Tech Info Library

Computer Viruses (part 3 of 4)

Revised: 5/17/89
Security: Everyone

Computer "Viruses" (part 3 of 4)

==========

This article last reviewed: 15 April 1988

KNOWN VIRUSES

The Scores Virus

You can be almost positive your system has been infected by the Scores virus if the icons of your Note Pad file and Scrapbook file look like document icons instead of system icons. Launch ResEdit and look in your System folder. If you see files called "Desktop" and "Scores" you can be 99% sure that you have the Scores virus.

How Scores Spreads and What It Does

The Scores virus is relatively harmless. The initial infection is caused by an application with a modified CODE ID = 0 resource, and an additional CODE resource (first unused ID number plus 1). When the 'carrier' application is launched, the CODE ID = 0 resource runs the virus installer code. This code checks for previous installation of the Scores virus. If the virus is not there, the virus files are installed. The virus consists of three INITs, one atpl, and one DATA resource found in the files listed below:

FILE	TYPE	CREATOR	RESOURCES		SIZE
Desktop (invisible)	INIT	FNDR	atpl	ID = 128	2410 bytes
			DATA	ID = -4001	7026 bytes
			INIT	ID = 10	1020 bytes
Note Pad File	INIT	ZSYS	INIT	ID = 6	772 bytes
Scores (invisible)	RDEV	ZSYS	atpl	ID = 128	2410 bytes
			DATA	ID = -4001	7026 bytes
			INIT	ID = 10	1020 bytes

```
Scrapbook File       RDEV    ZSYS       INIT  ID = 6       772 bytes
                                               ID = 17      480 bytes

System File          ZSYS    MACS       atpl  ID = 128    2410 bytes
                                        DATA  ID = -4001  7026 bytes
                                        INIT  ID = 6       772 bytes
                                        INIT  ID = 10     1020 bytes
                                        INIT  ID = 17      480 bytes
-------------------------------------------------------------------
```

If the Note Pad and Scrapbook files do not exist, they are created. If they exist, the type and creator of the files are altered to those listed above, and the corresponding resources are added to the files. The files still appear to function normally with the Note Pad and Scrapbook DAs, but their icons change to document icons. The Desktop and Scores files are invisible, and are created during the infection process.

The next time the infected system is rebooted, the INITs are loaded into memory and are ready to infect other applications. The INITs install a VBL task that actually modifies and installs resources into an application. After an application has been launched, an internal timer is started. Somewhere between two and three minutes later, the open application is infected and becomes a carrier. A new CODE resource is added to the infected application, and the application's CODE ID = 0 resource is modified to execute the new CODE resource first, then continues with the application.

To determine if an application is infected, examine the CODE ID = 0 resource. If the eleventh word of the resource (third word on the third line in the ResEdit listing) is NOT "0001", the application is suspect. If the third word is something other than "0001", convert the value to its decimal equivalent (the numbers are in hexadecimal). Then determine the resource number of the CODE resource at the top of the ResEdit resource list. If these numbers are the same, the application is probably infected, and should be replaced. Some applications will appear to be infected even though they are not. If the eleventh word of CODE ID = 0 is not 1, check the tenth word; if it is '4EED' the application is most likely not infected.

How to Get Rid of the Scores Virus

It is not hard to remove this virus from a system, but it may take some time. Here's how:

1. Use Font/DA Mover to copy all fonts and DAs that you do not have backups of to font and DA suitcase files (this virus does not attach itself to DAs).

2. Start the system from a locked, not infected, floppy disk.

3. Throw away the System folder on the infected disk.

4. Use ResEdit to identify all suspect applications on the infected disk.

5. Make a list of all suspect applications.

6. Throw all suspect applications in the trash, and empty the trash.

7. Reinstall the system software from a known good System Tools installer disk.

8. Using locked masters, recopy any applications that were deleted from the infected disk (it is important to verify that the master disks have not been infected).

9. You're all done.

The nVIR Virus

How the nVIR Virus Spreads and What It Does

The nVIR virus is similar to the Scores virus in many ways. It does not appear to have malicious intent and is relatively harmless. Initial infection of a system is also caused by an application with a modified CODE ID = 0 resource. When a nVir carrier application is launched, the virus' code segment is executed first. This code checks for its INIT in the System File, and if it doesn't find it, the code copies the INIT there. Along with the INIT resource, eight 'nVIR' resources (0-7) are added to the System file.

The next time the system is restarted, the INIT ID = 32 is loaded into memory and tries to infect every application that is launched. The nVir virus adds a CODE ID = 256 resource and modifies the CODE ID = 0 so that the nVir code is executed first.

Again, infection of an application is determined by examination of the CODE ID = 0 resource. If the eleventh word of the resource (third word on the third line in the ResEdit listing) is NOT "0001", the application is suspect. If the third word is something other than "0001", convert the value to its decimal equivalent (the numbers are in hexadecimal). Then determine the resource number of the CODE resource at the top of the ResEdit resource list. If these numbers are the same, the application is probably infected, and should be replaced. Some applications will appear to be infected even though they are not. If the eleventh word of CODE ID = 0 is not 1, check the tenth word; if it is '4EED' the application is most likely not infected. The tenth word normally contains '3F3C'.

When launching an infected application, there is a one in sixteen chance that you will hear a short system beep. We have been told that if MacinTalk is installed you will hear the words "don't panic".

How to Get Rid of the nVIR Virus

Remove the nVIR virus the same way you remove the Scores virus except you do not need to throw away all of the files in the System Folder; just throw away the System file.

The MacMag Virus

We don't have much information regarding the MacMag virus. It was apparently uploaded to CompuServe, inside a HyperCard stack, in the form of an XCMD, and it installed an INIT ID = 6 with a name of 'RR'. Its sole purpose in life was to display a "universal message of peace" on your computer on March 2, 1988. The virus removed itself after displaying this message and should be of little concern now.

Tech Info Library Article Number:2823