Microware Review

Macintosh Computer Viruses: Descriptions and Eradication Methods

Sheila ffolliott

Computer viruses and trojan horse programs are computer programs that spread from computer to computer, sometimes (but not always) causing damage to data. Since the people who spread them are usually unaware that they are doing so, computer viruses pose a threat to those who use computers. This article concentrates on detection and prevention of viruses on Macintosh and IBM PC and compatible machines.

DEFINITIONS

A *trojan horse* advertises itself as a useful or interesting program in an attempt to get someone to run it. When it is run, it usually performs the useful action and then performs an undesirable one. The only way to get a trojan horse on your disk is to put it there yourself (although another person could put it on when you are not watching). The best way to avoid damage caused by a trojan horse is to be wary of unknown software and run it on a test system first.

A *virus* is a program that inserts itself into a legitimate program or the computer's operating system. Once there, it waits until someone runs another, uninfected program and then inserts itself into that program. Usually the owner of the infected program is not aware that a virus is in the program; viruses spread without warning. Some viruses are destructive and may wipe out all the information on a computer's disks, delete selected files on hard or floppy disks, or write wrong information to files. Some viruses are intended to be cute rather than harmful, but can cause programs to crash or malfunction because the author did not anticipate all possible interactions between the virus and other programs.

Viruses are spread when one person gives another person an already infected program, and the infected program is run on the first person's computer. It is possible to get certain viruses by simply inserting an infected disk in the floppy disk drive and looking at the contents. You cannot get a virus

CJEC.VOL. 18, NO 3, PAGES 229-236, ISSN 0710-4340

if you do not use other people's disks in your computer, and do not download programs from microcomputer bulletin boards.

A *worm* is a program that spreads from computer to computer, as does a virus, but it does not insert itself into another program. It hides itself in other ways. Worms can spread through the sharing of disks, and also through a computer network. The Internet program that made headlines around Christmas time, 1988, was a worm (but was often mistakenly called a virus). Microcomputer worms are rare, thus they will not be mentioned further in this article.

Atime bomb is a virus, trojan horse, or worm that waits for a certain time, a certain day (Friday the 13th, for example), or for a certain length of time before performing its action. In other words, you may have a time bomb on your disk for some time before it damages your data.

Note: With one important exception, data files cannot be infected with a virus (see the Init 29 information in the Macintosh Virus section). Only applications can become infected.

Virus "vaccines" are available, both in the public domain and commercially, that attempt to warn the user that infection is about to occur or that it has already occurred. Public domain Macintosh vaccines include Vaccine, Interferon, VirusDetective, KillVirus, Ferret, Disinfectant, GateKeeper, and Virus Rx (Disinfectant, Vaccine, GateKeeper and Virus Detective are the best ones).

When using a vaccine, take care to ensure that the vaccine program itself does not become infected. Get the vaccine program from a source that is known to be virus-free, and copy it onto a floppy with a copy of the original system disk for your computer. Once the vaccine is on the floppy disk, the disk must be write-protected. Never start a machine that is suspected of having a virus on its disk with a floppy disk that is not write-protected.

Some vaccine programs have options that will remove a virus from an infected program. Removal of a virus from a program using a vaccine is not guaranteed to work; part of the virus may remain to reinfect your Macintosh, or your application may be damaged by the attempt to remove the virus. It is safer to remove the program and reinstall it from the original program disk.

Vaccine programs are not foolproof, so other precautions should be taken.

Signs of a Virus Attack

- The size or creation date of a program has changed from the original (some programs alter themselves, so this is not conclusive).

- Unknown files that appear on your system without your knowledge (but some programs create temporary files that may not get deleted. If your computer crashes while you are running a program and you discover strange files on your disk, the files are probably left over from the crash).

- Deleted or damaged files; but there are many causes for damaged files, and most of them have nothing to do with viruses.

- Unusual slowness of a program, either in operation or in starting.

- Sudden problems with printing or other operation of a program.

- Large amounts of disk space suddenly vanishing.

Precautions Against Virus Attack

For personal use, and use with microcomputer networks:

- Write-protect all original program disks and make a copy before installing the programs onto a hard disk; put the originals in a safe place.

- Check all new disks with a virus detection program before using their programs.

- Never use the original program; use a copy instead.

- When possible, do not use any floppy disks that contain programs or the operating system unless they are write-protected; the action of placing a disk in a drive and looking at it can be enough to infect it (a virus cannot attack a floppy that is write-protected).

- System files and programs should be marked as read-only whenever possible, so a virus cannot write to them (but some viruses are smart enough to get around this).

- Public domain software should be obtained only from reliable sources, such as the original author or a commercial bulletin board service (GEnie, CompuServe).

- Commercial software must be obtained only from a software vendor (in addition to being illegal, pirated software is more likely to have a virus).

- Before using any new or suspicious software, run it several times on a test computer and check to make sure that programs and system files have not been altered or deleted.

- Check the size and creation date of programs and system files against the originals, and reinstall the original software if any unexplained change has occurred (but some programs write information into themselves, such as WordPerfect 4.2).

- Consider using a checksum program, which looks at a file, performs a calculation based on its size and contents, and produces a checksum number; if a virus infects a file, the checksum will usually change. Run the checksum periodically and check the results.

- Know your system; note any unknown files and determine their origin, and be suspicious of any unusual changes in how your software works (slower speed, unexplained disk activity).

- Back up all important data files on a regular basis (this is a good idea anyway).

VIRUS ERADICATION

The first thing to remember if you think that you have been infected with a computer virus is DON'T PANIC. Most of the time, damage caused by what you think is a virus is really caused by something else - error on your part, or error on your program's part (bugs in your software). If you do suspect a virus and you don't have very much computer experience, find someone who does and have them look at your computer.

To get rid of *a* virus, follow these steps:

a) boot the computer with an original, write-protected system disk;
b) backup any important data (NOT APPLICATIONS) if you have not already done so;
c) delete all infected applications. For best results, erase the entire disk;
d) restore your backed up data from write-protected backup disks (or tape);
e) restore the applications from original, write-protected disks;
f) check the disk with a virus detector to make sure that the virus is gone; and
g) repeat for all infected floppy and hard disks.

If you regularly back up your data, congratulations; you are a singular person. However, if you are using your backup to restore your data after a virus attack, remember that you may have had this virus for some time and your backup may contain infected programs. Do not restore programs from your backup, or you may become reinfected. Only restore the data from your backup, and use the original program disks to reinstall programs.

KNOWN MACINTOSH VIRUSES

There are several widespread viruses for the Macintosh, which have different symptoms and cures. None of the known viruses were written to delete data, although they may cause your programs to crash or printing to fail. For more information about Macintosh viruses, read the article entitled "Mad Macs" in the November 1988 issue *of MacWorld.*

nVIR. So called because it inserts a resource called nVIR into applications and into the system file. There are at least two different variants of nVIR with the same name. It can be detected by using a virus detection program or by using ResEdit to check if the nVIR resource exists in a program. An infected program will occasionally beep when you start it up, for no apparent reason; if you have MacinTalk installed on your Macintosh, it will say "Don't Panic" instead of beeping. Programs infected with nVIR often have printing problems. One version of nVIR installs itself over and over again into a program, causing it to grow to an enormous size.

hPAT. This is a variation of nVIR, with similar symptoms.

Scores. Scores creates two invisible files inside the System folder, one called "Scores" and one called "Desktop" (not the real Desktop file, which is not in the System folder). These files can be seen if you use a utility program such as DeskZap. As well, the icons for the notepad and the Clipboard files change from being a tiny Mac to being a text-only file icon. An infected application contains an extra CODE resource of size 7026, numbered two higher than the previous highest numbered CODE resource. This program is targeted against programs with resources named VULT or ERIC, which are programs written and used by a defense company in the United States.

Init 29. This is the only virus discovered to date that will infect data files. In fact, Init 29 will infect just about any type of Macintosh file, such as programs, printer drivers, data files, font files, and the System. It also infects the Desktop file, an invisible file that resides on every Macintosh floppy or hard disk. If an infected program is copied to a disk, the disk's Desktop file becomes infected. If a disk is inserted into an infected machine, it becomes infected unless it is read-only. If the virus tries to infect a write-protected disk, it will fail, and the Macintosh will display the "Disk needs minor repairs" error message. The virus detection program "VirusDetective," version 2.0 and higher, will detect this virus.

MACINTOSH VACCINE PROGRAMS

Each virus protection program works in a slightly different way. Here are brief descriptions of each of the programs mentioned above, to aid you in choosing a virus protection program for your computer. The programs are listed in order of most to least desirable. The virus protection programs are divided into virus prevention - taking place, and virus detection - programs that detect viruses after they have infected your computer.

VIRUS PREVENTION PROGRAMS

Vaccine 1.0. Vaccine is an INIT file. When placed into the System folder, it installs itself into the memory of the Macintosh when the machine is rebooted. Once installed, Vaccine monitors the activity of other programs and warns you if a program is about to insert code into another program. If this happens, Vaccine will put up a dialogue box asking if the insertion is to be allowed. The appearance of this dialogue box does not necessarily mean that you have a virus on your machine; compilers and programs that create FKEYS will trigger Vaccine. If you are running a program that is not supposed to alter your applications or your system files, answer "no" when Vaccine asks if it is all right to let an insertion take place, stop what you are doing and check your computer for viruses.

Occasionally, a program will hang (stop) as you are starting it if you have Vaccine installed. This may be caused by a virus; certain viruses will disable the ability of Vaccine to put up a dialogue box, but Vaccine is still waiting for a yes or a no. If a program that you have used before hangs when you are just starting it, and you have not made any changes to your system since you last used the program, you may have a virus. Press the 'n' key; if the program continues, you have been attacked by a virus. Even if the program does not restart, check your computer for a virus. Programs may hang even if a virus is not present, particularly if you have recently installed a new INIT or CDEV.

GateKeeper. GateKeeper is similar in operation to Vaccine, but can be told not to flag the actions of compilers and FKEY programs as dangerous. If you are a programmer, you will probably want to use GateKeeper rather than Vaccine.

KillVirus. KillVirus is an INIT that 'inoculates' your System file against the nVIR virus. To use it, place it into your system folder. The next time you start your Macintosh, KillVirus will insert a fake nVIR virus into your System file; when the real virus sees the fake virus, it thinks that the System is already infected and will not reinfect it. KillVirus will also detect attacks by the real nVIR virus on your System, and will delete the virus from infected programs automatically.

Note: The KillVirus program will be flagged as infected with the nVIR virus by Interferon, but it is not infected. After you use KillVirus, Interferon will flag the system file as infected as well, but the fake nVIR is harmless and will not spread.

VIRUS DETECTION

Disinfectant. Disinfectant checks every file on a disk for the presence of known viruses. If it finds as infected file, it displays a message and gives you the option to remove the virus from the program.

Interferon 3.1. Interferon checks every file on a disk for the presence of Scores and nVIR, as well as "anomalies" - conditions that may signal a virus, but usually do not. If Interferon finds an infected program, it displays a warning message. Interferon will also eradicate a virus, which means that it will delete the infected program, so use this option with caution.

Note: Some files created by the LightSpeed C compiler are flagged by Interferon as having an anomaly, but this is normal; the files are not infected by a virus. Version 5.0 of the LaserPrep and LaserWriter files from Apple also cause Interferon to flag an anomaly, but they are not infected with a virus. Other versions of the LaserWriter and LaserPrep files do not have this anomaly.

Ferret 1.1. This application checks a disk for the presence of the Scores virus. It will flag any infected programs, and will remove the virus from infected programs.

VirusDetective 1.2. VirusDelective is a DA and must be installed into your System file using the Font/DA Mover program. It will check your disk for the presence of nVIR and Scores. It is possible to get VirusDetective to check for other unknown viruses, as it allows you to check files for resources of your choice. VirusDetective will also attempt to remove viruses from infected programs.

Virus RX1.0A2. Virus RX prints out the names of all INITs and CDEVs on your disk, as well as suspicious resources in your System files. Once the list is compiled, you must check to see that you know what each file is; unknown files may be part of a virus. If Virus RX itself is infected by the Scores virus, it will change its name to "Throw me in the trash"; throw it away immediately and check the rest of your disk for Scores with another virus detection program.

Note: Virus RX does not signal the presence of the nVIR virus, so a different program must be used to check for that virus.

Agar 1.0. Agar is not a virus detection program per se. It is a small dummy application that does nothing but wait to be infected. It is very small (361 bytes), thus it is easy to see if Agar has been infected by a virus. To use it, copy it onto each disk that contains applications or a System folder and check it periodically to see if it has been altered.

CRC 1.0. This small program will calculate a CRC (cyclical redundancy check) for your application programs. A CRC is a number produced by performing a calculation using the bytes of an application; an example of a simple CRC would be to take the length of a program and divide the result by 23. If the program changes in any way, the CRC will probably change (but it may not), thus signalling infection. Since the program CRC must be run once on each of your application programs, and the resulting number written down, it is awkward to use unless you have few programs to check.

AUTHOR

Sheila ffolliott is with the Department of Computing Services, University of Saskatchewan, Saskatoon, Saskatchewan, S7N OWO.