Coping With the Macintosh nVIR Virus[1]

Technical Report CS88/30

by

Lawrence Brown,
Department of Computer Science,
University College, UNSW,
Australian Defence Force Academy,
Canberra ACT 2600.
Australia.

6/5/1999

Abstract

Computer viruses are causing increasing concern amongst the computer community, particularly among the users of microcomputers where the spread of such code happens with tremendous speed. Amongst Macintosh users there have been a number of reported viruses. One of the earliest, and best known families are the **nVIR** viruses. The original author is unknown, however the source for this virus was briefly published on Compuserve, and hence became widely known. A number of derivatives have appeared. This paper outlines one member of this family (probably the original member), and provides some suggestions for combating it.

[1] This is an abridged version of ADFA Computer Science Technical Report CS88/29 "Anatomy of a Macintosh nVIR Virus", which is available on request to selected parties.

1. Introduction

Computer viruses are causing increasing concern amongst the computer community. The concept of a virus was first propounded in Brunner's book "The Shockwave Rider" [Bru75]. A virus is a piece of code whose purpose is to examine other programs, and if they do not already contain the virus, to copy itself into them, and arrange for itself to run whenever such infected programs run[2]. Consequently, they can spread extremely rapidly, especially when programs are shared amongst a number of people, as is prevalent in the microcomputer community. A good description of viruses and other related security risks may be found in Witten [Wit87], or Denning [Den88].

Amongst Macintosh users there have been a number of reported viruses. One of the earliest and best known families are the **nVIR** viruses. The original author is unknown, however the source for this virus was briefly published on Compuserve by Matthias Urlich, and hence became widely known. This was reported in the electronic newsgroup "comp.risks" (DH Spector Jan 1988). A number of derivatives have appeared. Several articles on this virus subsequently appeared in the newsgroup "comp.sys.mac" (C Borton, M Urlichs Mar 1988). The more benign (and luckily also more aggressive) variants either beep, or if Macintalk is installed, say "Don't Panic". The more harmful variant randomly deletes a file. This paper analyses one member of this family, the one which simply beeps when the system is booted (sometimes - depending on the current date/time), and provides some suggestions for combating it.

2. Components of the nVIR Virus

The **nVIR** virus is so called because it stores its various components as resources[3] of type **nVIR**. These resources are summarized in Table 1.

Table 1 - nVIR Resources

ID	Size	Description
0	2_{16}	Counter, found in infected systems when counter reaches zero, this variant of the virus becomes inactive
1	$1AC_{16}$	Virus code
2	8_{16}	Original main routine jump table entry in infected application which has been replaced in CODE0 by a jump table entry to CODE256
3	$1A0_{16}$	Virus code
4	$1A6_{16}$	Virus code
5	8_{16}	Prototype jump table entry to call CODE256
6	42_{16}	Virus code
7	$83A_{16}$	Virus code
10	0_{16}	Flag resource, if present disables operation of the virus

The virus has two major modes of operation.

If present in an infected application, it will attempt to install itself in the system file under which it is running. The system file is first checked to see whether it has already been infected by an **nVIR** virus. If the system file is not infected, or has been infected by another member of the family, then this variant of the virus will copy itself

[2] If the program is already infected by a virus, the situation becomes more complex. If it is infected by another member of the same family of viruses, ie another **nVIR** virus, then this particular variant will replace the previous infection with a copy of itself. Other variants may simply assume that the program has already been infected and do nothing. If the program has been infected by another family of virus, it is most likely that they **both** will run in succession, possibly interfering with each other (depending on the assumptions made and how well the infection code is written).

[3] For a detailed description of resources and how the Macintosh file system is structured, consult **Inside Macintosh**, or your favourite book on programming the Macintosh.

into the system file (overwriting the previous infection if necessary). The application then continues running normally.

If the virus is present in the system file, at boot time it will patch the **TeInit** trap. Subsequently any application run under this system which calls this trap (just about all applications do), will be infected by the virus (replacing any previous infection by **nVIR** virus if necessary).

If resource **nVIR10** is present in the system file, it blocks the activation of the virus (although it is still present).

3. Removing the nVIR Virus

An **infected system** contains resources: INIT32, nVIR0, nVIR1, nVIR4, nVIR5, nVIR6, and nVIR7. If you boot from a known clean system, and use an uninfected copy of ResEdit and remove all of these resources, then the virus will be removed. However, any infected applications could reinfect the system (including ResEdit if it is run under the infected system at some time). This process must be done with care.

An **infected application** contains resources: CODE256, nVIR1, nVIR2, nVIR3, nVIR6, and nVIR7. Also the first jump table entry (at offset 16 in resource CODE0) has been replaced by a pointer to CODE256, and the original saved in nVIR2. If you boot from a known clean system, and use an uninfected copy of ResEdit, you can copy the 8 bytes from nVIR2 into the third line (offset 16) of CODE0, and then delete all the above resources to remove the virus. This process is not for the faint-hearted, as it is very easy to make a mistake and destroy the application.

Two utilities are available to automatically remove the **nVIR** virus. They are the **KillVirus INIT**, and the **Vaccination** application.

KillVirus INIT should be placed in the system folder of an infected system, and the mac rebooted. It will delete all the nVIR resources from the system file, and then add an (empty) resource **nVIR10**. This is a flag which disables all known versions of the nVIR virus. It will however trigger any of the virus search programs (such as Interferon) described later. It also installs a patch which checks every application run, and if any are infected, removes the nVIR virus. Once all traces of the infection have been removed, it is best to remove this INIT and replace the System with a clean version to avoid triggering any subsequent search programs, due to the presence of the nVIR10 resource.

Vaccination is an application which will remove an nVIR virus from an infected application. It should be run after booting from a clean system. Each infected application is selected in turn, and **Vaccination** will remove the infection.

The preferred technique for removing a virus is to replace the affected files with known clean copies (from locked distribution disks), as this is much safer than attempting to remove the virus from an infected file. However if this is not possible, then the above process should be followed. Make sure you have a backup of the infected file before using ResEdit. If the operation is successful, destroy the backup to prevent accidental reinfection.

4. Preventative Measures

There are two basic techniques used to combat the spread of viruses such as this one.

The first is to examine all files on your disks for telltale signs of a virus by searching for any resources of a particular unusual type (eg **nVIR**), for specific resources (eg **CODE256**), or for patterns of code (eg first jump table entry calls the highest numbered CODE resource). This may be done with programs such as: **Interferon**, **VirusDetectiveDA**, **RezSearch** or **VirusRX**. These programs will in general only detect known viruses, since they need to be told which resources or patterns of usage to look for. **Interferon** is probably the most powerful of these, since it can search for patterns of usage as well as resources of unusual types. It can however be misled (in particular it generates warnings about the Laserwriter and Laserprep files in System 6.0 when no actual problems exist). It also cannot easily be told to search for new resource types. **VirusDetectiveDA** is probably the easiest to use being a desk accessory, and hence is a good candidate for use on all new programs. It only searches for nominated resources though, not patterns of usage. It is easy to reconfigure to search for new resource types should new viruses be found.

Should an **nVIR** virus be detected, the methods outlined previously should be used to remove it.

The second method is to use **Vaccine** (a Control Panel device)[4] which patches your system to check for any attempt to

[4] Vaccine uses the new Control Panel, and hence may only be used on System 4.2 or greater.

write code into files. This is a fairly good defence (provided you do not actually need to legitimately write code out regularly, ie to be doing program development). Any such attempt will cause a dialog box to be displayed, and the user to be prompted as to whether the operation is permitted or not. Whilst the code in Vaccine can be circumvented, to do so is quite difficult, and no known virus has yet escaped detection by it. An earlier routine **VirusWARNING INIT** also installs patches which detect, but do not prevent, infection. Thus it is preferable to use Vaccine if possible.

All of these utilities have been placed in the public domain, and may be obtained from Macintosh User Groups, or your local Microcomputer consultant. The help information from each of these utilities has been included as appendices to this report.

5. Conclusion

Viruses are a pain! However there are some precautions which can be taken, with relatively little inconvenience to minimize the possibility of infection. This paper has outlined a how particular Macintosh virus propogates, and has provided some suggestions for combating it.

Acknowledgements

To the members of the Crypto group, to Dr. Andrzej Goscinski, to Alan Beswick, and to Willma Nelowkin, for their comments, suggestions and encouragement.

References

[Bru75] J. Brunner, *The Shockwave Rider*, Ballantine, 1975.

[Den88] P. J. Denning, "The Science of Computing - Computer Viruses," *American Scientist*, vol. 76, no. 3, pp. 236-238, May-June 1988.

[Wit87] I. H. Witten, "Computer (In)Security: Infiltrating Open Systems," *Abacus*, vol. 4, no. 4, pp. 7-25, Springer-Verlag, New York, SUMMER 1987.

Appendix[5] - Interferon 2.0

Interferon 2.0 Copyright © 1988 Robert Woodhead, Inc. - All Rights Reserved

Interferon is a program that detects and destroys digital viral infections. It currently recognises the modus operandi of several of the virus strains, and will be updated to recognise other strains as they appear.

If you have just received an updated version, please reread this document carefully.

How to use Interferon

Place the **Interferon** program on a new floppy diskette, along with fresh copies of the System folder and Finder. Use the latest System and Finder you have obtained from Apple or your dealer.

WRITE-PROTECT THIS DISKETTE!!!

Boot your computer from this diskette, and double-click on **Interferon** to start it running. A window will appear and a greeting will be displayed.

Select what volumes you wish to search by using the **Options** menu. You may **Search all volumes**, **Search selected volumes only**, or **Search internal floppy disk only**. If you select **Search selected volumes only** a new menu, **Volumes**, will appear. It will contain the names of all mounted volumes, all of which will be checked; simply select the ones you don't want to search. If you mount or unmount volumes, you can update the list in the **Volumes** menu by again selecting **Search selected volumes only**.

Next, select **Search for Infection** from the File menu. **Interferon** will scan all the volumes you selected and scrutinize all the files it can see. Each one will be carefully checked for signs of an infection.

Most of the time, nothing will be found. Messages will appear telling you which volumes were looked at and how many files were in the volumes, etc. If you don't get big nasty warning messages, you are OK.

If you get an INFECTION message, you have a virus. To remove the virus, you have to delete the files and replace them with fresh, uninfected copies. MAKE A BACKUP OF YOUR INFECTED DISKS BEFORE YOU START DELETING FILES! That way, you won't accidentally delete an important, uninfected file. Delete the infected files and replace them with fresh copies. Then run **Interferon** again to confirm you have cleaned up the infection.

Interferon can delete the files for you, by using the **Eradicate Infection** option. Only use it if you have made a full backup of your infected disks!!!! Note that this can render a disk unbootable if important operating system files get deleted.

Other Interferon Options

The **Do not report anomalies** option is checked when you enter the program. Anomalies are "quirks" that may identify new virus types, but may also be perfectly normal things that certain programs do. If you want, try running **Interferon** with this option disabled; you will probably get a lot of messages, especially about system files. I added this option as a diagnostic aid for people who are trying to identify a new viral strain; most users can just ignore it.

The **File** menu is completely operational. **Cut**, **Copy**, **Paste** and **Clear** work fairly normally. They all currently operate on the full report that is in the window (a List, for you techies). If you paste something in, it gets added to the end of the list.

If you want to make a printout of a report, Copy it into the clipboard and then paste it into a word-processor (my favorite is MockWrite) and print it.

Current report types generated by Interferon

001 The SCORES virus. So named because it puts, among other things, a file named SCORES in your system folder. This is the latest and most virulent strain known, as well as the most sophisticated. It replicates rapidly and can cause your machine to behave unpredictably. If any of your applications are infected by SCORES, assume that your SYSTEM FILE has been infected!

[5] this appendix has been adapted from the file "Interferon Instructions" which is distributed with the Interferon program.

002 The nVIR virus. This virus places nVIR resources all over. Simpler than SCORES, but just as much a pain.

003 VULT/ERIC. This is a Warning. The SCORES virus is looking for the string VULT or the string ERIC as a file creator or type. If you get this warning, please let me know the details.

004 A SNEAK virus. This is a virus that adds it's code to a common System folder file and changes it's type to INIT so that it is run at boot time. SCORES does this, although it does other things as well. Type 004 is a generic "Virus sniffer" that detects if common System folder files have been adulterated in this way. If you get a type 004 virus, please get in contact, you may have discovered a new strain.

005 This is an Anomaly. It detects when CODE resource #0 jumps to the last CODE resource (call it resource #N) and CODE resource N-1 does not exist. This is a pattern exhibited by SCORES. There may be legitimate applications out there that also have this pattern, thus this is flagged as an anomaly that you should look at further.

006 This is an Anomaly. It detects when CODE resource #0 jumps to the last CODE resource. It is not as selective as #005, and so more legitimate applications may have this pattern. You should examine any application that triggers this anomaly carefully.

007 This is an Anomaly. It is set off when a CODE resource appears in a non-application or system file. Many legal programs can do this, especially MPW tools.

008 This is an Anomaly. It is set off when an INIT resource appears in a non-INIT or system file. Again, this can be perfectly kosher and harmless.

009 Another Anomaly. Similar to 008, but looking for cdev's that are wandering far from home.

If you encounter a new viral strain that **Interferon** does not detect, please let me know as soon as possible so that I can add it to the list and modify the program.

Known Problems and Limitations

Interferon directly loads the resource map of files with a resource fork. If it runs into a file with a damaged resource map, it usually can detect this and will display an error message. If it does not, it will crash as it chokes on the bad data, usually with an ID=02 message. The guilty file is displayed at the bottom of the screen. Remove it and try again. I think I have this whipped -- let me know if you run into it.

Interferon cannot scan MFS (non-HFS) volumes. If you attempt to scan a MFS diskette Interferon will tell you that it cannot be scanned. My thanks to Raymond Lau for sending me the latest version of StuffIt on a MFS diskette -- you only caused me an hour of abject paranoia, Ray!

The Vision Fund

The Vision Fund is a charitable fund that gets all my "Shareware" donations. When it has enough money (about $3000) it will buy a special reading machine for a visually impaired Wizardry fan (Wizardry is my claim to fame) who needs it to be able to go to University. Any extra will help set him up with some decent computer hardware, and any left over from that will be given to some deserving charity.

The Vision Fund was set up a few years back to take in "Shareware" donations for my shareware products (currently 3: Reversi, MandelColor and Interferon). All the proceeds go towards buying some special hardware for a visually impaired computerist. He is going into college this year and we hope to get him something really decent. Anything left over will go to one or more major charities.

Interferon is FREE. Although it is a copyrighted program (and not public-domain!), you have my permission to reproduce and distribute it as much as you want. In fact, spread it far and wide - as far and wide as the plague it is intended to cure.

However, if **Interferon** helps you kill viruses on your computers, please consider how much time the program saved you (killing infections by hand takes hours!). How much was that time worth to you? $10? $50? $100? Only you can judge. However, please consider writing a cheque for some fraction of that amount (whatever you think fair) and send it to:

The address is:

The Vision Fund, c/o Robert Woodhead, Inc., 10 Spruce Lane, Ithaca, NY 14850.

Thankyou.

Interferon 2.0 - Version of 24 April 88 -

Appendix[6] - VirusDetective 1.1

VirusDetective is a DA to search through files looking for specific resources. Once found, the resource may be removed. NOTE: Not all viruses are stopped by removing a single resource.

Commands

Commands which may be given to **VirusDetective** are:

Start Check - Searches all files in the selected directory and all subdirectories
About/Help - The About/Help dialogs
Cancel - Cancels the search in progress
Continue - Continues search after an offending resource is found
Remove - Removes the found offending resource. Make sure you have a backup!

Specifying Resources to Search For

The resources **VirusDetective** searches for can be adjusted. This is done by adding search strings of the appropriate form to **VirusDetective**, using the Modifications option (under About/Help). The strings have the following syntax which must be followed EXACTLY:

TTTT Any - matches any resource of type TTTT
TTTT ID I - matches resource ID I of type TTTT
TTTT Name N - matches resource named N of type TTTT
TTTT Size S - matches resource of type TTTT and size = S
TTTT Range L H - matches resource of type TTTT and size >= L & <= H
TTTT Filetype - matches file with file type (Not included in virus file count)
CCCC Creator - matches file with creator CCCC (Not included in virus file count)

Examples:

nVIR Any
CODE Size 7026
INIT Name RR

Other Remarks

VirusDetective is a ShareWare program. If you like VirusDetective, send $10.00 (non-US users $15.00) to receive a user license.

Please send all funds in US currency with checks drawn on US banks.

Permission granted for non-commercial distribution.

Jeffrey S. Shulman, P.O. Box 521, Ridgefield, CT 06877-0521

[6] this appendix has been adapted from the internal help information provided by VirusDetective.

Appendix[7] - Vaccine 1.0

Vaccine 1.0 Copyright © 1988 CE Software by Donald Brown.

Vaccine is designed to provide you PARTIAL protection against worms and viruses. There will be viruses that **Vaccine** cannot stop. (See later screens for more information)

This is a FREE program from CE Software. You may distribute it freely, post it on bulletin boards, etc. The only limitations are that no fee (other than normal duplication fees) can be charged and that Vaccine must be distributed unchanged.

Please note that we CANNOT be responsible for others modifying our program. To be sure you've got a true copy, CompuServe, GEnie, Delphi, and MacNet will always have a clean version uploaded. BMUG, BCS, and The Rest of Us will also have a clean copy in their libraries. Finally, for ten dollars, we can provide you with a disk that contains Vaccine and our other no-charge programs.

Since this is a free program, CE Software CANNOT offer any support. Bug reports should be submitted by letter only. (Sorry, but we've got bills to pay!)

Using Vaccine

Vaccine is a Control Panel device (CDEV). To alter it's options, and to read the internal help information, you should open the **Control Panel** (from the Apple menu), and click on the Vaccine icon on the left-hand side. The available options are presented as check boxes to be selected or not.

Turn protection on

When checked, **Vaccine** is enabled as of the next time this System is booted. When enabled, **Vaccine** warns you whenever certain significant resources are being modified. You can grant permission for the change to take place (if you're running an installer program for example), but you're in control.

When installing many utilities, you may want to temporarily turn Vaccine off. To do so, uncheck the "Turn protection on" button and restart your Mac. Don't forget to turn the protection back on when you're finished!

Vaccine normally warns you when changes are being attempted by putting up a window, telling you what's being changed. It'll be up to you to determine whether or not the change is successful. If you're running a program that should be making these changes (installing some utility), click on the Granted button. If there's no reason that changes should be made and it appears that something's happening behind your back, click "Denied".

Expert display

You can request an expert mode, that will be faster and harder for a clever virus to fool. The expert mode uses some very small icons in the upper right corner of your screen instead of the larger window. If you wish to view the normal window, click on the question mark. If you want to immediately grant permission to make the change, click on the very small "Add" button. If you want to immediately stop the change, click on the very small "No" button. To use the expert mode, click the appropriate checkbox and restart your machine.

Always compile MPW INITs

MPW is a popular package for people developing new programs. The current MPW linker has an odd effect on vaccine. It sets off Vaccine's warning flags, but does so in a state where Vaccine cannot display its dialogs. **Vaccine** recognizes this condition, and so waits, silently, for you to press either "Y" (to grant permission) or "N" (to deny permission). If your machine appears to hang, try pressing "Y" (if you're linking a file in MPW) or "N". You can tell Vaccine to automatically assume "Y" when it encounters this condition by checking off the MPW checkbox and restarting your machine. THIS LEAVES YOU VULNERABLE TO ANY INIT THAT MIMICS THIS CONDITION!

Show Icon

When Vaccine boots, it draws its icon on the screen, so you know that you're protected. Some people find this distracting. Also, a few rare utilities may conflict with the icon-drawing routine and may crash. If you don't want the icon display, uncheck the "Show Icon" checkbox

[7] this appendix has been adapted from the internal help information provided by Vaccine.

Further Hints

Vaccine can only provide partial protection against viruses. It stops simple viruses, but can be overcome. The most important steps are up to you:

- Back up your hard disk or floppies regularly. Keep more than just the most recent backup.
- Whenever you get a new program, write-protect the diskette and make a copy. Never insert a master into a drive when it is not write-protected. If you ever need to rebuild your hard disk, you'll want to be sure you have unaffected programs.
- NEVER use your original master diskettes, even for a moment.
- Run new public domain/shareware/freeware software on a floppy until you know it's safe.
- DON'T PANIC

There are very few viruses actually out there. These steps are useful because they protect you against bugs and hardware failures as well as malicious programs. But don't lose any sleep over it.

Some people may invent a virus that defeats **Vaccine**. Big deal. It does not take a genius of a programmer to do so. It will not get you acclaim, it will not prove you're better than anyone else. If you want a challenge, write a better tool. Not only will you get more fame, you can also make money with it.

I do not intend to write further versions of **Vaccine**. People expressed concern about a continuing spiral of ever-nastier viruses being fought by ever-nastier defences. I will not fuel this spiral.

Some people still fail to see the harm in spreading viruses. I think they're wrong. The whole thrust of the personal computer has been bringing control of the computer to the user. Viruses steal that control away and replace it with fear, uncertainty, and doubt. Why would we want to take such a gigantic step backward?