VIRUS ANALYSIS 2

Fridrik Skulason

Michelangelo - Graffiti Not Art

A number of reports of this virus spreading in the UK have been received in recent weeks, which have prompted the following analysis.

The Michelangelo virus resembles the New Zealand (Stoned) virus in several ways. It is more than a simple modification of New Zealand - large parts of the virus have been rewritten - but the overall structure and various bits of code are identical, so the virus might best be classified as belonging to the New Zealand family. It is obvious that the author has examined New Zealand and has attempted to correct the most serious problem associated with the original virus, i.e. its inability to infect diskettes larger than 360 Kbytes ‘correctly’.

The origin of the virus is not certain, but it appeared first in Australia, and has now spread to Europe, being particularly prevalent in the UK and Scandinavia.

Operation

When the computer is booted from infected media, the virus gains control. It creates a 2K ‘hole’ in memory, by decreasing the number at 40H:13H, and copies itself to that area. After hooking into INT 13H, the virus checks whether it entered the system as the result of a boot from an infected floppy.

If so, the virus reads the Master Boot Sector, and checks whether it is infected. Just like the New Zealand virus it does this by comparing the first 4 bytes of the Master Boot Sector to the first bytes of itself, and attempts to infect the Master Boot Sector if it finds a mismatch.

Master Boot Sector Infection

The virus stores the original Master Boot Sector at Track 0, Head 0, Sector 7. The Partition Table itself (the last 66 bytes of the Master Boot Sector) is copied to the end of the virus, which is then written to Track 0, Head 0, Sector 1. After infecting the hard disk, the virus simply transfers control to the original Master Boot Sector.

Activation

If the computer is booted from the hard disk, or if the Master Boot Sector is already infected, the virus checks the current date, assuming the machine is equipped with a real-time clock. If the current date is the 6th of March, the virus will systematically proceed to destroy all data on the infected disk.

[*It was a researcher (not the virus writer) who named the virus after Michelangelo Buonarroti, the Italian Renaissance artist, on the grounds that Michelangelo was born on the 6th March 1475. The connection between the virus’ trigger date and the anniversary of the birth of the artist is tenuous in the extreme - it is almost certain that the virus writer had a different reason for selecting 6th March as a trigger date.*]

Destruction

The virus first destroys any information on Track 0, then Track 1 and so on. On a 360K diskette, it will destroy sectors 1-9, heads 0 and 1, but on other types of diskettes it will destroy the first 14 sectors on each track.

On machines with an infected hard disk the destruction will be more severe as the virus may trash the entire disk, forcing the user to reformat it and restore everything from backups. On a hard disk the virus will destroy the first 17 sectors on every track, heads 0, 1, 2 and 3.

Destruction is accomplished not by formatting, but by overwriting with whatever is stored at memory location 5000H:0000H. This will probably be a block of zero bytes.

INT 13H Servicing Routine

The virus will only interfere with INT 13H operations if the user is accessing drive A and the drive motor is not already running. The original boot sector is then read into memory, and checked for infection, in the same way as the Master Boot Sector. If it is not infected, the virus attempts to infect it. The media descriptor byte (offset 15H) is checked to see whether it contains 0FDH, which indicates a 360K diskette. If so, the boot sector is stored at Track 0, Head 1, Sector 3 - the last sector of the root directory.

The major difference between Michelangelo and New Zealand has to do with high density diskettes. If the media byte does not contain 0FDH, the virus will write the original boot sector to Track 0, Head 1, Sector 14 - tactfully avoiding the problems associated with the New Zealand virus.

Detection

The following pattern will be found in the Master Boot Sector of an infected hard disk and the boot sectors of all densities of infected diskette.

```
BE00 7C33 FFFC F3A4 2EFF 2E03 7C33 C08E
```

Disinfection

Disinfection of the Michelangelo virus is relatively straightforward. The virus can be removed from hard disks even when it is active, but disinfection of diskettes requires a ‘clean’ machine. The hard disk may (under DOS 5) be cleaned with the FDISK /MBR command. Alternatively, or under previous DOS releases, it can be restored manually with a disk editor by moving the Master Boot Sector from Track 0, Head 0, Sector 7 to its original position (Track 0, Head 0, Sector 1).

To disinfect a floppy disk it is necessary to determine first the location of the original boot sector. This can be done by examining byte 8 within the virus body, which will contain either 3 or 14, giving the sector number in which the boot sector is located (on Track 0, Head 1).

An alternative and more practical method of disinfecting diskettes is to transfer data and programs using the DOS COPY command. This must be done in a clean DOS environment. Once all items have been copied, the diskette should be formatted using DOS FORMAT. Do not use DISKCOPY as this is an image copier and and will transfer the exact contents of the disk including the virus code in logical sector 0.