders. Writable shared folders are inherently insecure, and no kind of anti-viral or other security software can prevent damage to their contents. To minimize these problems, we recommend that you limit write access to your shared folders to only trusted individuals. Never grant write access to guests (“any user”). The only way to eliminate the problems completely is to never grant the “make changes” privilege to anyone except yourself.

Windows

This section describes each of Disinfectant's windows.

The Main Window

The main Disinfectant window is the one you will use most often. It contains the main controls for the application and it displays the report generated by the application. The main window is always open and cannot be closed.

The operation of Disinfectant is controlled by six buttons in the main window:

• Drive and Eject. Use these buttons to select the disk you want to scan or disinfect. The Drive button cycles through all of your hard disks and floppy disks. The Eject button is used to eject a floppy disk.

• Scan and Disinfect. Use the Scan button to scan the disk you selected. Disinfectant will check the disk for infections, but it will not try to repair infected files.

Use the Disinfect button to scan and disinfect the disk you selected. Disinfectant checks each file for infection and attempts to repair any infected files which it finds.

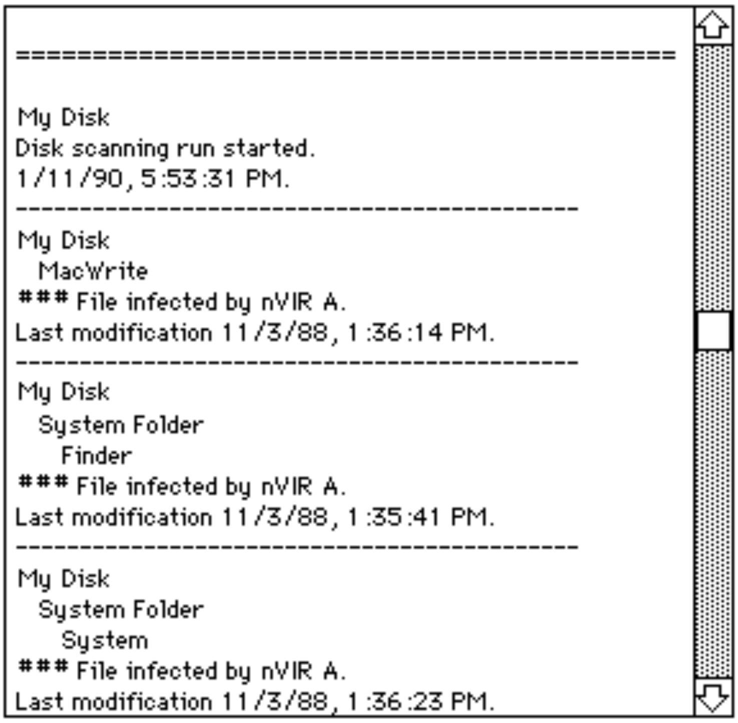
For other kinds of scans, you can use the menus or command keys. The Scan and Disinfect menus are described in detail in the section titled "Menus." You can also hold down the following key or keys while clicking on the Scan or Disinfect button:

Option key: Scan a single folder or file.
Command key: Quickly scan a sequence of floppies.
Option and command keys: Scan all mounted volumes.

• Cancel. This button is active during disk scans. Use it if you want to cancel the scan. You can also type Command-Period or Escape to cancel a scan.

• Quit. Quits the application.

Both the Scan and Disinfect buttons produce a detailed report in the field on the left side of the screen. When the scan is complete, you can use the scroll bar to view the entire report.

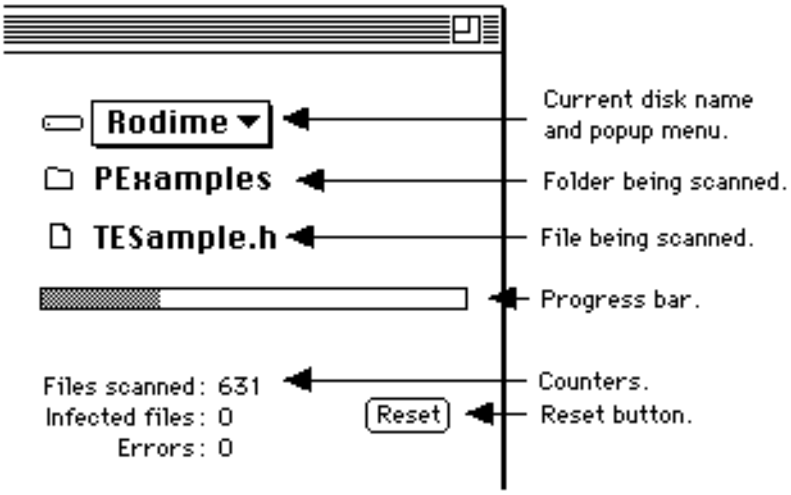


```
============================================

My Disk
Disk scanning run started.
1/11/90, 5:53:31 PM.
------------------------------------------
My Disk
  MacWrite
### File infected by nVIR A.
Last modification 11/3/88, 1:36:14 PM.
------------------------------------------
My Disk
  System Folder
    Finder
### File infected by nVIR A.
Last modification 11/3/88, 1:35:41 PM.
------------------------------------------
My Disk
  System Folder
    System
### File infected by nVIR A.
Last modification 11/3/88, 1:36:23 PM.
```

In addition to using the scroll bar, you can also use the up and down arrow keys to scroll the report backwards or forwards one line at a time (if your keyboard has these keys). To scroll up or down one screen at a time, hold down the command key while pressing the up or down arrow key (or use the Page Up or Page Down key on the extended keyboard). To jump to the beginning or end of the report, hold down both the command and shift keys while pressing the up or down arrow key (or use the Home or End key on the extended keyboard).

Several other pieces of information are displayed in the top right corner of Disinfectant's main window:



Rodime ▾

PExamples

TESample.h

Files scanned: 631
Infected files: 0
Errors: 0

The current disk name is a popup menu. You can click the disk name and keep the mouse button held down to get a popup menu listing all of your disks. This is an alternative to using the Drive button.

During a disk scan, the names of the folder and file currently being scanned are displayed next to the small folder and file icons. In addition, a progress bar fills with gray to indicate the progress of the scan. The progress bar is only available on full disk scans. It is not present on folder scans, file scans, or scans of server disks.

The three counters show a running total of how many files have been scanned, how many infected files have been discovered, and how many errors have been encountered. You can click the small Reset button next to the counters to reset all of them to zero.

The Help Window

This window displays the manual you are reading now. It is opened by the "Disinfectant Help" command in the Apple menu or by the Command-H keyboard equivalent.

Use the scroll bar to scroll through the manual.

In addition to using the scroll bar, you can also use the up and down arrow keys to scroll the manual backwards or forwards one line at a time (if your keyboard has these keys). To scroll up or down one screen at a time, hold down the command key while pressing the up or down arrow key (or use the Page Up or Page Down key on the extended keyboard). To jump to the beginning or end of the manual, hold down both the command and shift keys while pressing the up or down arrow key (or use the Home or End key on the extended keyboard).

You can quickly jump to any section of the manual by clicking on the section title in the table of contents on the right side of the window. The table of contents is a scrolling menu. Click the triangles at the top and bottom of the menu to scroll up or down.

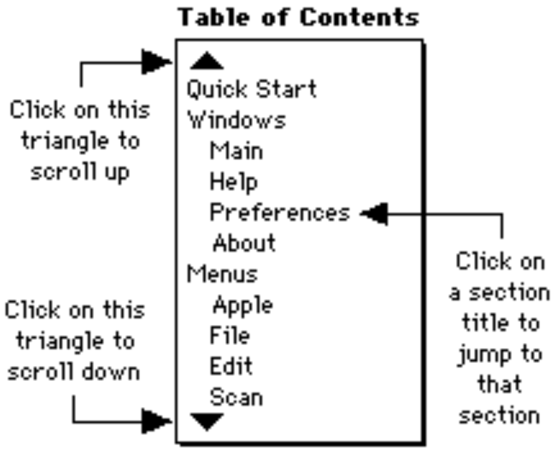


Table of Contents
▲
Quick Start
Windows
Main
Help
Preferences
About
Menus
Apple
File
Edit
Scan
▼
Click on this triangle to scroll up
Click on this triangle to scroll down
Click on a section title to jump to that section

The manual can be printed and you can save it as a text file. See the section about the File menu for more details.

Disinfectant offers a method to help you quickly locate information in the manual. Press Command-? (or the Help key on the extended keyboard) and the cursor will turn into a question mark. Then click any object in any of Disinfectant's windows or select any menu command. Disinfectant will bring up the Help window and scroll to the description of that object or command.

If Disinfectant issues an error message in the report, press Command-? (or the Help key) and click any error message line (any line that begins with "###") to get a detailed description of that error message.

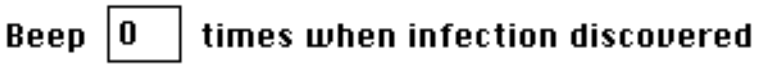
If Disinfectant reports that a file is infected by a virus, press Command-? (or the Help key) and click the infection message in the report to get a detailed description of that virus.

Help mode can be canceled at any time by pressing Command-Period or by pressing Escape or by pressing Command-? (or the Help key) again.

The Preferences Window

This window lets you set various options and parameters for Disinfectant. It is opened by the “Preferences” command in the File menu.

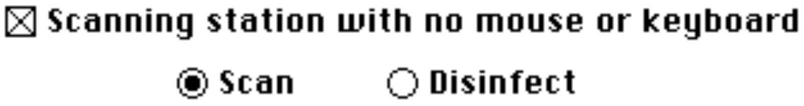
• Beeping option.



Beep 0 times when infection discovered

This option specifies how many times Disinfectant should beep when an infection is discovered. The default is no beeping.

• Scanning station options.



☒ Scanning station with no mouse or keyboard

● Scan ○ Disinfect

If you wish, you can establish a special Mac in your lab or office to be used for nothing but checking for viruses. People can simply insert their floppies to have them scanned or disinfected. You can even remove the mouse and keyboard to discourage use of the Mac for anything but checking for viruses.

If you do remove the mouse and keyboard, you should first build a special System 6 scanning station startup disk:

Step 1. Make a copy of your Virus Tools floppy. Do not unlock the Virus Tools floppy, but leave the copy you made unlocked until step 9 below. Eject and put away your original Virus Tools floppy. The remaining steps will use the copy.

Step 2. In the Finder, click the Disinfectant icon to select it. Then use the “Set Startup” command in the “Special” menu to set Disinfectant as the startup program for this disk.

Step 3. Restart using the disk you just made. Disinfectant should run automatically.

Step 4. Select the “Preferences” command from the “File” menu to open the Preferences window.

Step 5. Check the “Scanning station with no mouse or keyboard” option.

Step 6. Select either the “Scan” or the “Disinfect” option.

Step 7. Close the Preferences window and quit Disinfectant. Click the Restart button when you get the “Finder is busy or damaged” alert.

Step 8. Reinsert your floppy disk after your Mac restarts. You should see a third file on the disk named “Disinfectant Prefs.”

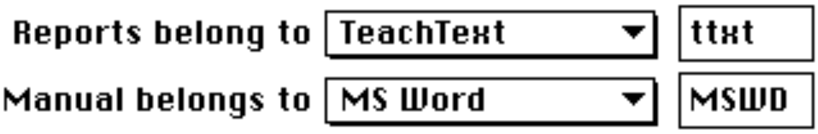
Step 9. Eject and lock the disk. This is your special scanning station startup disk.

You should use this special startup disk whenever you restart your scanning station. Disinfectant will automatically start in its floppy scanning mode. You should need neither the keyboard nor the mouse at any time during the startup process.

This scanning station option also tells Disinfectant to avoid any situations which might require use of the mouse or keyboard in the future.

We do not recommend that you check this option in any other situation. Use it only for scanning stations.

- Saved text file options.



Reports belong to TeachText ▼ ttxt

Manual belongs to MS Word ▼ MSWD

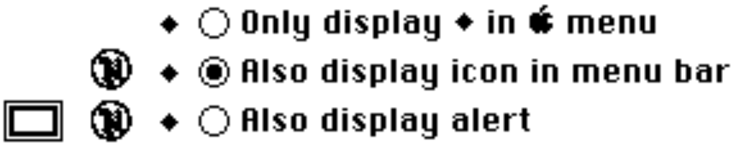
You can save the reports generated by Disinfectant and you can also save text-only versions of the manual. These files are always saved as plain text files without any formatting and they can be read by any Macintosh word processor or editor.

By default, Disinfectant saves reports as TeachText files and it saves the manual as a Microsoft Word file. This means that if you open a saved report from the Finder, TeachText will be opened, whereas if you open a saved manual from the Finder, Microsoft Word will be opened (if it is available on your Mac).

You can change the applications which own these saved files. The boxes containing the names of the applications are popup menus which let you select any of the more popular word processors and editors. You can also type “creator types” directly in the fields to the right of the application names.

You may notice that the popup menu for saved reports contains more application names than does the popup menu for the saved manual. This is because the saved manual is very large and not all of the applications can handle such large files.

- Background notification options.



◆ ○ Only display ◆ in menu

◆ ● Also display icon in menu bar

◆ ○ Also display alert

Disinfectant can run in the background under System 7 or under System 6 with MultiFinder. This option specifies how you wish to be notified if an infection is discovered or if Disinfectant requires attention for some other reason. The default is to display a diamond next to Disinfectant’s name in the Application menu (System 7) or in the Apple menu (System 6) and to flash the small Disinfectant icon in the menu bar.

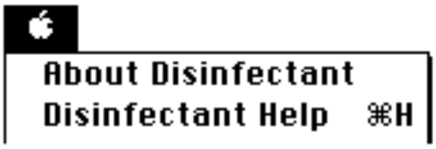
The About Window

This window presents Disinfectant’s About box. (Our apologies to Monty Python.) It is opened by the “About Disinfectant” command in the Apple menu.

Menus

This section describes each of Disinfectant's menus.

The Apple Menu



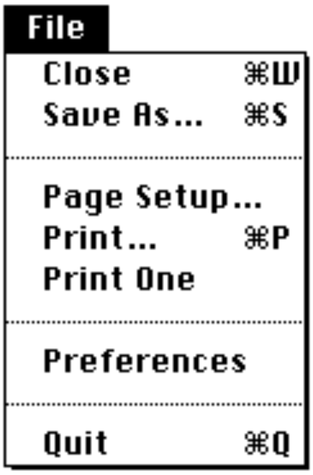
• About Disinfectant

This command opens Disinfectant's About window or brings it to the front if it is already open.

• Disinfectant Help (Command-H)

This command opens Disinfectant's Help window or brings it to the front if it is already open.

The File Menu



• Close (Command-W)

This command closes the active (front) window.

• Save As…(Command-S)

This command saves reports and the manual as text files. If the main window is active, the report is saved as a TeachText file. If the Help window is active, the Disinfectant manual is saved as a Microsoft Word text file. A standard new file dialog appears, asking you to specify the file's name and location.

These saved text files can be read by most any Mac word processor or editor. You can change the type of the file (TeachText and Microsoft Word by default) in the Preferences window.

You can save a separate report for each disk you scan or you can scan many disks and save the combined reports as a single file. The latter option is particularly appropriate when scanning a sequence of floppies.

When the manual is saved, only the text from the manual is saved, without the pictures, and without any of the formatting. The primary purpose of this feature is to let you save the text so that you can copy and paste it into newsletter articles or other documents. We grant you permission to do this, if it is not for profit, and if you give appropriate credit to the author and to Northwestern University.

• Page Setup…

This command presents an expanded version of the standard page setup dialog. The extra items in the bottom half of the dialog are used to specify additional options for a printed report or manual. You can specify the font and font size, all four margins, and an option to print the pages in reverse order.

Disinfectant maintains separate sets of page setup options for printed reports and the printed manual.

Disinfectant supplies reasonable default values for all of these options, with different default values supplied for LaserWriters and ImageWriters. Other kinds of printers may be treated as either LaserWriters or ImageWriters. If you are using some kind of printer other than an Apple LaserWriter or ImageWriter, you should use the Page Setup command to check the settings before printing and adjust them appropriately.

The maximum permitted font size is 24 points.

With large fonts sizes and/or large margins, there may not be enough printable area on the page for Disinfectant to print properly. In this case, an alert is presented which informs you of the problem and gives you advice on how to correct it.

In particular, when printing reports using font sizes over 18 points, with most fonts you will have to use landscape orientation instead of portrait orientation. This problem should not occur with the printed manual, even at 24 points, provided you do not increase the default margins.

The page setup options are saved in the Disinfectant Prefs file in the System folder. You only need to set them once; they will be remembered even when you quit Disinfectant and run it again later. Separate options are saved for printed reports and for the printed manual.

• Print… (Command-P)

This command is used to print reports and the manual. It presents the standard print job dialog.

If the main window is active, the report is printed. If the Help window is active, a formatted copy of the Disinfectant manual is printed.

The printed version of the manual has a title page, table of contents, page headers, smart page breaks, and other nice formatting features. Paragraphs are reformatted to fit the margins specified in the page setup dialog.

Printing on a Macintosh without a hard drive is possible, but it requires a special startup disk. This topic is discussed in detail in the “Special Features” section.

• Print One

This command prints one copy of all pages of a report or the manual. It does not present the standard print job dialog.

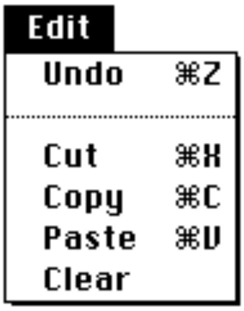
• Preferences

This command opens the Preferences window or brings it to the front if it is already open.

• Quit (Command-Q)

This command quits Disinfectant.

The Edit Menu



• Undo (Command-Z)

This command is not used by Disinfectant. It is present only for use by System 6 desk accessories.

• Cut (Command-X)

This command cuts selected text to the clipboard. It is used only with desk accessories and the Preferences window.

• Copy (Command-C)

This command copies selected text to the clipboard. It is used only with desk accessories and the Preferences window.

• Paste (Command-V)

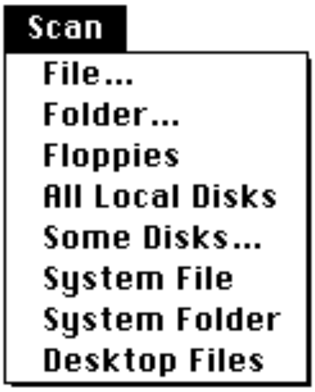
This command inserts the contents of the clipboard at the current cursor location or replaces the currently selected text by the contents of the clipboard. It is used only with desk accessories and the Preferences window.

• Clear

This command clears the selected text in a desk accessory or in the Preferences window.

When the main window is active, this command clears the report. If the report lists any infections, you will be presented with an alert asking whether you want to save the report before clearing.

The Scan Menu



- File…

This command scans a single file. It presents the standard open file dialog.

- Folder…

This command scans a single folder. It presents a modified open dialog which lists only folders.

- Floppies

This command is used to quickly scan a sequence of floppy disks. Disinfectant will prompt you to insert floppies and will eject them when they have been scanned. You can also use this command to scan CD-ROM disks or other kinds of removable media.

- All Local Disks

This command scans all mounted local volumes. This option is useful if you have more than one hard disk or multiple partitions and you want to scan all of them. Any network AppleShare file servers you have mounted are skipped.

- Some Disks…

This command presents a dialog in which you specify which mounted volumes you wish to scan. This option is useful if you wish to scan more than one disk, but not all of them.

- System File

This command scans just the currently active System file.

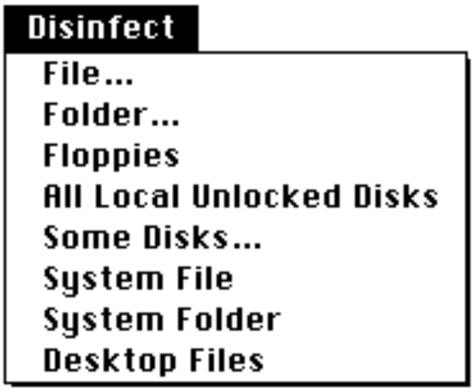
- System Folder

This command scans just the currently active System folder.

- Desktop Files

This command scans just the invisible System 6 Finder Desktop files. It scans all Desktop files on all of the currently mounted volumes. This command can be used to perform a quick check for the WDEF and CDEF viruses.

The Disinfect Menu



- File…

This command disinfects a single file. It presents the standard open file dialog.

- Folder…

This command disinfects a single folder. It presents a modified open dialog which lists only folders.

- Floppies

This command is used to quickly disinfect a sequence of floppy disks. Disinfectant will prompt you to insert floppies and will eject them when they have been disinfected. You can also use this command to disinfect other kinds of removable media.

- All Local Unlocked Disks

This command disinfects all mounted local unlocked volumes. This option is useful if you have more than one hard disk or multiple partitions and you want to disinfect all of them. Any network AppleShare file servers you have mounted are skipped. Any locked disks are also skipped.

- Some Disks…

This command presents a dialog in which you specify which mounted volumes you wish to disinfect. This option is useful if you wish to disinfect more than one disk, but not all of them.

- System File

This command disinfects just the currently active System file.

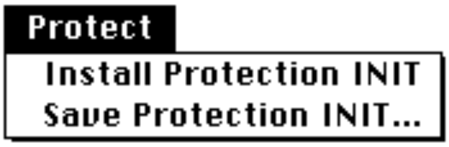
- System Folder

This command disinfects just the currently active System folder.

- Desktop Files

This command disinfects just the invisible System 6 Finder Desktop files. It disinfects all Desktop files on all of the currently mounted volumes. This command can be used to quickly remove the WDEF and CDEF viruses. You must be using Finder under System 6, not MultiFinder or System 7, to remove the WDEF and CDEF viruses. See the sections on WDEF and CDEF for details.

The Protect Menu



- Install Protection INIT

This command installs the Disinfectant protection INIT in the currently active System folder. Under System 7, the INIT is installed in the Extensions folder inside the System folder.

After the INIT has been copied into your System folder, Disinfectant presents an alert informing you that you must restart your Mac to activate the INIT. Click the “Restart” button to restart your Mac. Click the “OK” button to return to Disinfectant.

See the section below titled “Protection” for more details.

- Save Protection INIT…

This command saves the Disinfectant protection INIT to any location of your choosing. A standard file dialog appears which lets you specify the location of the saved file.

See the section below titled “Protection” for more details.

Protection

The Disinfectant application by itself will not protect your system against infection. It will only locate and repair previously infected files and disks. To protect your system against infection, you must install a protection extension (protection INIT).

Disinfectant includes such a protection INIT. When properly installed, it will protect your system against all of the known Macintosh system viruses.

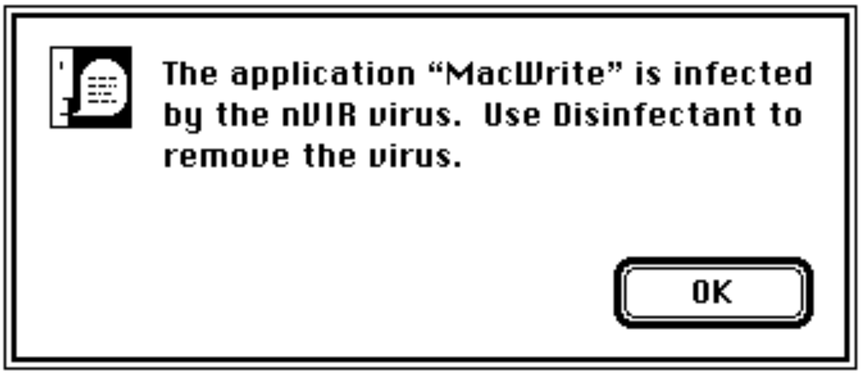
WARNING: The Disinfectant protection INIT will not protect your system against unknown viruses! If a new virus appears, we will have to release a new version of Disinfectant to recognize it.

Use the “Install Protection INIT” command in the “Protect” menu to install the Disinfectant INIT in your currently active Extensions folder (under System 7) or in your currently active System folder (under System 6). You must restart your Macintosh to activate the INIT.

Use the “Save Protection INIT” command in the “Protect” menu to save a copy of the Disinfectant INIT to any location of your choosing.

The Disinfectant INIT is simple, small, efficient, and unobtrusive. It does not need to be configured. In fact, it has no control panel interface at all, so it cannot be configured. The INIT will never ask you to make a decision. It should have no noticeable effect on the performance of your Mac. It is very small and can easily be used on floppy startup disks (e.g., in university labs with floppy-only Macs). The INIT does not interfere with the normal operation of Disinfectant or other anti-viral applications, or with programming environments, installer applications, or other system software.

If you run an application which is infected by one of the known Mac viruses, the Disinfectant INIT beeps ten times, quits the application, and presents an alert. For example, if the application “MacWrite” is infected by the nVIR virus, the following alert appears when you try to run MacWrite:



The application “MacWrite” is infected by the nVIR virus. Use Disinfectant to remove the virus.

The Disinfectant INIT only detects and blocks viruses; it does not remove them. To remove a virus, you must use the Disinfectant application.

With System 6, if you use a disk which is infected by the WDEF virus or by the CDEF virus, the Disinfectant INIT beeps ten times, presents an alert, and temporarily neutralizes the virus. You can safely use the disk; the virus will not spread. To remove the virus from the disk, you can either rebuild the Desktop file or use the Disinfectant application. Rebuilding the Desktop file is usually easier.

If you use a HyperCard stack which is infected by the MacMag virus, the Disinfectant INIT beeps ten times, presents an alert, and temporarily neutralizes the virus. You can safely use the stack; the virus will not spread. You should use the Disinfectant application to remove the virus from the stack.

If you have an INIT file which is infected by the INIT 1984 virus, when the virus attacks during startup, the Disinfectant INIT beeps ten times, and an alert is presented at the end of the startup sequence. The virus is neutralized and does not spread or cause any damage, but the non-viral part of the infected INIT runs as usual.

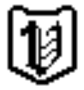
The name of the Disinfectant INIT begins with a special invisible character. This special character does not appear in Finder windows. In standard file dialogs and in some other contexts, it appears as a box.

The special symbol is present to force the Disinfectant INIT to be the first INIT loaded when you start up your Macintosh. This is important: the Disinfectant INIT should be loaded first! If you rename the INIT, make certain that you rename it so that it comes first in alphabetical order in your Extensions folder or your System folder. With System 7, be very careful to leave the INIT in the Extensions folder. Do not move it to the System folder proper or to the Control Panels folder. To avoid problems, we recommend that you do not rename the INIT.

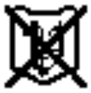
The reason the Disinfectant INIT should be loaded first is to properly detect and block the INIT 1984 virus, which spreads from INIT to INIT at startup time. If the Disinfectant INIT does not load first, and if some earlier INIT is infected by the INIT 1984 virus, then the Disinfectant INIT will not be able to detect or block the virus when it attacks during startup.

A number of other popular INITs also have the requirement that they should be loaded first. Before installing such an INIT, scan it with the Disinfectant application to make certain it is not infected by the INIT 1984 virus or any other virus. Then install it. Depending on how the INIT is named, it may load before or after the Disinfectant INIT. Don't worry if the other INIT loads first. You have already made certain that it is not infected, so it shouldn't cause any problems.

The Disinfectant INIT icon should appear at the bottom of your screen every time you restart your Macintosh. If an error occurs and the INIT cannot load properly, the INIT will beep ten times and it will draw a special error version of the icon (the normal icon with a large "X" superimposed.)



Normal Disinfectant INIT icon. This icon should appear at the bottom of your screen every time you restart your Macintosh.



Error icon. This icon appears at the bottom of your screen if the Disinfectant INIT did not load properly.

The Disinfectant INIT icon normally appears first in the row of INIT icons which appear when you restart. One exception to this is under System 6 with Apple's Communications Toolbox installed. The Communications Toolbox icon may appear first, in which case the Disinfectant INIT icon appears second.

If you wish to remove the Disinfectant INIT for some reason, open your Extensions folder (under System 7) or your System folder (under System 6) and drag the INIT icon to the trash (or anywhere else outside of the System folder). Then restart your Macintosh.

Contrary to the instructions found in many software manuals, it is not necessary to remove the Disinfectant INIT when installing software. There are no known cases where the Disinfectant INIT interferes in any way with installers.

The Disinfectant INIT detects and blocks viruses at their initial point of attack. Unlike some other virus protection INITs, it does not scan floppies each time they are inserted into a disk drive and it does not scan files each time they are opened. This strategy is what makes the Disinfectant INIT so small and efficient.

The Disinfectant INIT will not detect files which are partially infected but not contagious, since these kinds of infections never attack the system. These non-contagious infections are harmless, so this is not a major problem. The Disinfectant application does detect these kinds of infections.

Recommendations

There is no need to panic over the current virus situation. However, you should take the problem seriously. Using Disinfectant, it only takes a few minutes per week to effectively protect your Macintosh against the known viruses.

- If you do nothing else, religiously use the Disinfectant INIT. It only takes a minute to install and it can save you much grief.

- Keep original software on locked floppies. Use copies. When you obtain a new piece of software, immediately lock the disk on which it came, make a copy, and use the copy. Never unlock the original disk. It is impossible for a virus to infect files on a locked floppy.

- Make periodic backups of your hard drive, at least once per week.

- Keep your anti-viral software up-to-date. This is very important. Old versions of anti-viral software are very often ineffective against new viruses. This is particularly true of Disinfectant, which only protects against known viruses and makes no attempt to detect new viruses. If you do not have access to a reliable source of information about new Disinfectant releases, we recommend that you use a commercial anti-viral product instead of Disinfectant. Purchase a product which offers an update service.

For most people, this is all you have to do to protect your personal Macintosh. It is not necessary to scan all new software before using it or to scan all floppy disks before using them. This is a waste of time. As long as you have the INIT properly installed, it will detect and block viruses before they can spread or cause any damage.

It is also not necessary to scan your hard drives frequently. Let the protection INIT do its job and trust it.

You should, however, periodically do a full scan of all your hard drives just to make certain that they are still uninfected. For example, if you start up from a floppy disk which does not have the Disinfectant INIT installed, it is possible for a virus to infect your hard drives. Doing a scan every once in a while will detect any such infections.

One strategy which many people use is to do a full scan just before every backup. This has the added advantage that it makes certain your backups are clean.

The remaining recommendations are for people who manage Mac networks, Mac laboratories, Mac bulletin boards, or collections of public domain and shareware software. An environment where many people share Macs, or share a Mac network, is a perfect breeding ground for viruses. People who sell software also have a special responsibility to make certain that their software is free from infection.

- Install the Disinfectant protection INIT on all your lab startup disks.

- Check all your lab disks frequently with Disinfectant to make certain that they are uninfected. Also check to make certain that the Disinfectant protection INIT is still installed and active on all your startup disks. We have discovered that students love to play with the start-up disks.

- Educate the people in your organization about viruses and how to protect against them. Give them copies of Disinfectant and teach them how to use the application. Distribute printed copies of the Disinfectant manual.

- Consider creating a special “virus scanning station” in your lab. See the section about the Preferences window for details.

• Try to put software in write-protected folders on AppleShare server disks. Viruses cannot infect applications if they are in folders which do not have the “Make Changes” privilege. On the other hand, if an application is in a writable server folder, any infected Mac on the network which accesses the disk and uses the application might spread the infection to the application on the server. If it is a popular application, it will in turn quickly infect any other Macs on the network which are not protected by a protection INIT. This is one way in which viruses can spread very rapidly. Since some applications insist on writing to their own file or folder, it is not always possible to put applications in write-protected folders, but you should make every attempt to do this when it is possible.

• Check server disks frequently with Disinfectant to make certain they are uninfected. For best results, you should take the server out of production and restart it using your Virus Tools or emergency startup disk. This is the only way to guarantee that Disinfectant will be able to scan all the files on the server disk. At Northwestern, we try to check all our servers once per week. For more details on scanning servers, see the discussion in the “Special Features” section.

• Check all new software with Disinfectant before installing it on a server.

• Back up your servers frequently. Run Disinfectant just before each backup.

• The WDEF virus can cause serious performance problems if it infects an AppleShare server. To avoid these problems, administrators should never grant the “make changes” privilege on server root directories. We also recommend deleting the Desktop file if it exists. See the section about the WDEF virus for details.

• Bulletin board operators and other people who maintain and distribute public domain and shareware software have a special responsibility to the Mac community. Please carefully test all new software before distributing it. You should also, of course, run Disinfectant on all new software you receive.

• If you sell software, please check your master disks for infections before sending them out to be duplicated and distributed.

Problem Clinic

This section discusses what you should do if you think that your system may be infected by a new virus, but Disinfectant reports that it cannot locate any known viruses.

There are many, many things which can go wrong on a Macintosh. Almost all of them have absolutely nothing to do with viruses. Thousands of people have reported strange behavior on their Macintoshes to anti-virus experts but, after careful investigation, only a handful of these cases were actually new viruses.

If your Macintosh begins to malfunction or behave unusually, please do not yield to the temptation to immediately blame the malfunction on a new virus. There are several things you can do to try to isolate the problem.

The most common cause of problems is simple errors in software. An error in an application, extension (INIT), control panel (cdev), or other piece of software can cause crashes, hangs, damaged files, trashed disks, or any other kind of problem imaginable.

Thus, the first question you should ask is, “Have I installed any new software lately?” If the answer is “Yes,” try removing the software and see if the problem disappears.

One very common symptom on the Macintosh is problems with the proper display of icons in Finder windows. This symptom is almost never due to a virus, save for the Scores virus which does change the appearance of a few icons. This problem is almost always due to a damaged “desktop.” If your icons are not being displayed properly, you should rebuild the desktop.

To rebuild the desktop on a hard drive, if you are using System 6, first use the “Set Startup” command in the Finder’s Special menu to specify that you want to start up using Finder instead of MultiFinder. For either System 6 or System 7, restart your Macintosh, keeping the Command and Option keys held down throughout the startup process. An alert will appear asking if you really want to rebuild the desktop. Click the OK button when the alert appears.

To rebuild the desktop on a floppy disk, hold down the Command and Option keys while inserting the floppy into a floppy drive. Click the OK button when the alert appears.

Another common problem is damaged applications. If an application begins behaving unusually, try replacing it with a known good copy from your locked original master floppy.

Another common problem is damaged system files in the System folder. The best way to cure this problem is to rebuild your System folder from scratch. Restart your Macintosh from a startup floppy. Drag the Finder file outside of the System folder on your hard drive. Rename your hard drive System folder “Old System Folder.” Then use your Apple installer disks to install a completely new System folder on the hard drive. Restart from this hard drive. If your problem disappears, then you have verified that the cause of the problem was something in your old System folder.

Under System 7, open both your old and your new System files. Drag all of your old fonts and sounds from your old System file to your new System file. Under System 6, use the Font/DA Mover to copy all of your fonts and desk accessories from your old System file to your new System file.

Next, copy files, a few at a time, from your old System folder into your new System folder. Restart your Mac after each copying operation and use it for a while to see if the problem has come back. If the problem has not come back, copy a few more files over and repeat the process. If the problem reappears, you will have narrowed down the cause of the problem to the last few files which you copied. You can now remove these last few files from your new System folder one at a time to locate the file which is causing the problem. Replace the problem file by a known good version. If the problem persists, delete the problem file. Finally, remove the old System folder.

In some cases, software errors can damage the areas on your disk which contain file directories and other important system information. This can sometimes be so serious that all or some of the files and folders on the disk become inaccessible, or the system may not even be able to mount the disk at all, or the system may simply behave strangely. In this case, you may attempt to use a disk recovery utility, or you may be forced to reinitialize and reformat the disk and reload your files from backup floppies or tapes. There are several good disk recovery utilities available, including Apple's Disk First Aid, which is included with every Mac sold. If you have access to Apple's Macintosh Technical Notes, consult note number 134, "Hard Disk Medic & Booting Camp."

Some problems can be cured by resetting the parameter RAM.

To reset the parameter RAM under System 7, hold down the Command, Option, P, and R keys while restarting your Mac. When the RAM has been zapped, you will hear a beep, and the system will restart again. You can release the keys at this point.

To reset the parameter RAM under System 6, hold down the Command, Option, and Shift keys while opening the Control Panel desk accessory.

If all else fails and you still suspect that your system may be infected by a new virus, there are a few additional things you can try. Monitor application file sizes and last modification dates with the Finder's Get Info command. If your applications are consistently growing in size, or if their last modification dates are consistently changing, this is one indication that there may indeed be a virus spreading on your system. Do not, however, be concerned about changes in size or changes in the last modification date of your System file; this is normal and does not indicate a virus. Also, some applications modify themselves, and in these cases you may see a legitimate increase in size and/or change in the last modification date. Look for consistent patterns of change which affect several files.

If your problems continue, try to obtain the assistance of a knowledgeable friend or local expert. If you are a university student, staff member, or faculty member, ask for assistance at your campus computing center. If you work for a corporation with a computer department, ask the local gurus within the department for help. Go to a meeting of your local Mac user group and ask for help.

If you have followed all of this advice and if you still think that you may have a new virus, then you should feel free to contact the author of Disinfectant for assistance. His addresses are at the end of this manual. Please mail him a detailed report and, if it is at all possible, include copies of files which you suspect may be infected. Please do not try to call him on the phone.

The Viruses

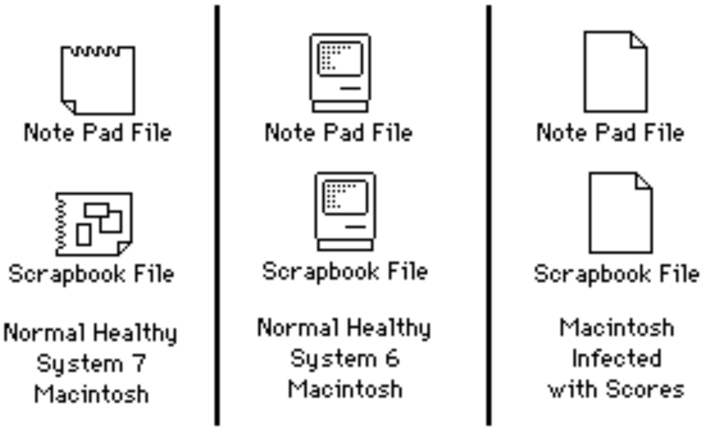
The following sections describe all of the known Mac viruses.

The Scores Virus

According to news reports, the Scores virus was written by a disgruntled programmer. It specifically attacks two applications which were under development at his former company. Fortunately, neither of the two applications was ever released to the general public. Scores was first discovered in the Spring of 1988.

Scores is also sometimes known 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 for the Note Pad and Scrapbook files. They should have distinctive icons under System 7, or look like little Macintoshes under System 6. If they look instead like blank sheets of paper with turned-down corners, your software may have been infected by Scores.


Note Pad File
Scrapbook File
Normal Healthy System 7 Macintosh
Note Pad File
Scrapbook File
Normal Healthy System 6 Macintosh
Note Pad File
Scrapbook File
Macintosh Infected with Scores

It is possible to be partially infected by Scores and still have normal Note Pad and Scrapbook icons. Consequently, we recommend running Disinfectant to make certain your system 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 or some other utility program. Do not confuse Scores’ invisible Desktop file with the Finder’s invisible Desktop file; they have nothing to do with each other. The Finder’s Desktop file lives at the root level on your disk, outside the System folder, while Scores’ Desktop file lives inside the System folder. Also, Scores’ Desktop file has an extra space character at the end of its name.

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

Scores gets its name from the invisible “Scores” file that 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 the two specific applications. It does occupy memory and disk space, however, and this can cause problems all by itself. People have reported problems printing and using MacDraw and Excel. There are also several errors in Scores which could cause system crashes or other unexplained behavior.

There is a serious conflict between Scores and Apple’s System Software release 6.0.4 and later releases of System 6. In System 6.0.4, Apple began using some resources with the same type and 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. When Disinfectant repairs the file, it deletes the Scores viral resources, but it does not replace the Apple versions. In this situation, Disinfectant issues a special error message, telling you that the resulting file is damaged and should not be used. You should immediately delete the damaged System file and replace it with a copy from original locked Apple release disks.

The nVIR Virus

According to news reports, 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 basic strains, which we call “nVIR A” and “nVIR B.”

We have reliable reports of an earlier third version of nVIR which was malicious. It destroyed files in the System folder. This earlier version appears to be extinct, and we have not been able 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 it does not create any invisible files. nVIR begins spreading to other applications immediately, without the two day delay. Whenever a new application is run, it becomes infected immediately, without the two to three minute delay. As with Scores, some applications are immune to infection, the Finder and DA Handler usually also 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 (if MacinTalk is not installed in the System folder). 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” twice or beep twice with a probability of 1/256.

When the counter reaches zero, nVIR B will sometimes beep. nVIR B does not call MacinTalk. 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. Disinfectant will report that such offspring are infected by both nVIR A and nVIR B and will properly repair them.

Unlike Scores, there is no way to tell that you have an nVIR infection just by looking at your system. You must run Disinfectant or some other virus detection tool.

One of the viral resources added to infected files by nVIR has the resource type “nVIR,” which is how it got its name.

As with Scores, nVIR occupies both memory and disk space, and this alone is enough to cause problems.

In addition to the two basic strains of nVIR, many “clones” of nVIR B have appeared. These clones are all identical to nVIR B with the exception of a few very minor technical differences. Disinfectant recognizes all of these clones and treats them exactly the same as nVIR B.

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 between the two strains. The original strain is called "INIT 29 A". The variant is called "INIT 29 B".

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. The ANTI B strain was 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 used. It only spreads when Finder is used under System 6.

There is an error in ANTI which causes it to slightly damage applications in such a way that Disinfectant cannot perfectly repair them. In other words, the application as repaired by Disinfectant is usually not identical to the uninfected original application. The damage is very minor, however, and in almost all cases it does not cause any problems. If you experience problems with an application which was infected by ANTI and repaired by Disinfectant, we recommend that you delete the repaired copy and replace it by an uninfected original copy. This is good advice in any case.

(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 the 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, hence 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. Disinfectant reports that such applications are infected by both strains and repairs them properly.

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 (because 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 this virus. Disinfectant will nevertheless recognize it and repair infected files just in case you have some very old disks which might still be infected.

Disinfectant repairs both infected System files and infected copies of the original HyperCard stack. If you try to run the repaired stack, HyperCard will issue an error message.

There were two slightly different versions of MacMag. The differences were very minor and both versions were programmed to behave identically. Disinfectant properly detects and repairs both versions.

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 (hard drives and floppies) used under System 6 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, 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 (the IIci and later models). The virus also causes other Macs to crash much 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. See the “Problem Clinic” section for details. It is often easier to get rid of a WDEF infection by simply rebuilding the Desktop file than it is to use Disinfectant. 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, however.

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, VirusDetective, or some other tool 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 cause for concern.

When using Disinfectant to repair WDEF infections under System 6, you must use Finder instead of MultiFinder. Under MultiFinder, the Desktop files are always “busy,” and Disinfectant is not able to repair them. If you try to repair using MultiFinder, you will get an error message.

In addition to the two known strains of the WDEF virus, Disinfectant will also detect and repair other strains which may exist but have not yet been reported. If an unknown strain is detected, Disinfectant places the following message in the report:

```
### File infected by an unknown strain of WDEF
```

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 behave 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 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.

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 you cannot use the last modification dates in the Disinfectant report to trace the source of a ZUC infection.

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 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 usually 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.

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 Disinfectant cannot repair them properly. In this situation, Disinfectant removes the virus from the application and issues a special error message, telling you that the resulting file is damaged and should not be used. You should immediately delete the damaged file and replace it with a known good copy from an original release disk.

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 or some other tool.

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 quite 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 then causes the Atari to crash.

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 simple 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. See the "Problem Clinic" section for details.

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, however, is cause for concern.

When using Disinfectant to repair CDEF infections under System 6, you must use Finder instead of MultiFinder. Under MultiFinder, the Desktop files are always "busy," and Disinfectant is not able to repair them. If you try to repair using MultiFinder, you will get an error message.

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. Unfortunately, the new version escaped detection by the Disinfectant version 2.9 protection INIT (but not by the application). The Disinfectant version 3.0 INIT fixes this problem. In version 3.0, both the INIT and the application recognize both the original virus and the new version.

In addition to the known strain of CDEF, Disinfectant will also detect and repair other strains which may exist but have not yet been reported. If an unknown strain is detected, Disinfectant places the following message in the report:

```
### File infected by an unknown strain of CDEF
```

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 a number of people around the world were affected. The games were named “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.

Disinfectant identifies both infected files and the Trojan horse as being infected by the MBDF virus. Repairing an infected file removes the virus and returns the file to the state it was in before being infected. Repairing the Trojan horse renders it ineffective and inoperable.

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 the 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.

We also have 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 or some other tool.

Special thanks 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. We strongly encourage other vendors to 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 drives 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 (also known as startup documents or system extensions). It does not infect the 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.

If you have an INIT file which is infected by the INIT 1984 virus, when the virus attacks during startup, the Disinfectant INIT beeps ten times, and an alert is presented at the end of the startup sequence. The virus is neutralized and does not spread or cause any damage, but the non-viral part of the infected INIT runs as usual.

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 not 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 game 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. When you use Disinfectant to attempt to repair an infected application, Disinfectant removes the virus from the file, but leaves the file damaged. You should not attempt to use such a file. Disinfectant issues the following error message:

```
### This file was damaged by the virus, and it cannot
### be repaired properly. You should delete the file
### and replace it with a known good copy.
```

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. Disinfectant cannot repair this damage to the System file. If the virus damages your System file, you will have to reinstall it.

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 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.

The INIT-M Virus

The INIT-M virus was discovered at Dartmouth College in April, 1993.

INIT-M is a malicious virus. It is designed to trigger on any Friday the 13th. The virus severely damages a large number of folders and files. File names are changed to random 8 character strings. Folder names are changed to random 1-8 character strings. File creators and types are changed to random 4 character strings. This changes the icons associated with the files and destroys the relationship between programs and their documents. File creation and modification dates are changed to Jan. 1, 1904. In some cases, one file or folder on a disk may be renamed “Virus MindCrime”. In some very rare circumstances, the virus may also delete a file or files.

The virus can also sometimes cause problems with the proper display of windows.

The virus only spreads and attacks under System 7.0 or later. It does not spread or attack under System 6. The Disinfectant protection INIT, however, will detect an infected application under any system.

The virus infects all kinds of files, including extensions, applications, preference files, and document files.

The virus creates a file named “FSV Prefs” in the Preferences folder. If you use Disinfectant to repair an infected system, it will delete this file.

The damage caused by the INIT-M virus is very similar to that caused by the INIT 1984 virus. Despite this similarity, the two viruses are very different in other respects and should not be confused.

The CODE 1 Virus

The CODE 1 virus was discovered at several colleges and universities on the east coast of the United States in November, 1993.

The virus infects both applications and the System file. It does not infect document files. It spreads under both System 6 and System 7.

The virus renames the system hard drive to “Trent Saburo” whenever an infected Mac is restarted on any October 31. Although the virus does not contain any other intentionally destructive code, it can cause crashes and other problems.

The INIT 9403 Virus

The INIT 9403 virus was discovered in Italy in March, 1994. This virus is also sometimes called the “SysX” virus.

Unlike most of the other Mac viruses, INIT 9403 is very destructive. After a certain number of other files have been infected, the virus will erase disks connected to the system. It attempts to destroy disk information on all connected hard drives (> 16 Mb) and attempts to completely erase the boot volume.

The current strain of the INIT 9403 virus has been found only on Macs running the Italian version of the Macintosh system (so far). However, we strongly urge you to protect yourself against this virus even if you do not run the Italian system.

It appears that the virus was initially spread by an altered version of some pirated software. The software, when run, installs the virus on the affected system.

Once present, the virus alters the Finder file and may insert copies of itself in various compaction, compression, and archive programs. These infected files can then spread the virus to other Macintoshes.

The virus spreads under both System 6 and System 7.

Sample Report

The following example shows a report generated by a disinfection run on a Scores-infected hard disk drive.

```
My Hard Drive
Disk disinfection run started.
12/16/88, 10:04:12 AM.
----------------------------------------------
My Hard Drive
  My Programs
    Games
      SuperGame
### File infected by Scores.
Last modification 11/2/88, 11:15:03 PM.
File repaired.
----------------------------------------------
My Hard Drive
  My Programs
    Word Processors
      MacWrite
### File infected by Scores.
Last modification 12/15/88, 5:02:49 PM.
File repaired.
----------------------------------------------
My Hard Drive
  System Folder
    Desktop
### File infected by Scores.
Last modification 12/13/88, 2:48:40 PM.
File deleted.
----------------------------------------------
My Hard Drive
  System Folder
    Finder
### File infected by Scores.
Last modification 12/14/88, 3:02:24 PM.
File repaired.
----------------------------------------------
My Hard Drive
  System Folder
    Note Pad File
### File infected by Scores.
Last modification 12/13/88, 2:48:34 PM.
File repaired.
----------------------------------------------
My Hard Drive
  System Folder
    Scores
### File infected by Scores.
Last modification 12/13/88, 2:48:33 PM.
File deleted.
----------------------------------------------
My Hard Drive
  System Folder
    Scrapbook File
### File infected by Scores.
Last modification 12/13/88, 2:48:35 PM.
File repaired.
```

```
----------------------------------------------
My Hard Drive
  System Folder
    System
### File infected by Scores.
Last modification 12/13/88, 2:48:40 PM.
File repaired.
----------------------------------------------
My Hard Drive
Disk disinfection run completed.
12/16/88, 10:08:30 AM.

Summary:
984 total files.
0 errors.
8 files infected by Scores.
8 infected files total.

Earliest infected file: SuperGame
Last modification 11/2/88, 11:15:03 PM.
```

The last modification dates in the report are sometimes useful for tracking down the history and source of an infection. The infected application with the earliest last modification date is often the source of the infection.

E.g., in the sample report above, SuperGame is the earliest infected application, with a last modification date of 11/2. The System file was last modified on 12/13. If you obtained your copy of SuperGame sometime after 11/2, and if you first ran it on or before 12/13, then SuperGame was probably the source of the infection. You should contact the source of the application and tell them that their software is probably infected too. You should likewise contact anybody else to whom you have given copies of SuperGame or any of your other infected files, because their software may also be infected.

If Disinfectant’s report notes that a System file is the earliest infected file, this means that the application that caused the original infection of your system is no longer on, or never was on, the disk being scanned. Check all your other disks (hard drives and floppies) to attempt to locate the file that introduced the virus to your system.

This kind of analysis is not infallible, but it can sometimes be useful in tracing back a chain of infections.

The ZUC, Frankie, and MBDF viruses do not change the modification date when they infect a file, so this kind of analysis will not help locate the source of an infection by one of those viruses. This kind of analysis is also useless when trying to locate the source of a WDEF or CDEF infection, since those viruses only infect Finder Desktop files, which are constantly being modified legitimately by the Finder.

Special Features

In this section we discuss various advanced features of Disinfectant, technical topics, and other miscellaneous items.

• It is very important to realize that detecting and repairing infected files is quite complicated and it is highly likely that there are some rare cases we do not handle properly. Read the disclaimer at the beginning of this manual and take it seriously.

• Disinfectant is “modeless.” This means several things. You can have multiple windows open at the same time, you can use desk accessories, and you can use application switching. You can start a scan and switch to some other application and the scan will continue in the background. You can do just about anything except start another scan while a scan is in progress. You can read the manual in the Help window, adjust options in the Preferences window, use the online help facility, admire the About window, etc.

• Disinfectant requires a Mac 512KE or later model and system 6.0 or later. If you try to run Disinfectant on a Mac which does not meet these requirements, it will present an error message alert and quit.

• Disinfectant is 32-bit clean and may be run under A/UX.

• Disinfectant can scan in the background. The Notification Manager is used to notify you if an infection is discovered or if Disinfectant requires attention for some other reason.

• Disinfectant can scan and repair both MFS and HFS disks. Single-sided 400K floppies are usually in MFS format, whereas other disks are usually in HFS format.

• Disinfectant tries to perform careful error checking. E.g., it properly reports disk full errors on attempts to save files, out of memory errors, and errors on attempts to disinfect “busy” and “damaged” files. The summary at the end of the report tells you if there were any errors. All error messages and messages reporting infected files begin with “###,” to make them easy to find in the report.

• Disinfectant has a “preferred” memory partition of 1000K and a “minimum” memory partition of 300K. On 1 megabyte Macintoshes running System 6 with MultiFinder, there is not enough memory to allocate the preferred partition and you will have to run with the smaller minimum partition. The large memory partition is desirable because some applications use surprisingly large resources and Disinfectant must have enough memory to load them and check them for viruses. Some very large programs require even more memory, and you may have to use the Finder’s “Get Info” command to give Disinfectant more memory.

• Disinfectant may be used to scan AppleShare server disks and remote disks on a TOPS network. For the best results, however, we recommend that you remove servers and shared disks from production and scan them using the Mac to which they are directly connected. This is the only way to avoid file busy errors, insufficient privileges errors, and other problems. Scanning a local disk is also much faster than scanning a disk over a network. This is also the only way to scan the Server folder on an AppleShare server disk.

One problem with System 6 AppleShare server disks is that they use a different kind of “desktop” file than is used on regular disks. If the server disk contains a large number of applications, it may not be possible to start up the server using a regular startup disk. (The Finder will bomb or hang during the process of building its version of the Desktop file.) You can avoid this problem by creating a special Virus Tools startup floppy that contains a copy of Apple’s “Desktop Manager” startup document file. Use this special startup floppy only for scanning System 6 AppleShare servers.

On a TOPS network, we have noticed that TOPS sometimes beeps and flashes an alert intermittently while scanning with Disinfectant. The problem is not serious. It is annoying, but it does not interfere with the scan.

• Viruses sometimes damage applications in such a way that they cannot be run at all. Sometimes viruses only partially infect files. It is also possible for a file to be infected by more than one virus. In most of these special cases, Disinfectant is able to repair the files. If it is impossible for Disinfectant to properly repair such a file, an appropriate error message is issued. Consult the section in this manual titled “Error Messages” for detailed information on what each message means and for advice on what to do if you get an error message.

• Disinfectant may be installed on a server and used by more than one person simultaneously.

• Disinfectant may be used on Macs with no hard drive and only a single floppy drive. In this minimal configuration, you need to use your Virus Tools disk.

Start up Disinfectant from your Virus Tools disk. Disinfectant will run automatically. Click the Eject button to eject your startup disk. Use the floppy drive to insert the disks you wish to scan or disinfect.

When you eject the startup disk, we preload the information Disinfectant needs to do scanning from the disk. This minimizes “floppy shuffling” on these systems. Disinfectant displays a dialog telling you to “Please wait” while it does this preloading, which can take quite some time. Please be patient.

• Printing is possible on a Mac with no hard drive, but it requires a special startup disk. The problem is that printing requires extra disk space for the printer driver files and ImageWriter spool files. There isn’t enough free disk space for these files on a normal 800K startup disk.

To solve this problem, you should prepare a special printing startup disk containing a copy of the 6.0.5 System file, a copy of Disinfectant, and the appropriate printer driver files. For ImageWriter printing, you need the file named “ImageWriter.” For LaserWriter printing, you need the two files named “Laser Prep” and “LaserWriter.” Use original locked Apple System Software release disks for your copies of the System file and the printer driver files.

Do not include a copy of the Finder file on this special printing startup disk! Eliminating the Finder file is the trick which creates enough extra disk space to make printing possible.

After you have copied all of the files mentioned above to your printing startup disk, use the Font/DA Mover to install the fonts you wish to use for printing. For ImageWriter printing, we suggest that you include at least the Geneva 10 font. For LaserWriter printing, we suggest that you include at least the Palatino 10 and Helvetica 10 fonts. In any case, you also need Geneva 9 and Chicago 12 for the proper display of text on the screen.

After you have installed your fonts, click the Disinfectant icon to select it and then use the Finder’s Set Startup command to set Disinfectant as the startup application for this disk.

Do not lock your printing startup disk. The Chooser does not work with locked startup disks. Printing to ImageWriters also requires an unlocked startup disk.

Start up your Macintosh using the printing startup disk you just created. The Disinfectant application should open automatically. Use the Chooser desk accessory to select the printer you wish to use.

With this printing startup disk, you should be able to use all the features of Disinfectant, including printing.

It is not possible to print all of the Disinfectant manual at one time on an ImageWriter using this printing startup disk. We suggest that you print the manual in 10 or 15 page sections. For example, use the Print command to print pages 1 through 10. After the first 10 pages have been printed, use the Print command again to print pages 11 through 20, and so on.

When you quit Disinfectant, you will get an alert saying that the Finder is “busy or damaged.” This is normal with the printing startup disk. Click the Restart button to restart using some other floppy startup disk.

Error Messages

This section presents all of Disinfectant's error messages, in alphabetical order, with a brief explanation of each one.

```
### An error or inconsistency was detected while
### trying to repair this file.
### WARNING: This file may still be infected!
```

Your file was infected, but while attempting to repair it, Disinfectant discovered something wrong with the file. The file may still be infected. Scan the file again with Disinfectant to find out if it is still infected. If it is still infected, you should delete it. If Disinfectant reports that it is no longer infected, you can try running it to see if it works. It may be usable or it may be damaged in such a way that it cannot be used. This error is not common, but it can occur in unusual situations.

One situation in which this error can occur is if an application is infected by more than one virus and you attempt to use some other virus tool to repair the file before running Disinfectant. Some other virus tools cannot handle multiple infections properly and they sometimes leave the application damaged in such a way that Disinfectant cannot repair it properly.

```
### An I/O error occurred while trying to check
### this file.
```

```
### An I/O error occurred while trying to repair
### this file.
### WARNING: This file may still be infected!
```

These error messages are listed in the report if a hardware error occurs while trying to read or write a file. They usually mean that the disk itself or the disk drive is not operating properly. You can try running Disinfectant again on the same file. If the hardware problem is intermittent, it might work the second time.

```
### File infected by xxxxx.
```

Your file is infected by a virus. "xxxxx" is the name of the virus (Scores, nVIR A, etc.).

```
### File infected by an unknown strain of xxxx
```

Your file is infected by a strain of the WDEF or CDEF virus which has not yet been reported. If you have not already repaired the file, we would appreciate it if you would send us a copy of the infected file. See the sections on the WDEF and CDEF viruses for more information.

```
### File partially infected by xxxxx,
### but not contagious.
```

Your file is partially infected by the virus named "xxxxx," but the infection is not contagious. These kinds of infections are not dangerous and they cannot spread to other files. You may choose to leave the infection in the file or you may use Disinfectant to remove the infection.

Partially infected files sometimes are the result of other virus tools which have errors. The other virus tool may remove part of an infection, but not all of the infection.

Partial infections can also arise on Gatekeeper-protected systems. In particular, if the Scores virus attacks a Gatekeeper-protected system, a harmless part of the Scores infection will manage to evade Gatekeeper's protection mechanisms.

### File partially infected by nVIR A or nVIR B,
### but not contagious.

nVIR A and nVIR B are different viruses, but some of their parts are identical. It is possible for only these common parts to be present in an infected file. In this case, Disinfectant has no way of knowing which virus originally attacked the file, so it issues this special message.

### NOTE: Some errors were reported. For a detailed
### explanation of an error message, press Command-?
### and click the error message text.

This message appears in the summary section of the report if any other error messages occurred during a scan.

### Scan canceled.

You canceled a scan or disinfection run.

### System files cannot be scanned over TOPS.

This error should only occur if you try to scan a disk over a TOPS network. TOPS does not permit access to currently active System files over the network. We recommend that you scan the disk using the Mac to which the disk is directly connected.

If this error occurs in some other situation, it means that there is probably an error in Disinfectant. We would appreciate it if you would send a report to the author.

### The disk is too full to repair this file.
### WARNING: This file may still be infected!

This error may occur if a disk is very full and you attempt to repair an infected file on the disk. Disinfectant requires at least a small amount of free space on the disk before it can repair the file. Try moving some of the files on the disk to some other disk to make more room and run Disinfectant again.

### The inserted disk is uninitialized, damaged,
### or not a Mac disk. It cannot be scanned.

This error occurs if you insert an uninitialized, damaged, or non-Macintosh disk on a scanning station with no mouse or keyboard. The disk is ejected and not scanned.

### The resource fork of this file is damaged or
### in an unknown format. It cannot be checked.

Macintosh files have two parts or “forks:” the resource fork and the data fork. When Disinfectant checks a file, it tries to open the resource fork. This message means that the information stored in the resource fork is not valid resource information. The data fork may still be intact and usable. For document files, this is usually not a problem. For applications and system files, this usually indicates that something is seriously wrong with the file and you should replace it with a known good copy of the file.

WARNING: It is possible for an application to be damaged and yet still be infected and contagious. For this reason, you should not attempt to use applications which have damaged resource forks.

For some reason, we have seen invalid resource information in a number of StuffIt archive files. These “damaged” files are usually still usable since StuffIt stores the archived files in the data fork, not the resource fork.

Disinfectant also reports that all Reflex database files are “damaged.” Reflex makes non-standard use of the resource fork in its database files. These files are not really damaged. They are still usable, but only by Reflex.

The same problem has been reported with some files created by MacTran, which also makes non-standard use of the resource fork.

The same problem has also been reported with the "phrase library" files created by Studio Session and Super Studio Session.

```
### There is not enough memory to check this file.
```

```
### There is not enough memory to repair this file.
### WARNING: This file is probably still infected!
```

Disinfectant was unable to get enough memory to check or repair the file.

This error is usually caused by applications which contain very large CODE resources. Disinfectant must load these resources into memory to check them for viruses and, if there is not enough memory available, you get this error message.

Another possible cause of this error is that the file is damaged.

If you get this error, you should give Disinfectant more memory. Quit Disinfectant. Select the Disinfectant program icon in the Finder. Select the Finder's "Get Info" command in the "File" menu. Increase the amount of memory allocated to Disinfectant in the Get Info window. Close the Get Info window. Run Disinfectant again.

```
### This file is busy and cannot be checked.
```

Your file could not be opened for reading because the file was already open with exclusive access by some other application. This message should only occur on server disks. For server disks, we recommend that you remove the server from production and restart using a startup floppy disk. This should avoid file busy errors. For more details on scanning servers, see the "Special Features" section.

```
### This file is busy and cannot be repaired.
### Restart using your emergency startup
### disk and try running Disinfectant again.
### WARNING: This file is still infected!
```

```
### This file is busy and cannot be repaired.
### Restart using your locked "Virus Tools"
### disk and try running Disinfectant again.
### WARNING: This file is still infected!
```

```
### This file is busy and cannot be repaired.
### To repair this file, rebuild the desktop.
### WARNING: This file is still infected!
```

Your file could not be opened for writing because the file was already open by some other application. This error is common when using System 7, System 6 with MultiFinder, or when scanning server disks. For server disks, we recommend that you remove the server from production and restart it using a locked startup floppy. This should avoid file busy errors. For more details on scanning servers, see the "Special Features" section.

The first message above is only issued under System 7. The second message above is only issued under System 6.

The third message above is issued when a Finder desktop file is infected and busy. In this case, the easiest way to remove the infection is to rebuild the desktop. See the "Problem Clinic" section for details.

```
### This file was damaged by the virus, and it cannot
### be repaired properly. You should delete the file
### and replace it with a known good copy.
```

Viruses sometimes damage files in such a way that they cannot be repaired properly. In this case, Disinfectant removes the virus from the file, but leaves the file damaged. You should not attempt to use such a file. You should delete it and replace it with a known good copy of the file.

In particular, the T4 virus damages files when it infects them. Files infected by T4 cannot be repaired. If you attempt to repair a file infected by T4, you will get this error message. See the section on T4 for details.

This error message is also issued when the Scores virus has infected a System file from Apple's System Software release 6.0.4 or later. See the section on Scores for details.

The MDEF D virus can also sometimes damage applications. See the section on MDEF for details.

```
### Unexpected error (nnn).
```

```
### Unexpected error (nnn) occurred while trying
### to open this file for repair.
### WARNING: This file is still infected!
```

Unexpected errors should not occur. It means that there may be an error in Disinfectant. We would appreciate it if you would send a note to the author describing what you were doing when the error occurred. Please specify the error number reported in the message. If possible, also send us a copy of the file that was being scanned when the error occurred.

```
### Unexpected error (nnn). If you are using
### Gatekeeper, check to make certain you have
### granted privileges to Disinfectant.
### WARNING: This file is probably still infected!
```

One possible cause of unexpected errors is attempting to repair infected files on a Gatekeeper-protected system when you have forgotten to grant Disinfectant privileges. You should grant Disinfectant all privileges ("File" and "Res" privileges for "Other," "System" and "Self").

```
### WARNING: You do not have the proper privileges
### to access files in some of the folders. Some
### files in those folders may be infected!
```

```
### You do not have Make Changes privilege
### to the folder containing this file.
### It cannot be repaired.
### WARNING: This file is still infected!
```

```
### You do not have See Files privilege
### to this folder. Files within this folder
### cannot be checked.
```

```
### You do not have See Folders privilege
### to this folder. Folders within this folder
### cannot be checked.
```

```
### You have neither See Files nor See Folders
### privileges to this folder. This folder
### cannot be checked.
```

These error messages are issued if a server folder is encountered for which you do not have the necessary access privileges. To avoid these errors, we recommend that you remove the server from production and restart it using a locked startup floppy. For more details on scanning servers, see the “Special Features” section.

Alerts and Dialogs

This section presents all of Disinfectant's alerts and dialogs, in alphabetical order, with a brief explanation of each one.

• A virus may still be active in memory. Some of your files may have or could become reinfected. You should immediately restart your Macintosh using a locked startup floppy and run Disinfectant again.

When you quit after a disinfection run, Disinfectant checks to see if any infected files were found in the currently active System folder. If any were found, this alert is presented.

Click the Restart button to restart your Macintosh. Click the Cancel button to return to Disinfectant. Click the Quit button to quit Disinfectant.

• An old version of the Disinfectant INIT is installed on this system. Do you want to install the new version?

When Disinfectant starts up, it checks to see if an old version of the Disinfectant INIT is installed in the currently active System folder or Extensions folder. If an old version is installed, this alert is presented. Click the Install button to install the new version. Click the Cancel button to leave the old version installed. Installing the new version also removes the old version.

• An unexpected error (nnn) occurred while trying to save a file.

This alert is presented if Disinfectant encounters an unexpected error while trying to save a copy of the manual, a report, or the protection INIT. This alert should not happen. If it does, it might be an error in Disinfectant and we would appreciate it if you would notify the author.

• Disinfectant has found an infected file.

This alert is presented if, while running in the background under MultiFinder, Disinfectant finds an infected file and you have selected the "Also display alert" option in the "Notification options" section of the Preferences window.

• Disinfectant is unable to repair files on this system. One possible reason is that you are using Gatekeeper and you forgot to grant Disinfectant privileges. Another possible reason is that you are using the special University of Michigan version of Vaccine (Vaccine.UofM). You must remove this version of Vaccine from your System folder before using Disinfectant to repair files. You may use Disinfectant on this system to check for viruses, but you will not be able to use the Disinfect button to repair infected files.

Some virus prevention tools can interfere with Disinfectant in such a way that it is impossible for Disinfectant to properly repair infected applications. If Disinfectant detects such a virus prevention tool, it presents this alert. When you click the OK button, the current scan is canceled and the Disinfect button is disabled.

The version of Vaccine mentioned in the alert is not the normal Vaccine. It is a special version that was prepared just for the University of Michigan.

You may also get this alert if you are using the regular version of Vaccine and you click the Denied button instead of the Granted button by mistake.

• Disinfectant requires attention.

This alert is presented if, while running in the background, Disinfectant requires your attention (for some reason other than the discovery of an infected file) and you have selected the "Also display alert" option in the "Notification options" section of the Preferences window.

• Disinfectant requires a Mac 512KE or newer model. It does not work on the Mac 128K, 512K, or XL.

Disinfectant cannot be used on Macs with the old 64K ROMs.

• Disinfectant requires System 6.0 or later.

Disinfectant requires System 6.0 or later. If you try running Disinfectant on an earlier system, it will present this alert. When you click the OK button, Disinfectant quits to the Finder.

• Out of memory. Disinfectant has unexpectedly run out of memory. Use the Finder's "Get Info" command to give Disinfectant more memory, then try running it again.

This alert is presented if Disinfectant runs out of memory. When you click the "Quit" button, Disinfectant quits.

If you get this error, you should give Disinfectant more memory. Select the Disinfectant program icon in the Finder. Select the Finder's "Get Info" command in the "File" menu. Increase the amount of memory allocated to Disinfectant in the Get Info window. Close the Get Info window. Run Disinfectant again.

In most cases, if Disinfectant does not have enough memory to check a file, you will get the error message "There is not enough memory to check this file" in the report section of the main Disinfectant window, and then Disinfectant will continue to scan the next file. The "Out of memory" alert described here is much less common, although it is possible in some unusual circumstances.

• Please wait…

This message is displayed if you eject the disk containing Disinfectant and/or the System file. Before ejecting the disk, Disinfectant loads all the information from the disk that it might need later. This can take quite some time, so you should be patient.

• Printing error—could not locate printer driver in System folder.

This alert occurs if you try to print a report or the manual and the printer driver has not been properly installed. For example, to print on an ImageWriter, you must have the system file named "ImageWriter" in the same folder as your System file.

• Printing error—the startup disk is full.

This alert occurs if there is not enough room on your startup disk to complete a printing operation. Try to make more room on your startup disk, then try printing again.

• Printing error—the startup disk is locked.

This alert occurs if printing fails because the startup disk is locked. Unlock the startup disk, or create an unlocked copy of your startup disk, and try printing again.

• Printing error—you must use the Chooser to select a printer.

This alert occurs if you try to print when there is no currently selected printer. Use the Chooser desk accessory to select a printer.

• Printing error (error code = nnnn).

An unexpected error occurred during printing. "nnnn" is the error number. This alert should not occur. If it does, we would appreciate it if you would send a note to the author. Please specify the error number reported in the message. Click the OK button to return to Disinfectant.

• Printing "xxxxx." To cancel, hold down the Command key and type a period (.).

This informative message is displayed during printing.

• Replace existing “Disinfectant INIT”?

This alert is presented when you install the protection INIT if a file with the same name already exists. Click the Cancel button to abort the file save operation. Click the Replace button to delete the old file and replace it by the new one.

• Save report before clearing?

When you clear the report, Disinfectant checks to see if the report contains any messages for infected files. If it does, this alert is presented. There are three buttons: Save, Cancel, and Clear. The Save button presents a dialog which lets you choose the location of the saved report, saves the report, and then clears the report. The Cancel button returns to Disinfectant. The Clear button clears without saving the report.

• Save report before quitting?

When you quit Disinfectant, it checks to see if the report contains any messages for infected files. If it does, this alert is presented. There are three buttons: Save, Cancel, and Quit. The Save button presents a dialog which lets you choose the location of the saved report, saves the report, and then quits. The Cancel button returns to Disinfectant. The Quit button quits without saving the report.

• The application “xxxxxxxxxx” is infected by the yyyyy virus. Use Disinfectant to remove the virus.

This alert is presented by the Disinfectant protection INIT when it detects an infected application.

• The Disinfectant protection INIT has been installed. You must restart your Macintosh to activate the INIT. WARNING: If you restart now, you will lose all changes to any documents which may be open in other applications! To restart now, select the Restart button. To return to Disinfectant without restarting, select the OK button.

This alert is presented when you select the “Install Protection INIT” command.

• The disk cannot be repaired because it is locked. Please unlock and reinsert the disk.

If you try to disinfect a locked floppy disk, Disinfectant ejects the disk and puts up this alert. Unlock and reinsert the disk. Disinfectant will automatically begin scanning and repairing the disk as soon as you reinsert it. You can use the Cancel button in the alert to cancel the operation and return to Disinfectant.

• The disk cannot be repaired because it is locked. Please unlock and reinsert the disk or insert the next disk to be repaired.

This second form of the unlock alert is used only when the special “scanning station” option is checked in the Preferences window. In this case, you can either unlock and reinsert the original disk or you can insert some other disk. There is no Cancel button in this situation.

• The disk “xxxxxxxxxx” is infected by the yyyy virus. Rebuild the Desktop file on the disk or use Disinfectant to remove the virus.

This alert is presented by the Disinfectant protection INIT when it detects a WDEF-infected disk or a CDEF-infected disk.

• The document cannot be printed because some pages would be truncated on the bottom. To correct this problem, use the Page Setup command. Make the margins smaller or make the font size smaller.

This alert may appear if you try to print with a large font size and/or large margins.

• The document cannot be printed because some pages would be truncated on the right. To correct this problem, use the Page Setup command. Make the left and right margins smaller or make the font size smaller. You might also try printing with landscape orientation instead of portrait orientation.

This alert may appear if you try to print with a large font size and/or large margins. If you are trying to print a report in a very large font size (over 18 points) and you get this alert, try using the Page Setup command to select landscape orientation instead of portrait orientation.

• The file could not be saved because the disk is full.

This alert appears if you try to save a report or the manual and there is not enough room on the disk to save the file. Click the OK button. You may then try to save to a different disk.

• The file could not be saved because the old version of the file is locked.

This alert appears if you try to save a report or the manual or if you try to install or save the protection INIT and there is already a locked version of the file. Unlock the old version of the file and try again.

• The font size must be in the range 1 through 24. Please correct it or click the Cancel button.

This alert appears in the "Page Setup" dialog if you enter a ridiculous font size.

• The INIT file "xxxxxxxxxx" is infected by the INIT 1984 virus. Use Disinfectant to remove the virus.

This alert is presented by the Disinfectant protection INIT when it detects an INIT file which has been infected by the INIT 1984 virus.

• The margins you specified are too large. Please make them smaller or click the Cancel button.

This alert appears in the "Page Setup" dialog if you specified margins that are too big. Disinfectant requires that there be at least a five inch square available for printing after taking into account the margins and page size.

• The protection INIT could not be installed because the startup disk is locked.

This alert is presented if you try to install the Disinfectant protection INIT on a locked startup disk.

• The report is too big. It must be saved or cleared before the scan can continue. Save the report?

Disinfectant has an upper limit for the size of the report. Most people will never be affected by this limit. If you produce a very long report which approaches the size limit, you will get this alert, with three buttons: Save, Cancel, and Clear. Save is the default button. It saves the partial report as a text file, clears the report field, and continues the scan. The Cancel button cancels the scan without clearing or saving the report. The Clear button clears the report field without saving and continues the scan. If you have a single floppy system, you may eject the disk being scanned, insert a different disk, and save the report on that disk. Disinfectant will then ask you to reinsert the disk being scanned.

• The stack "xxxxxxxxxx" is infected by the MacMag virus. Use Disinfectant to remove the virus.

This alert is presented by the Disinfectant protection INIT when it detects a MacMag-infected HyperCard stack.

• This copy of Disinfectant has been damaged, infected by a virus, or otherwise modified. Please delete this copy and use an original unmodified copy.

Disinfectant checks itself when it starts up and notifies you if it has been modified. This may mean that it has been infected by a virus. If this notification occurs, you must remove this particular copy of Disinfectant from your disk and replace it with a known "good" copy of Disinfectant.

- You selected the page range xxx through yyy. There are no pages in this range.

This alert appears when printing if there are no pages in the range you requested. Nothing is printed in this case.

Version History

- Disinfectant Version 3.7.1. July 9, 1997

Version 3.7.1 fixes an error which could sometimes cause crashes when scanning very rare kinds of files while pass the new “more lenient” check for damaged resource forks which was introduced in 3.7.

- Disinfectant Version 3.7. July 7, 1997

Version 3.7 detects a minor variation of the MBDF B virus which was properly detected by the 3.6 INIT but not by the 3.6 application.

The Disinfectant manual now discusses the Microsoft macro virus problem. The introductory text displayed in Disinfectant’s main window warns that Disinfectant does not recognize the macro viruses and refers the user to the manual for more details.

The “All Disks” command in the “Scan” menu has been changed to “All Local Disks”. This command now only scans local disks, not network AppleShare servers.

The “All Disks” command in the “Disinfect” menu has been changed to “All Local Unlocked Disks”. This command now only disinfects local unlocked disks, not network AppleShare servers or locked disks like CD-ROMs or locked floppies.

If you want to scan or disinfect servers, scan or disinfect them individually, or use the “Some Disks” commands in the “Scan” and “Disinfect” menus.

In version 3.7, the check for damaged resource forks is more lenient. Some very large resource files like the “Netscape Resources” file used in Netscape Communicator strictly speaking violate Apple’s rules, but seem to work OK in practice. Version 3.7 no longer considers these kinds of files to be damaged.

This version fixes an error which could sometimes cause Disinfectant to quit with a strange alert message. For example, in some very rare circumstances, it could quit with the message “^0 is already open” when scanning Photoshop. The alert message was supposed to be Disinfectant’s “Out of memory” message.

We made a separate change to make it less likely that Disinfectant will fail with the “Out of memory” alert. Also, the “Out of memory” alert message has been expanded to give more information. It now tells you to use the Finder’s “Get Info” command to give Disinfectant more memory and try again. The “OK” button in this alert has been changed to “Quit”.

- Disinfectant Version 3.6. April 7, 1995

Version 3.6 detects another new clone of the nVIR B virus.

This version also lets you use the Finder’s “Get Info” command to increase Disinfectant’s memory partition. This is needed because programs with large CODE resources are becoming more common, and you sometimes need to give Disinfectant more memory to scan them.

You can also now use the Finder’s “Get Info” command to give Disinfectant a custom icon if you wish.

- Disinfectant Version 3.5. April 2, 1994

Version 3.5 detects the new “B” variant of the INIT 29 virus. See the section on INIT 29 for details.

• Disinfectant Version 3.4.1. March 11, 1994

This version fixes an error which sometimes caused unexpected error number -192 when scanning an enabler file under System 7.1.

The version 3.4 protection INIT incorrectly identified the new INIT 9403 virus using the wrong name for the virus. This error has been fixed.

• Disinfectant Version 3.4. March 3, 1994

Version 3.4 detects the new INIT 9403 virus. See the section on INIT 9403 for details.

Version 3.4 fixes an error which sometimes caused unexpected error number -192 when scanning the active System file on Macs with System 7.1 and an enabler. Thanks to Larry Atkin and Werner Uhrig for helping investigate and fix this error.

• Disinfectant Version 3.3. November 5, 1993

Version 3.3 detects the new CODE 1 virus and new B strain of the MBDF virus. See the sections on the CODE 1 and MBDF viruses for details.

This version also includes a new color icon suite. Thanks to John Stein for contributing the icons. If you don’t see the new color icons on your color monitor, try rebuilding your desktop file.

Under System 7, the new version stores its preferences file inside the Preferences folder instead of inside the System folder proper. The first time you run the new version, it moves your old preferences file from the System folder into the Preferences folder for you.

The new version also fixes an error which caused Disinfectant to crash on very rare kinds of damaged resource files.

• Earlier versions.

3.2 - 4/21/93. INIT-M.
3.1 - 4/12/93. INIT 17.
3.0 - 2/24/93. T4-C strain, new CDEF variant.
2.9 - 7/4/92. T4.
2.8 - 4/19/92. CODE 252.
2.7.1 - 3/25/92. Fix error in 2.7.
2.7 - 2/23/92. INIT 1984.
2.6 - 2/22/92. MBDF.
2.5.1 - 7/7/91. Fix error in 2.5 INIT.
2.5 - 6/28/91. ZUC C and MDEF D.
2.4 - 12/3/90. ZUC B.
2.3 - 10/23/90. MDEF C.
2.2 - 10/2/90. ANTI B.
2.1 - 8/18/90. MDEF B and CDEF.
2.0 - 7/8/90. Major new release with many new features. Also Frankie.
1.8 - 5/20/90. MDEF.
1.7 - 4/2/90. ZUC.
1.6 - 1/30/90. Generic nVIR clones.
1.5 - 12/14/89. WDEF B.
1.4 - 12/8/89. WDEF A.
1.3 - 11/29/89. nVIR B clone.
1.2 - 8/4/89. nVIR B clone.
1.1 - 4/16/89. nVIR B clone.
1.0 - 3/19/89. First release. Scores, nVIR, INIT 29, MacMag, ANTI.

Programmer Notes

I wrote several reusable modules to implement Disinfectant's human interface. You have my permission to use it in your own projects. All I ask is that you give me and Northwestern University appropriate credit in your about box or manual. The source code is in MPW C 3.2.

The source code includes modules that implement volume selection via Drive and Eject buttons and an optional drive popup menu, volume and folder scanning, report generation and display in scrolling fields, the Disinfectant online manual and help system, and miscellaneous reusable utilities.

The source code is available via anonymous FTP at:

ftp://ftp.nwu.edu/pub/disinfectant/

If you do not have access to FTP, mail me a floppy and a stamped self-addressed disk mailer. I will mail you back the sample code.

The virus detection and disinfection code is not available.

Author and Credits

John Norstad
Academic Technologies
Northwestern University
2129 North Campus Drive
Evanston, Illinois 60208 USA

j-norstad@nwu.edu

I enjoy getting mail, especially electronic mail, and I invite your correspondence. If you send me a letter through the regular mail, please include a self-addressed stamped envelope if you expect a reply.

Please do not try to call me. I do not have the time to do free consulting over the phone and I cannot return long distance phone calls from people I do not know.

If you think that you might have a new virus which Disinfectant does not detect, please read the section in this manual titled “Problem Clinic.” Follow the advice contained in that section before asking me for assistance.

With thanks to:

Mark H. Anbinder, Wade Blomgren, Chris Borton, Scott Boyd, Shawn Cokus, Zbigniew Fiedorowicz, Bob Hablutzel, Tim Krauskopf, Joel Levin, Robert Lentz, Bill Lipa, Albert Lunde, James Macak, Leedell Miller, Lance Nakata, Dave Platt, Leonard Rosenthol, Art Schumer, Dan Schwendener, Stephan Somogyi, David Spector, John Stein, Werner Uhrig, and Ephraim Vishniac.

This international group of Macintosh virus experts, programmers and enthusiasts helped design and test Disinfectant, edit the manual, locate copies of the viruses for testing, and analyze the viruses. I wrote all the code, but I could not have written the application without their help.

Disinfectant is an example of cooperative software development over the Internet. I send development and beta releases and technical design notes to the working group and they reply with error reports, suggestions, etc. This involves the exchange of many thousands of electronic mail messages. The result is an application which is much better than any one of us could have produced individually.

Since the initial release of Disinfectant, many hundreds of people have supplied error reports, comments, and suggestions for features. The application has in many ways become a community project. The author thanks everybody who has contributed.

Thanks also to Paul Mercer, Darin Adler, Paul Snively, Frédéric Miserey and Steve Capps for ShowINIT, and to François Grieu for his SafeStart code.

Last but not least, the author thanks his many good friends at Apple Computer for their advice, encouragement, and assistance, and for continuing to produce the very finest personal computers and system software.