New Macintosh Virus Discovered - 30 June 1992

Virus: T4-A, T4-B
Damage: altered boot code; altered/damaged applications
Spread: possibly significant
Systems affected: Apple Macintosh computers. All types, but see text.
A new virus has been discovered, in two slightly different strains. These were included with the game application GoMoku, versions 2.0 and 2.1. These files were posted to the Usenet comp.binaries.mac newsgroup, and uploaded to various ftp archives, including the one at sumex-aim.stanford.edu. [Note: the game was distributed under a falsified name. The name used in the posting, and embedded in the game, is that of a completely uninvolved person. Please do not use this person's name in reference to the virus. The actual virus author is unknown, and probably used this person's name as a form of harassment.]
When invoked, the virus attempts to alter the System file. This alteration attempt will be noticed by the SAM antivirus program (and possibly by Gatekeeper, depending on settings). The alert message that is displayed indicates that "Disinfectant" is trying to make the alteration -- whether Disinfectant is installed on the system or not. This is evidently an attempt to fool users into approving the modification attempt, thus allowing the virus to infect.
The change to the System file results in alterations to the boot code under both Systems 6 and 7. The damage may render some systems unbootable, but will usually result in INIT files and System extensions (respectively) not loading.
The virus also attempts to modify application files on the system disk. These alterations may damage some applications by overwriting portions of the programs with the virus code. These damaged applications *cannot* be repaired but must be reinstalled from distribution or backup media.
Once installed and active, the virus does not appear to perform any other overt damage. At least one version of the virus may print a message when run after a certain number of files are infected by it. This message identifies the infection as the T4 virus.
[Note: Although this note is unrelated to the T4 virus, we feel it appropriate and important to remind Mac users that neither Apple System 7 nor 7.0.1 should be used UNMODIFIED because they have the "disappearing folders" bug. Users should be sure they have installed the (free) System Tuner 1.1.1 from Apple on these systems; versions 1.0 and 1.1 of the Tuner are outdated or buggy and should not be used. Tuner 1.1.1 is available from authorized Apple dealers, from many user groups, from commercial networks, and on several places on the Internet. Also, System 7.0.1 is *not* the same as System 7 with the Tuner installed; 7.0.1 is a later release of System 7. System 7.0.1 also needs the update installed.]
Authors of all major Macintosh anti-virus tools are planning updates to their tools to locate and/or eliminate this virus. Some of these are listed below. We recommend that you obtain and run a CURRENT version of AT LEAST ONE of these programs.
Some specific information on updated Mac anti-virus products follows:
Tool: Disinfectant

Status: Free software (courtesy of Northwestern University and
John Norstad)
Revision to be released: 2.9
Where to find: usual archive sites and bulletin boards --
ftp.acns.nwu.edu, sumex-aim.stanford.edu,
rascal.ics.utexas.edu, AppleLink, America Online,
CompuServe, Genie, Calvacom, MacNet, Delphi,
comp.binaries.mac
When available: soon (probably by July 6)
Tool: Gatekeeper
Status: Free software (courtesy of Chris Johnson)
Revision to be released: 1.2.6
Where to find: usual archive sites and bulletin boards --
microlib.cc.utexas.edu, sumex-aim.stanford.edu,
rascal.ics.utexas.edu, comp.binaries.mac
When available: soon
Tool: Rival
Status: Commercial software
Revision to be released: T4 Vaccine, Rival Refresh 1.1.9w
Where to find it: AppleLink, America Online, Internet, Compuserve.
When available: Immediately.
Tool: SAM (Virus Clinic and Intercept)
Status: Commercial software
Revision to be released: ???
Where to find: CompuServe, America Online, Applelink, Symantec's
Bulletin Board @ 408-973-9598
When available: immediately
Notes: User definition information:
Virus Name: T4
Resource type: CODE
Resource ID: Any 0
Resource size: >= 5600
Search String: Hex 2F2EFFD02F2EFFC43F3CA97B486E
String offset: >= 714 from end
Check value should be 'E7FA' if all fields entered correctly
Tool: Virex
Status: Commercial software
Revision to be released: 3.82
Where to find: Microcom, Inc (919) 490-1277
When available: 6 July 1992
Comments: Virex 3.82 will detect the virus in any file, and repair any file that has not been permanently damaged by the virus. All Virex subscribers will automatically be sent an update on diskette. All other registered users will receive a notice with information to update prior versions to detect T4. The information necessary to update immediately is also available on Microcom's BBS: (919)419-1602 and on America OnLine. The update string follows:
Guide Number = 7381312
1: 0230 FEAC 7500 00A9 / 36
2: 7B48 6EFF D62F 0E4E / BE
3: BA81 0230 FEA0 7500 / 3A
4: 00A9 7B48 6EFF D62F / 5D

5: 0E4E BA81 8280 9090 / 25
Tool: VirusDetective
Status: Shareware
Revision to be released: 5.0.5
Where to find: Usual bulletin boards will announce a new search string.
Registered users will also get a mailing
with the new search string.
When available: Immediately.
Comments: search strings are:
Resource CODE & Size > 3900 & Pos -1200 & WData 3F3CA9CC*31BC4E71 ; For finding T4

If you discover what you believe to be a virus on your Macintosh system, please report it to the vendor/author of your anti-virus software package for analysis. Such reports make early, informed warnings like this one possible for the rest of the Mac community. Also, be aware that writing and releasing computer viruses is more than a rude and damaging act of vandalism -- it is also a violation of many state and Federal laws in the US, and illegal in several other countries. If you have information concerning the author of this or any other computer virus, please contact any of the anti-virus providers listed above. Several Mac virus authors have been apprehended thanks to the efforts of the Mac user community, and some are awaiting trial for their actions. This is yet one more way to help protect you computers.

Information Provided Via: SOUTH BEACH BBS - MIAMI - 305-891-1062