CERT Advisory CA-1992-02 Michelangelo PC Virus Warning

Original issue date: February 6, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a personal computer virus known as Michelangelo. The virus affects IBM PCs and compatibles. A description of the virus, along with suggested countermeasures, is presented below.

I. Description

The Michelangelo virus is a computer virus that affects PCs running MS-DOS (and PC-DOS, DR-DOS, etc.) versions 2.xx and higher. Note, however, that although the virus can only execute on PCs running these versions of DOS, it can infect and damage PC hard disks containing other PC operating systems including UNIX, OS/2, and Novell. Thus, booting an infected DOS floppy disk on a PC that has, for example, UNIX on the hard disk would infect the hard disk and would probably prevent the UNIX disk from booting. The virus infects floppy disk boot sectors and hard disk master boot records (MBRs). When the user boots from an infected floppy disk, the virus installs itself in memory and infects the partition table of the first hard disk (if found). Once the virus is installed, it will infect any floppy disk that the user accesses.

Some possible, though not conclusive, symptoms of the Michelangelo virus include a reduction in free/total memory by 2048 bytes, and some floppy disks that become unusable or display "odd" graphic characters during "DIR" commands. Additionally, integrity management products should report that the MBR has been altered.

Note that the Michelangelo virus does not display any messages on the PC screen at any time.

II. Impact

The Michelangelo virus triggers on any March 6. On that date, the virus overwrites critical system data, including boot and file allocation table (FAT) records, on the boot disk (floppy or hard), rendering the disk unusable. Recovering user data from a disk damaged by the Michelangelo virus will be very difficult.

III. Solution

Many versions of anti-virus software released after approximately October 1991 will detect and/or remove the Michelangelo virus. This includes numerous commercial, shareware, and freeware software packages. Since this virus was first detected around the middle of 1991 (after March 6, 1991), it is crucial to use current versions of these products, particularly those products that search systems for known viruses.

The CERT/CC has not formally reviewed, evaluated, or endorsed any of the anti-virus products. While some older anti-virus products may detect this virus, the CERT/CC strongly suggests that sites verify with their anti-virus product vendors that their product will detect and eradicate the Michelangelo virus.

The CERT/CC advises that all sites test for the presence of this virus before March 6, which is the trigger date. If an infection is discovered, it is essential that the user examine all floppy disks that may have come in contact with an infected machine.

As always, the CERT/CC strongly urges all sites to maintain good backup procedures.

The CERT/CC wishes to thank for their assistance: Mr. Christoph Fischer of the Micro-BIT Virus Center (Germany), Dr. Klaus Brunnstein of the Virus Test Center (Germany), Mr. A. Padgett Peterson, P.E., of the Technical Computing Center at Martin-Marietta Corp., and Mr. Steve R. White of IBM's Thomas J. Watson Research Center.

Revision History

```
September 19,1997  Attached copyright statement
```