Tech Info Library

Macintosh: Virus List (4/94)

Article Created: 1 December 1992
Article Reviewed/Updated: 1 April 1994

TOPIC ---

This article lists all known Macintosh viruses, when they were discovered and the effects of each virus if not discovered and removed from the affected Macintosh computers.

DISCUSSION --

Part I: Benign Viruses

Benign viruses replicate with no real damage to data files.

Peace
- One-time peace message - destroyed itself after 3/22/88

Extension
- Gives message “this disk needs minor repairs” for a locked floppy
- Infects unlocked floppies upon insertion
- Printing problems
- Extension conflicts
- MultiFinder crashes

ANTI, ANTI-ANGE
- First virus to modify code resource. Only affects application and Finder.
- May cause system crashes
- Cause applications to crash once infected (Anti-Ange)

CDEF
- Non-destructive
- Adds devices to the Desktop file

CDEF Mutation (discovered 24-Feb-93)
- Minor changes to the code
- same effects as original CDEF virus.

CODE 252
- Designed to spread from January 1 through June 5 of any year
- Virus triggered on and after June 6
- No intentional damage to file or disks

- Displays following message:
  "You have a virus."
  "Ha Ha Ha Ha Ha Ha Ha"
  "Now erasing all disks..."
  "Ha Ha Ha Ha Ha Ha Ha"
  "P.S. Have a nice day."
  "Ha Ha Ha Ha Ha Ha Ha"
  "(Click to continue...)"
- System may behave erratically
- Periodic system crashes
- Infects the System, Finder, and Applications
- Spreads very quickly under System 6.0.x

GARFIELD
- Odd menu behavior, most common is menus will not pop down.
- System files and applications are the most likely to get infected.
- Unknown how virus is spread.

INIT 29-B (Discoverd late March, 1994)
- no malicious intent.
- Spreads very rapidly.
- Infects all types of files: applications, system files and data files.
- Not contagious when found in a data file, meaning it can not spread from a data file
- Can reinfect a file again and again and again. This multiple infection characteristic can result in a wide variety of problems including out of memory error when running applications, the usual unexpected crashes, erratic behavior and an unexpected increase in file size.
- Running an application infected with INIT 29-B can spread the infection to the System file. Once the machine is rebooted, the virus will then spread from the infected System file to any file that is opened.

INIT-M (discovered May 1993)
- Designed to trigger on any Friday the 13th.
- The virus may infect all kinds of files -- including extensions, applications, preference files, and document files --
- Causes problems with the proper display of windows.
- The virus spreads and attacks only under System 7.0 or later.
- It does not spread or attack System 6.

MBDF A
- Spreads quickly
- System crashes
- Infects applications-adds MBDF resource with id 0
- Infects System file-adds MBDF resource with id 0 and renumbers existing MBDF id 0 to id 1.

MERRY CHRISTMAS VIRUS (discovered December, 1993)
- Only affects HyperCard stacks
- The Merry Christmas virus is written in HyperTalk, the HyperCard scripting language.
- Many stacks can function properly when infected, some such as Apple's Service Source cannot.

- Basically, the virus traps these messages:
  - openbackground
  - closebackground
  - idle

Then it looks in the Home stack script for itself, and if it isn't there it copies itself. From the Home stack it checks the currently active stack for itself, and if it isn't there it copies itself.

- merryxmas vaccine (HyperCard stack) will remove any occurances of the virus, as well preventing future infections. The stack is available on online services.

WDEF
- Instructs Finder to infect desktop
- Infects diskettes immediately upon insertion
- Slow performance
- System crashes
- System beeps
- Easily eradicated by rebuilding the desktop, or using SAM Virus Clinic
- Does not affect Macintosh computers running System 7 and higher.

Part II: Malicious Viruses

Malicious viruses damage files, and can even alter applications.

CHINATALK - Trojan Horse
- System extension
- Claims to be a female sound driver that is MacinTalk compatible
- Erases Hard Disk

CPRO - Trojan Horse
- application
- found in a file named CPRO141.SEA, looks like an update to a popular file compression program.
- If the CPro application is run, it attempts to format mounted hard disks and floppy disks.
- Only successful in formatting floppy disks.

FONTFINDER - Trojan Horse type
- Trigger date of Feb 10th, 1990
- Before date, displayed lists of fonts and point sizes in the System file
- On or after date, destroys directories of all mounted volumes

INIT 1984
- Trigger date of Friday 13th in 1991 and after
- Changes names and attributes of large number of folders and files to random strings
- Deletes a small percentage of files (< 2%)

INIT-9403 (discovered 3 March 1994)
- Damage: Alters applications and system files.
  May destroy all disk volumes.
- Spreads: only in Italian version of MacOS so far, but extensive there.
- Systems affected: All Apple Macintosh computers, all systems.

- Once present, the virus alters the Finder file, and may insert copies of itself in various compaction, compression, and archive programs.
- These infected files can then spread the virus to other Macintoshes.
- This virus can only spread under the Italian release of MacOS.
- After a certain number of other files have been infected, the virus will erase disks connected to the system: it attempts to destroy disk information on all connected hard drives (> 16 Mb) and attempts to completely erase the boot volume.

MOSAIC - Trojan Horse type
- Destroys directories
- Renames attached disks to "GOTCHA"
- All available unmounted SCSI disks are mounted and destroyed

NVIR (including nVIRa, nVIRb, nVIR-f nFLU, AIDS, Hpat, Jude, MEV#)
- Infects by installing first in System file, often infects Finder and DA Handler. Lies dormant, then makes itself known.
- Applications beep when launched
- Files disappear mysteriously
- System crashes
- MacinTalk, if installed, says "don’t panic"

SCORES
- Creates invisible SCORES file
- Creates new desktop file in System folder
- Changes Notepad and Scrapbook to generic documents
- Causes system crashes after a certain time
- Difficulty running applications, and printing
- MS Excel files show damage
- Unexplained increases in file size
- Slow system

STEROID - Trojan Horse type
- Trigger date of July 1, 1990
- INIT which claims to speed up QuickDraw on 9-inch screens
- Shipped with a file name (Steroid) preceded by 2 invisible characters (so it loads before SAM Intercept and other extensions)
- Zeros your volume directories
- If file renamed, so that it runs after SAM, in advanced or custom modes you will get SAM alerts saying "There is an attempt to bypass the file system" when the Trojan attacks your volumes. Denying these attempts prevents the Trojan from doing damage.
- NOTE: Having CommToolbox installed seems to interfere with the INIT and keeps the erase from happening.

T4-A/T4-B
- Included with a game called GoMoku (versions 2.0 and 2.1)
- From GoMoku 2.0, virus will spread on August 15, 1992 and later
- From GoMoku 2.1, virus will spread on June 26, 1992 and later.
- Alters/damages The System file.
- System Extensions and INIT files unable to load
- System may become unbootable
- Attempts to modify applications on boot volume

- Damage applications by overwriting locations with infecting code. These damaged applications cannot be repaired.

T4-C

- Affects all Apple Macintosh computer systems and infects applications and System files.
- Under System 6, when activated, T4-C attempts to alter the System file, resulting in INIT files not being able to load. The system may be unbootable.
- Attempts to modify application files on the start-up volume. These damaged applications cannot be repaired.
- Damages the System file, therefore it is important to re-install your system if you think you may have been infected with this virus.

ZUC

- Adds a 1256 byte piece of code at the end of the first executed CODE resource (similar to ANTI)
- 90 seconds after launching infected application ZUC takes over cursor, moving it diagonally until you reboot.
- Only applications are infected.

Article Change History:
1 April 1994 - Added all viruses discovered since March, 1993.
5 March 1993 - Added info on variation of CDEF virus and new T4-C virus.

Support Information Services

Keywords: supt

==

This information is from the Apple Technical Information Library.

19960215 11:05:19.00
Tech Info Library Article Number: 11907