UCRL-MA-121975

Department of Energy

C I A C

Computer Incident Advisory Capability

The Disinfectant Package

for Macintosh Computers

CIAC-2315 R.0

by William J. Orvis

February, 1996

Lawrence Livermore National Laboratory

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

Introduction..... 1
- **Overview..... 1**
- **What's in this manual?..... 1**
- **Availability..... 1**
  - CIAC Archive.....1
  - North-western University.....2

The Dinfectant Package 3
- **Overview..... 3**
  - Virus Scanner.....3
  - INIT 3

Using the Virus Scanner 4
- **Overview..... 4**
- **Virus Signature Scanners..... 4**
- **Scanning with Disinfectant..... 4**
- **Strategy for Scanning..... 5**
- **Setting Disinfectant's Options..... 6**
  - Beeping Option.....6
  - Scanning Station Options.....6
  - Saved Text File Options.....7
  - Background Notification Options.....7

Using INIT 8
- **Overview..... 8**
- **Installing the Disinfectant INIT..... 8**
- **Removing the Disinfectant INIT..... 8**

Example Showing How Disinfectant Detects a Virus..... 9
- **Overview..... 9**
- **Running an Infected Program..... 9**
- **Scanning an Infected Disk..... 9**

Conclusion..... 12

Appendix A. Other Ways to Protect a Macintosh..... 13

Appendix B. Potential Disinfection Problems..... 14

Appendix C. Joke Programs 15
- **Overview..... 15**
- **Removing a Joke Program..... 15**

Appendix D. Macintosh Virus Operation..... 16
- **Overview..... 16**
- **Attachment..... 16**
  - Startup Files.....16
  - Patched CODE 0.....17
  - Replacement of a Valid Resource.....17

Introduction

Overview

In this age of computer viruses, it is critical that Macintosh users know about viruses as well as how to protect their computer systems from being infected.

What's in this manual?

This manual describes the Disinfectant package which contains an anti-virus scanner and INIT (memory resident program) for the Macintosh computer.

In addition, this manual contains information about other ways to protect your Macintosh, potential disinfection problems, joke programs, and how viruses operate in a Macintosh system.

Availability

The Disinfectant package was written by John Norstad at Northwestern University and is maintained by him. Disinfectant is available to the public at no charge.

Disinfectant is available on the CIAC Archive, and on many network sites and BBSs. The primary distribution site is at Northwestern University.

CIAC Archive

The Disinfectant program is available in the CIAC Archive which is accessible via telephone-modem, FTP and WWW.

FTP:
ftp://ciac.llnl.gov/pub/ciac/sectools/mac

WWW:
http://ciac.llnl.gov

The BBS server is connected to the telephone system. To access it with a modem and a terminal, set up your system as 8-bit, no parity, and one stop-bit. The access numbers are:

(510) 423-4753 — 14.4K baud (V.32, V.42bis)
(510) 423-3331 — 9600 baud (V.32)
(510) 423-9885 — 19.2K baud ISDN within LLNL
or LBNL.

North-western University	Northwestern University is John Norstad's primary distribution site for Disinfectant. You can download the program using FTP from: ftp://ftp.acns.nwu.edu/pub/disinfectant

The Dinfectant Package

Overview

The Disinfectant package consists of a single program for scanning files for the presence of a virus. Contained within the program is an INIT (memory resident program) that watches over a system for any virus-like activity.

Virus Scanner

Contained within the Disinfectant package is a program that scans attached hard disks and floppies for known viruses. The scanner scans the files on any attached disk volumes for virus signatures, which are sequences of bytes that uniquely identify known viruses. If an infected file is found, you can delete or disinfect that file.

INIT

INIT is a memory-resident, suspicious-activity detector that watches over your operating system for any virus-like activity, such as attempts to change system files or add resources to existing programs. INIT also checks the Desktop file of all inserted disks for virus code hiding there.

Using the Virus Scanner

Overview

Disinfectant scans the files on the indicated hard disk for known virus signatures. Disinfectant can:

- scan files for virus signatures
- scan and disinfect infected files
- install the Disinfectant INIT

Virus Signature Scanners

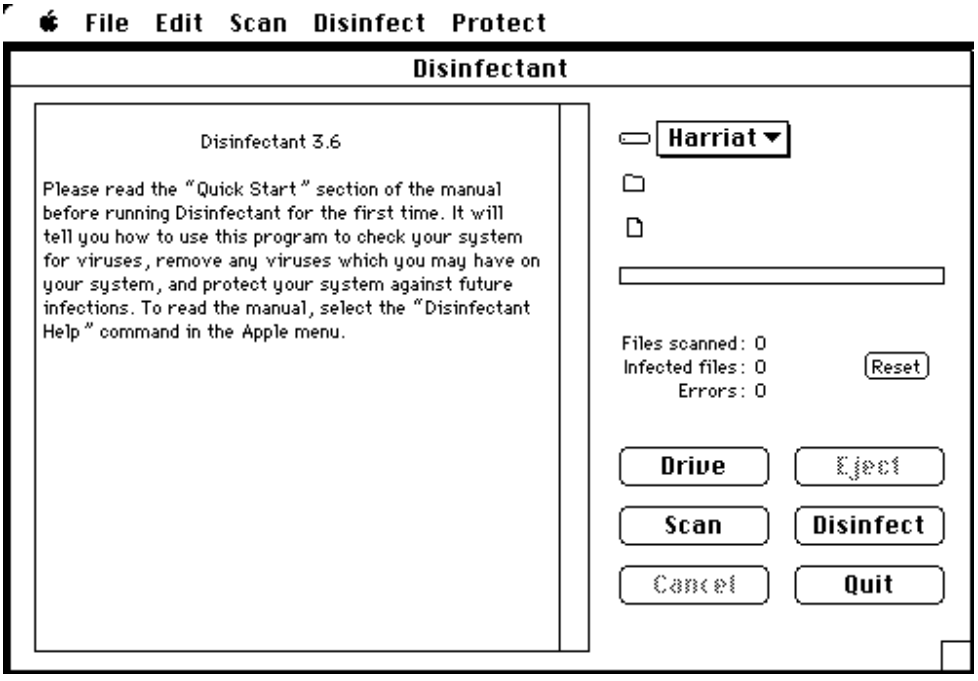
A signature scanner scans the hard disk for known virus signatures. Although other virus scanners get the signatures from an external file, the virus signatures for Disinfectant are built into the program itself.

Signatures on the Macintosh computer consist of resources with specific names or numbers, or unique sequences of code in a valid resource.

Scanning with Disinfectant

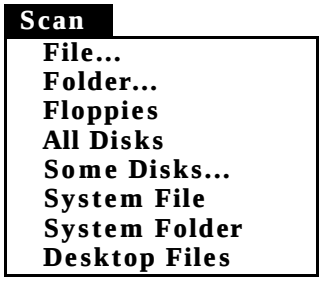
To scan a system with Disinfectant, perform the following steps:

1. Start the program by double clicking the Disinfectant icon. The following dialog box appears:



2. Select the disk to scan. At the top-right of the dialog box is the name of the currently selected disk (Harriat in this example). To select a different disk, click on the disk name and a drop-down list appears with the names of all the disks on the system.

3. Run the scanner. Click on the Scan button to scan the whole disk and locate any virus infections. To scan other than the whole disk, pull down the Scan menu and select one of the options shown below.



   If a virus is detected, it is listed in the large text window on the left side of the dialog box.

4. Disinfect a disk. If a virus is detected, press the Disinfect button to disinfect it. The disinfect button scans the disk again, but allows you to disinfect an infected file. The Disinfect menu has the same options as the Scan menu listed in step 3 above to allow you to selectively disinfect a disk.

Strategy for Scanning

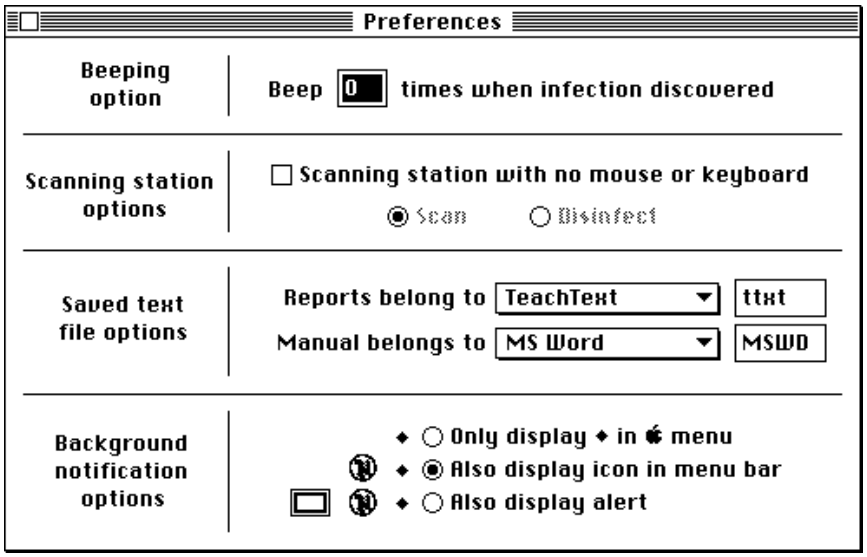
The Disinfectant package is generally setup to scan a whole disk, and while that is good to do occasionally, it can be time consuming considering the size of some of the newer disk drives. A better strategy is to scan the System folder on a regular basis and to only scan the whole disk when it is convenient, such as during lunch.

Setting Disinfectant's Options

Disinfectant has four options that can be set on the Options dialog box:

- beeping option
- scanning station options
- saved text options
- background notification options

Access the options dialog box by choosing the Options command on the File menu. The following dialog box appears.



Beeping Option

The beeping option sets how many times Disinfectant beeps when it detects a virus.

Scanning Station Options

The scanning station option allows you to set up Disinfectant in a stand-alone system with no mouse or keyboard for automated scanning or disinfecting floppy disks. Any floppy disk inserted into the machine is automatically scanned or disinfected, depending on how this option is set.

To use this option, create a special boot disk with Disinfectant as the startup program and the Scanning Station option selected. You can then boot a machine with this disk and no mouse or keyboard (to discourage other uses of the machine), and it will be available to scan any disk inserted into it.

Saved Text File Options	The Saved Text file options sets the file type for text files created by Disinfectant, including scanning and disinfection reports and a copy of the user manual.
Background Notification Options	Disinfectant can run in the background and scan a disk while you are doing other things. The background notification options determine what Disinfectant does if it discovers a virus or needs your attention in some way. The three options are to display: • a diamond in the apple menu, • an icon in the menu bar, or • an alert dialog box.

Using INIT

Overview

The disinfectant package includes a second program, the Disinfectant INIT. The Disinfectant INIT is a memory resident program that watches over a system for virus-like activity, and stops that activity if it is detected. The Disinfectant INIT watches for programs attempting to change the system file, adds new startup documents (INITs, CDEVs, etc.), and checks the Desktop file of inserted disks for attached virus resources.

Installing the Disinfectant INIT

Installing the Disinfectant INIT is a very simple process. Run the Disinfectant program and choose the Install Protection INIT command on the Protection menu. The INIT is installed in your system folder and is activated as soon as you reboot your computer.

Normally, the Disinfectant INIT is installed in the Extensions folder in your System folder. If you want to install it somewhere else, such as when creating special startup disks, use the Save Protection INIT command on the Protection menu and select the location from a standard file dialog box.

Removing the Disinfectant INIT

If you need to remove the Disinfectant INIT for any reason, open the Extensions folder in the System folder and drag the Disinfectant INIT out of the system folder into some other folder. Alternately, if you have the Extensions Manager (included with System 7.5), you can use it to remove the Disinfectant INIT. In both cases, you must reboot your computer to complete the removal.

Example Showing How Disinfectant Detects a Virus

Overview

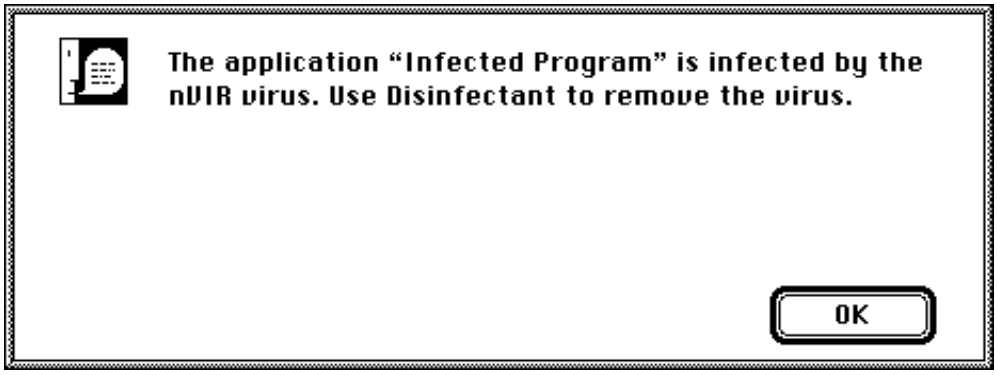
Using the nVIR virus as an example, this section demonstrates:

- what happens when a virus infects a computer
- what alerts are generated by the antivirus software while the infection is occurring

The nVIR virus attacks the system and application programs. It is spread by running an infected application which infects the system. The infected system then infects other applications.

Running an Infected Program

If you insert an infected disk and run an infected program, the Disinfectant INIT detects the infection, immediately stops the program and displays the following alert (note that the infected program is named "Infected Program" in this example.)



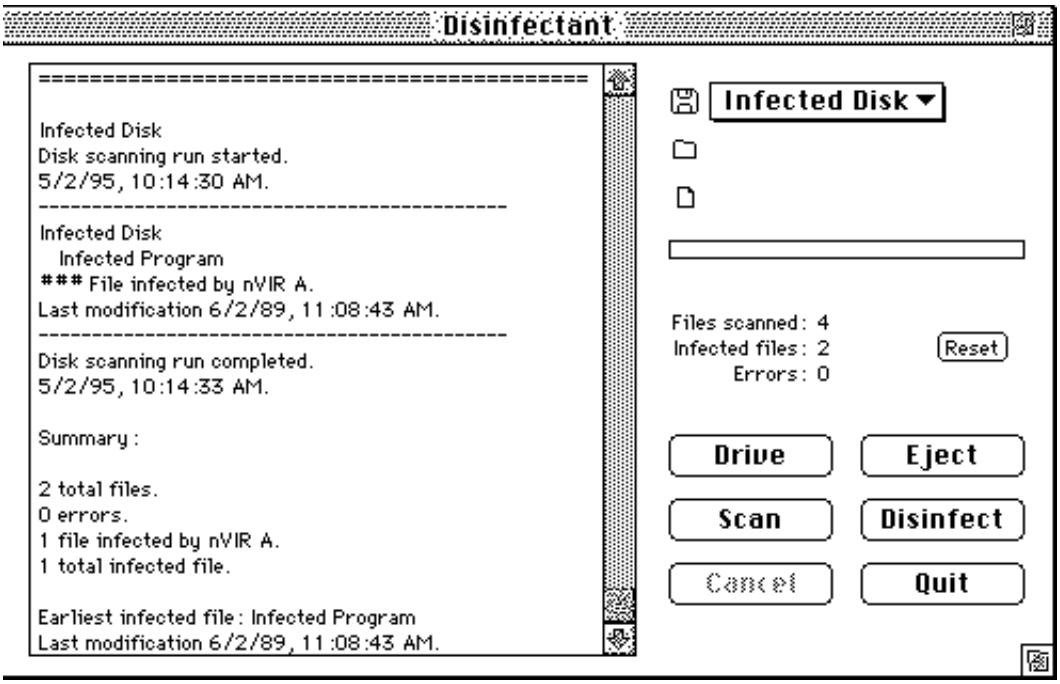
At this point, you have no option but to disinfect the program using the Disinfectant scanner. The Disinfectant INIT will not let the infected program run.

If the disinfectant INIT were not running, the nVIR virus would have infected the active system file. All you would notice is a slight hesitation while the program starts up. The next time the computer was booted, the virus would be active in memory and would infect other applications whenever you access them.

Scanning an Infected Disk

Scanning the infected disk with the Disinfectant program produces the following dialog box with the infection report in the window on the left of your screen. The report indicates the name of the infected file (Infected Program) and the name of the virus detected in it (nVIR). It also locates the earliest infection on the disk to help you determine when the disk was infected. Use this information to try and determine where the infection came from.

Example: How Disinfectant Detects a Virus, Continued



Looking at the contents of the report box for the scanning of the nVIR infected disk (left side of the window), note that the disk name is "Infected Disk" and the file name is "Infected Program".

Example: How Disinfectant Detects a Virus, Continued

To disinfect the disk, click on the Disinfect button. A report is produced, indicating whether Disinfectant was able to clean and repair the infected program. If Disinfectant cannot repair the program, you will have to delete the program and replace it with a fresh copy from the program master disks. Following is an example of a report generated while cleaning the nVIR infection.

```
Infected Disk
Disk disinfection run started.
5/2/95, 11:09:40 AM.
-----------------------------------------
Infected Disk
  Infected Program
### File infected by nVIR A.
Last modification 6/2/89, 11:08:43 AM.
File repaired.
-----------------------------------------
Disk disinfection run completed.
5/2/95, 11:09:46 AM.

Summary:

2 total files.
0 errors.
1 file infected by nVIR A.
1 total infected file.

Earliest infected file: Infected Program
Last modification 6/2/89, 11:08:43 AM.
```

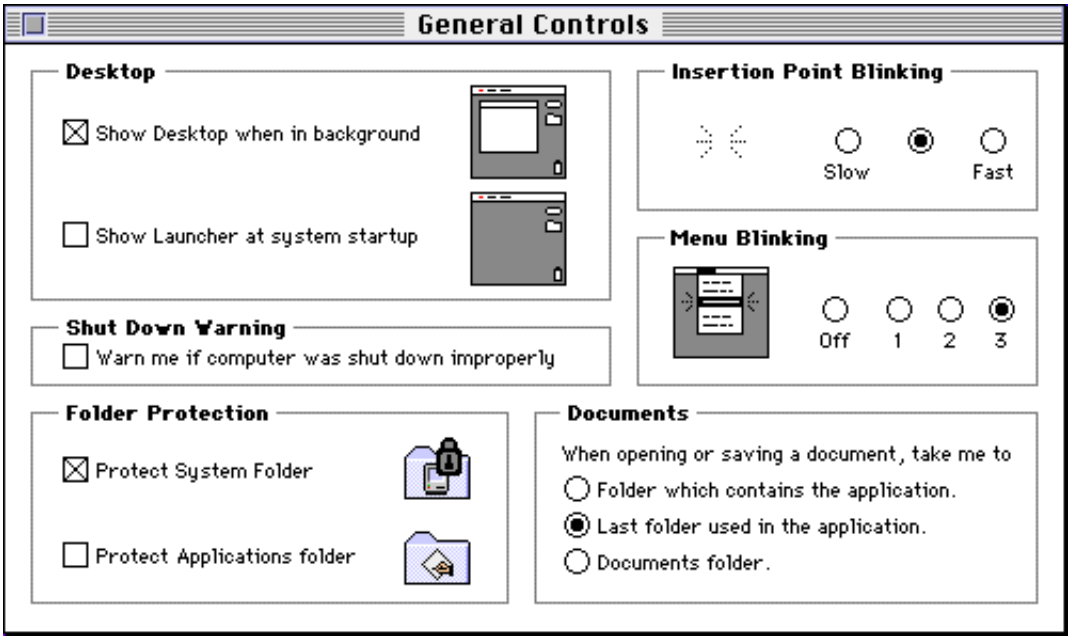
Be sure to warn any others who might have used their disks in your computer that they may also have a virus infection. You may want to contact any other organization that assists with viruses at your site such as your computer security organization.

Conclusion

The Disinfectant package is a useful, freeware package that detects viruses on the Macintosh. The package contains a virus scanner and a memory resident INIT program to watch for a virus infection. If used regularly, it will find or prevent most virus infections. As with any virus scanner, Disinfectant must be kept up to date by checking for and downloading new versions. Without regular updating, the scanner may not detect all viruses. Updates are available from the author or from the CIAC Archive.

Appendix A. Other Ways to Protect a Macintosh

Included in System 7 and later is a section of the General Controls control panel named Folder Protection shown below. Clicking on one or both of the check boxes turns on system protection of the indicated folders. Note that only the contents of the indicated folders are protected, and not the contents of other folders within the protected folders. This is a requirement for the System folder because numerous programs add or change files in the Preferences folder within the System folder.



Many older programs also save their preferences in the system folder. If you use any of these programs, you will not be able to use this protection method. If you use file sharing, both of these options are automatically turned off.

☞ **Warning: This option is not working well on all Macs. On one machine, it made the System folder disappear from the desktop and messed up the boot process. If this happens to you, boot from a floppy, open the System folder on the hard drive, click on the system file, and close the folder to get it blessed again (the folder has a picture of a Mac Plus on it,) reboot from the hard disk while holding down the shift key to turn off extensions, open the General Controls control panel, turn off the Folder Protection, and reboot the computer.**

Appendix B. Potential Disinfection Problems

If a data file you are using has been infected, the virus will be executed when you open the data file. Here's how it happens:

The system's resource manager looks first in the last file opened when it needs a resource for the running application. The application will get the virus-infected one instead of the correct one from the system file if:

- A virus is disguised as a commonly used, valid system resource such as a window definition (WDEF)
- That virus resource is attached to a data file opened by the currently running application
- The application requests that resource from the system

At this point, the virus code executes and takes control of your system.

Only a few viruses, such as WDEF and MDEF, take advantage of this capability. The WDEF virus appears to be a window definition resource. It is attached to the Desktop file that the system opens when you insert a floppy into a disk drive. The first time a window is created, the system gets the virus version of WDEF and runs it, letting the virus into memory.

☞ **System 7 and later is immune to the WDEF virus because of changes in the structure of the Desktop file.**

Appendix C. Joke Programs

Overview

Numerous "joke" programs exist for the Macintosh that fool people into believing they have a virus. Most of these joke programs produce virus-like behavior, but do not infect other programs. Joke programs must be installed on your system in order to run.

Joke programs can:

- Make the mouse pointer bounce.
- Make buttons jump away from the mouse.
- Make rude noises.
- Make your Mac talk to you.
- Make your Mac screen appear to be broken.
- Change the wording on standard dialog boxes.
- Make letters disappear or turn upside down.
- Make bugs or flies appear to be flying around inside your monitor.

Many of these programs are described in the book *The Macintosh Joker* (Linzmayer, Hayden, 1993) and are included with the book on a disk. Although joke programs are annoying, they are not damaging and are easily removed.

Removing a Joke Program

Rebooting your computer removes most joke programs, especially those that are simple application programs. If the joke is still running after a reboot, then it was probably installed as a startup file such as an INIT or a control panel.

Check for strange startup files in the system folder, the Extensions folder, the Control Panels folder, and the Startup folder. The Extensions Manager program is useful for locating these programs. If you cannot operate the computer because of the operation of a joke program, reboot your machine and hold down the shift key while booting to turn off all extensions (System 7 and later). At this point, the joke is out of memory and iyou can locate the joke file and remove it.

Appendix D. Macintosh Virus Operation

Overview

Macintosh virus operation is quite different from PC viruses. This is primarily due to the structure of the Macintosh operating system. An application file is not a single piece of code; it is a pile of resources. Each resource knows how to do something, and resources can be added or removed from a file by the system. For example, a WDEF resource is a window definition that contains the information needed to draw a window on the screen. Most application programs get the WDEF resource from the system file whenever they want to create a new window.

Attachment

Most Macintosh viruses invade a system by adding virus resources to a program file or to the system. Another way to add a virus is to create a startup file that the system runs at startup. The trick here is to add the virus code in such a way that it gets executed so the virus code can run and infect other applications. Macintosh viruses accomplish this in three ways:

- startup files
- patched CODE 0 resources
- replacement of valid resources

Startup Files

Startup files are special programs that are run during system startup to modify the operation of the system. They consist of INITs and control panels and reside in the System folder, the Extensions folder, and the Control Panels folder. At startup, the system searches these folders for startup files, loads any it finds, and executes them. Startup programs located elsewhere on the disk are not loaded.

A virus can invade a system by installing itself as a startup program. However, such programs are easy to spot and remove.

Patched CODE 0

Most of the executable code in a program is stored in CODE resources in the program file. The CODE #0 resource contains a map to all the procedures in the other CODE resources. A virus can attach itself to a program by attaching a virus CODE resource to an application and then modify the CODE #0 resource to send control of the program to the virus resource instead of to the normal starting place in the program.

When an infected program is run, the CODE 0 resource directs the execution point to the virus code, which then loads and executes. When the virus code has finished, it passes control back to the original starting point and the original application proceeds normally.

Replacement of a Valid Resource

When an application creates a standard object, such as a menu, it requests the resource that contains the information necessary to create the object. For a menu, it requests a MDEF menu definition resource. When searching for the resource, the systems resource manager looks in the last opened file first. Thus it looks in the data file, then the application file, then the Desktop file, then the Finder, then the System. The system was setup this way so applications could override the standard resources if they need to. A virus does the same by inserting a commonly used system resource in an application or data file. When that resource is requested by the application, the resource manager finds the virus version of the resource first and uses it instead of the identically named resource in the System file. At this point, the virus takes control, installs itself in memory and then passes the correct resource back to the application. But, the virus is now in memory and is free to spread itself to other files.

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

_____

_____

_____

_____

_____

_____

_____

List suggestions for improvement here.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Optional:

Name _____ Phone _____

The Disinfectant Package for Macintosh Computers, CIAC-2315, February, 1996

Stamp

Computer Incident Advisory Capability
Lawrence Livermore National Laboratory
P.O. Box 808, L-303
Livermore, CA 94551

Department of Energy

CIAC

Computer Incident Advisory Capabili

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551