Interferon 3.1 - 16-May-1988

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 gotten 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 as you would expect. Cut and Copy operate on the selected lines, Paste appends the clipboard to the report, Clear clears it. As an added convenience, **Copy All** copies the entire report to the clipboard.

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.

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.

I only ask that if Interferon helps you zap some viruses, you consider how much time it saved you, determine what that time was worth, and send in a cheque for some fraction of that amount.

The address is:

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

Thankyou very much.

Other Programs I reccomend that you get to fight Viruses

Vaccine is a "cdev" by Donald Brown that sits around watching for attempts by viruses to modify files. If it sees such an attempt, it lets you know!

Vaccine is very complimentary to Interferon. Interferon tells you if a file is infected, Vaccine tells you when a file gets infected.

Ferret is a program that only looks for the Scores virus, but it has the ability to repair infected programs. I don't know how well it works, but it may save you the hassle of deleting and recopying infected applications.

Both these programs are available on Compuserve and other services, as well as many local bulletin boards.

Spreading Inteferon around

PLEASE upload Interferon to your local bulletin boards, give it to friends, and distribute it at user groups. As new versions become available, they will be uploaded to Compuserve APPDEV DL0 in file INTERF.SIT.

Current report types generated by Interferon

Viruses

001 The SCORES **virus**. So named because it puts, amoung 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!**

002 The nVIR **virus**. This virus places nVIR resources in your System file and CODE resources in your applications. Simpler than SCORES, but just as much a pain.

003 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. Type 003 is a generic "Virus sniffer" that detects if common System folder files have been adulterated in this way. If you get a type 003 virus, please get in contact, you may have discovered a new strain.

Warnings

Interferon reports a warning when it finds a file that it knows a particular Virus is looking for. Nothing to worry about, but if you get one, we would like to know.

101 VULT/ERIC. This is a **Warning**. The SCORES virus is be 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.

Anomalies

Anomalies are unusual things that are legal for applications to do, but not commonplace. However, when a virus infects a program, it may trigger one of these anomalies. Because perfectly healthy applications can trigger anomalies, you should only turn anomaly reporting on if you suspect you have a new type of infection and you can use tools like Resedit to track it down.

If you suspect an infection and you are not a "power-user", go get help!

201 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.

202 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.

203 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.

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

205 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.

Version Notes

1.0 07-April-88. First release. Detects type 0001-0004 strains.

1.1 10-April-88. Second release. Many bug fixes, including more robust checking for damaged resource forks and less chance of stack-heap collision. Fixed error in type 0001 virus detection caused due to mistake in filename "Desktop ". Added ability to scan boot volume or internal floppy only. Added diagnostic on # of files searched.

1.1b 11-April-88. Corrects a stupid typo in my code that made checking of the resources unreliable. WARNING: previous versions might not detect some viruses - don't use them!

1.2 14-April-88. Changed the report so that you see the full pathname of files, one element (volume, file or folder) per level. Also, made a correction to the SCORES "sniffer" so that it detects when SCORES has infected the System file (A typo prevented it from detecting the virus correctly).

Interferon now attempts to unmount and eject all volumes that it searches, except the boot volume. It will succeed when it tries to eject a floppy diskette, which saves you a step and avoids a conflict with Multifinder. If you are running Multifinder with multiple hard disks, you will see the non-boot volume hard disks disappear from the desktop. Multifinder will remount them as soon as it gets some time, usually at the end of an Interferon scan.

1.3 20-April-88. Made some improvements to the type 002 VULT check. Type 004 checks are now better as well. Type 006 anomalies no longer trigger on Fullwrite. Added type 007-009 anomalies. Fixed a few minor bugs that were causing strangenesses on small memory machines.

2.0 24-April-88. Made many user interface improvements. Cut, Copy, Paste & Clear now supported. Allows user to pick which volumes get searched.

2.01 28-April-88. No longer incorrectly reports version 5.1 LaserWriter and LaserPrep files as infected. Apple changed the creator of this files in their latest upgrade in order to change the Icon (sneaky, sneaky...)

2.10 05-May-88. Fixed "false alarm" problem with Type 004 checker.

3.0 13-May-88. The Friday the 13th special. This version improves checking for type 002 "nVIR" viruses so that it catches infected applications as well as infected system files. Thanks to Apple for information on this Virus. I also renumbered the alerts, warnings and anomalies and made some minor improvements in some of the other checkers to make them slightly faster.

3.1 16-May-88. Minor cosmetic improvements. Cut&Copy are better supported now - you can cut parts of the report out as you desire. Copy All lets you copy the entire report without selecting it. Also, on large screen machines, a bigger window (and bigger font) is used for ease of reading.

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.

Inteferfon **cannot** scan MFS (non-HFS) volumes. If you attempt to scan a 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

Inteferon 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 plauge 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 Vision Fund
c/o Sir-tech Development
10 Spruce Lane
Ithaca NY 14850

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.

Thankyou