A History Of Computer Viruses — The Famous 'Trio'

Harold Joseph Highland FICS, FACM

Editor-in-Chief Emeritus

It was not until the fall of 1987 that computer viruses began to command worldwide attention in the popular press as well as in the trade and technical press. Late in 1987 computer viruses struck at two universities in the States and one in Israel.

- In October 1987 the Brain or Pakistani virus struck at the University of Delaware.
- One month later, the Lehigh or COMMAND.COM virus was discovered at Lehigh University in Pennsylvania.
- In December, the Hebrew University at Jerusalem found itself attacked by a computer virus. In its search it found the Friday the 13th virus but also uncovered during that search were two variations of the April 1st or April Fool virus.

These three incidents presented us with two different types of computer viruses. The Brain or Pakistani virus was a boot sector infector. The Lehigh virus and the Israeli viruses infected executable code. The former attached itself only to COMMAND.COM; the Israeli viruses infected .EXE and/or .COM programs.

The trio [1] also differed in the media attacked. Aside from the Lehigh virus that infected both floppy disks and hard disks, the others only infected floppy disks. These were the original versions of the viruses. Since then a number of variants or mutations have surfaced.

- Another difference was the damage or operating difficulties caused by these viruses.
- The Brain sometimes destroyed several sectors of a disk but often did little more damage.
- The Lehigh virus, depending upon its host, would wipe out an entire disk after a set number of DOS operations.

The Israeli viruses were replicators, causing an increase in the size of programs. Although most viruses will not reinfect a previously infected program, the coding of one of the Israeli viruses was defective. It permitted the reinfection of an infected program. Because of the viral infection some programs were unable to be executed

[1] We use the term, trio, because most reports late in 1987 were about the Pakistani/Brain, the Lehigh and the Hebrew University viruses. Actually the Hebrew University virus was not a single virus but consisted of several very similar viruses.

0167-4048/97$17.00 © 1997 Elsevier Science Ltd

since there was insufficient memory. In other cases there was a substantial increase in program execution time.

How Each Virus Operates

Along with each virus we have a technical report on how the specific virus operates. These reports are written for the technician familiar with both the microcomputer operating system and the hardware.

These reports are based on extensive research using the virus to infect a system as well as the 'cracking' of the virus. Each virus was disassembled into assembly language code in order to study how it worked. To verify our work we asked Bill Kenny, a programmer with Digital Dispatch, Inc. to assist.

The Pakistani or Brain Virus

The Brain virus has the distinction of being the first computer virus to strike in the United States outside of a test laboratory. It was reported to the Computer Center of the University of Delaware on October 22, 1987 but it had been found in other locations on the campus one or two days earlier. This virus has struck at many universities in all parts of the world and even some businesses, such as the Journal-Bulletin in Rhode Island in the United States.

It was named the Brain because it wrote that word as the disk label on any floppy disk it infected. An initial analysis of this virus on an infected disk revealed two names, Basit and Amjad, with their address in Lehore, Pakistan. Because of this, the virus has also been called the Pakistani virus.

This virus is a boot sector infector. Since its code is longer than the original boot sector, it takes over two additional clusters on the disk. The original boot sector is copied in these two clusters as is the remainder of the virus code.

How the Pakistani/Brain Virus Operates

The Pakistani or Brain virus is a boot sector infector that keeps part of itself 'hidden' in bad sectors on the infected disk; it is not complete within its boot sector.

The target disks are 360K DSDD 5 1/4" disks only. They are identified by the signature byte at the start of the FAT. All other disks will not be infected by this virus.

The bad sectors are located at a minimum of cluster 37H and consist of three continuous clusters or six sectors. The first sector contains the original boot sector for the disk, with the virus itself taking up the remainder of the bad sectors.

At boot time, the Brain boot sector loads the virus itself from the infected boot sector and the three bad sectors, the location of which is kept in the infected boot record. It reserves the top 7K of memory, moves the boot record and just-read virus into it and jumps into the virus code itself.

The virus initialization code consists of taking over the INT 13H vector [disk BIOS] so that it points to the Brain. It also sets the INT 6DH vector to the original INT 13H vector so that the virus can use INT 6DH to call the BIOS without invoking itself. The original boot sector is then read, and control is passed to it so that DOS may continue the boot process.

In operation, the virus watches the INT 13H operations for reads to floppy disks in either the A or B drives. Based on an 'access count' [apparently used to avoid excessive disk overhead], the Brain virus will check to see if this is an infected disk. If the signature is not present [the signature, 1234H, is the word at offset 4], the disk is infected with the Brain. If the function is a READ, the Brain will change the head, track, and sector to the saved boot record so that the infected boot record is hidden from casual inspection.

During infection, three bad clusters are put into the FAT of the disk. The original boot record is written, as noted earlier, to the first of the bad sectors and the rest of the virus is written as the remaining sectors. The Brain boot sector, kept in memory, is given the location of the bad clusters of the newly infected disk. The infected boot sector is then written as the boot record of the disk being infected. If all goes well with the infection, the label of the floppy is modified (or created) with the name "(C) Brain" further marking the disk. This labelling is not used as an infection signature.

Known Bug

- The BRAIN boot sector does not have the 55H, AAH signature as the last two bytes of the sector. As a result it may not be treated as a boot record by some BIOSes.

Added Notes

Wandering into psychology for a moment, the Brain virus seems to be a **"look at what I can do!!"** statement by its author. Supposedly written to discourage foreigners from stealing their already-stolen software, the virus contains a copyright notice and information about the author(s). The code quality is between fair and poor. One portion is supposed to hide the string used for the copyright notice in the volume label and the code that creates it. Yet the Brain contains several other copyright notices, and anyone with basic knowledge of the 8088 processor can see their way through the hidden code.

In detecting the Brain virus, it should be noted that wide distribution and general interest have created at least one, and probably many hacked versions of the virus. This makes the rendering of any signature unreliable. The signature used by the virus itself for identification, 1234H at offset 4 in the boot record, is trivial to change. Also, checking for the use of INT 6DH as the re-directed INT 13H is a simple change. For detection and removal, the Brain should be treated as any generic boot sector infector.—**Bill Kenny**

Some Misconceptions About the Brain

Many misconceptions exist about this virus because of incomplete and/or inaccurate statements that appeared in newspapers. Even computer trade and professional publications have included errors in their accounts. Some of the professional writers, both in the United States and abroad, based their articles on previously published information. Most did not have a working copy of the Brain virus and even the few who did, often failed to fully analyze the program's code. The following are some of the incorrect claims about this virus.

[1] "The Brain virus does not notify the user that the disk has been infected immediately before it ruins a disk." The brain does not ruin the disk. It may overwrite part of a file as it infects the disk.

[2] "The Brain virus demands a ransom from the user." This is the result of a story printed in The New York Times in January 1988. We were misquoted by the author of that story. There is a message to contact the virus author(s) in the boot sector. This can be read only if the system is booted with a write protected bootable disk and examined by using special utilities, such as The Norton Utilities or PC Tools. A copy of the infected boot sector is shown in *Figure 1*.

[3] The Brain virus will infect a hard disk." Actually the virus code is written so that it will never infect a hard disk. It is media specific attacking only double-sided, nine-sectored 5 1/4-inch floppy disks.

[4] "The Brain is a benign virus."Yet Ms Ann Webster, the spokeswoman for the University of Delaware, as well as others, have reported that the virus was destructive as some files on a number of infected disks were destroyed. It is impossible to be both benign and destructive. This oxymoron can be explained by the fact that the virus may remain on the floppy disk without doing any damage. Although the virus looks for its "signature" before infecting a floppy disk, we have found that it sometimes reinfects a disk. It not only rewrites the boot sector but then takes over two clusters. If these clusters contain active files, these files might be lost.

[5] "The Brain virus will not infect any disk unless an infected disk is used to boot the system."The virus can infect a microcomputer and spread to floppy disks even if the boot disk is not infected. If a non-bootable infected disk is used first in an

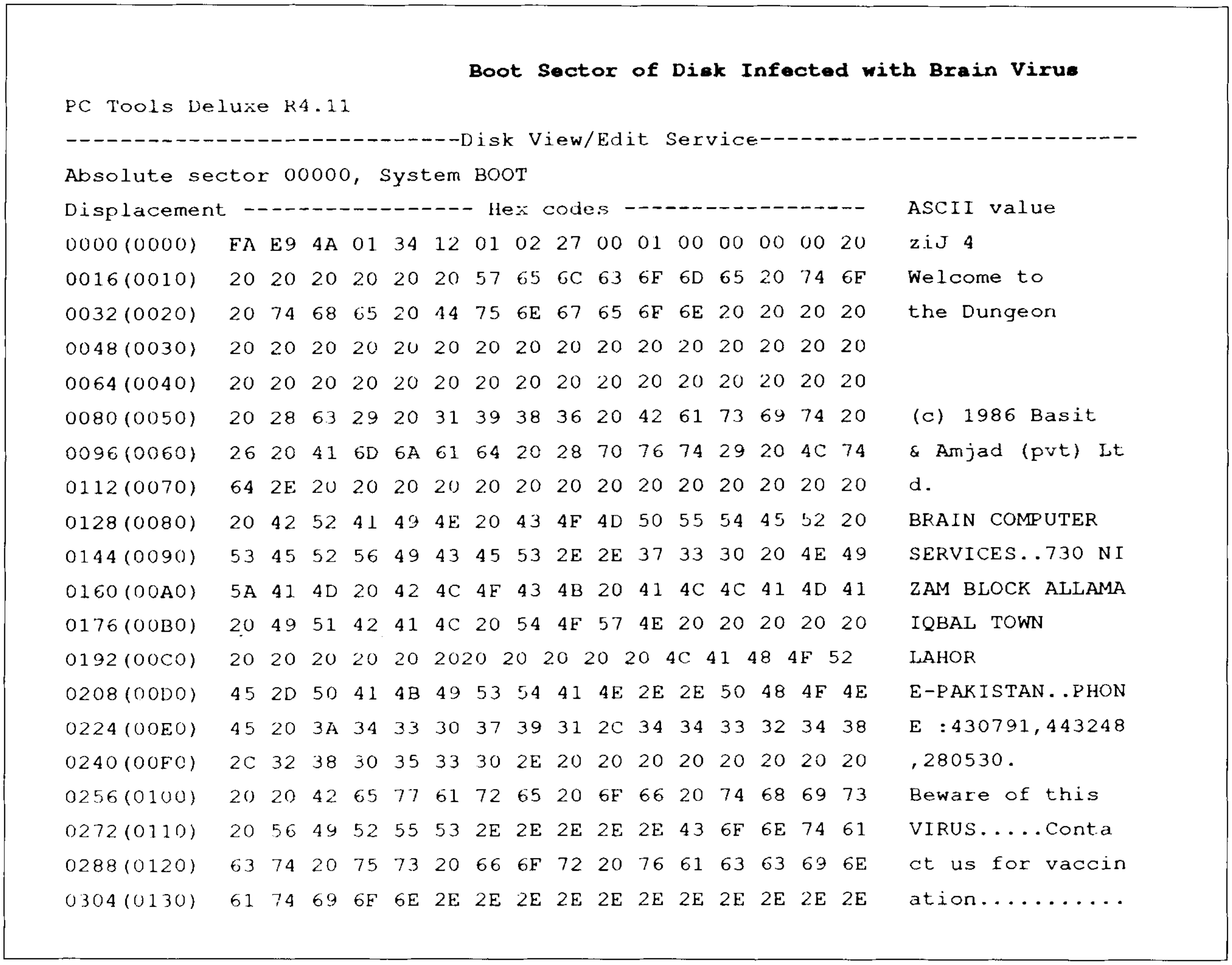
attempt to boot a system, the following message will be displayed on the screen:

Please Insert a Bootable Disk
Then Type [Return]

By that time the virus has already hidden itself in memory. Using a clean bootable disk to start the system will result in that disk becoming infected. The virus will then spread to any other floppy used on the system during that session.

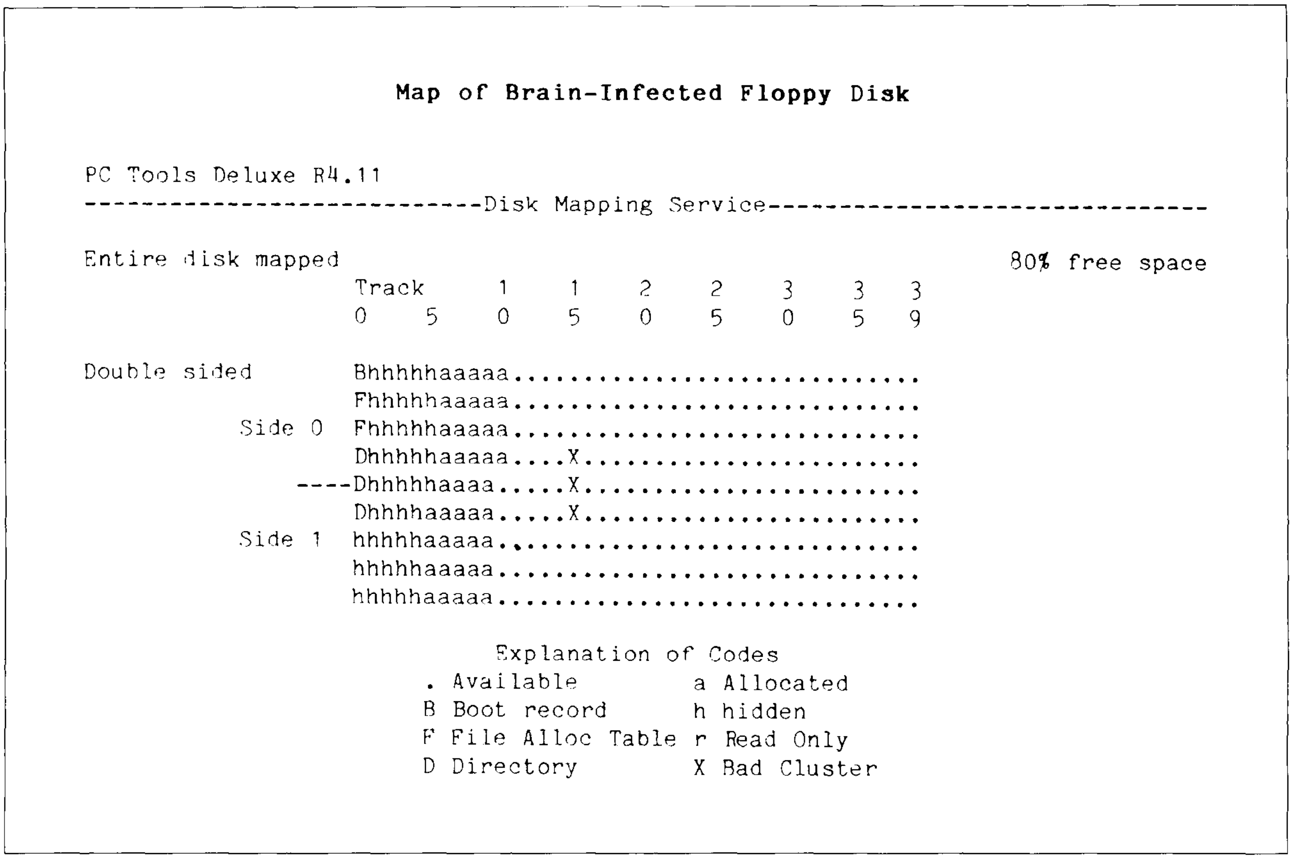
How the Virus Infects a Disk

When a Brain-infected disk is inserted into a system, the virus first copies itself to the highest area in memory. It resets the memory size by altering interrupt vector A211(18) so as to protect the RAM-resident virus. It resets interrupt vector 13H to point to the virus code in high memory and also resets interrupt vector 6H [unused under DOS to point to the original interrupt vector 13H. After that the normal boot process is continued with the loading of both IBMBIO.COM and IBMDOS.COM under PC-DoS



```
                         Boot Sector of Disk Infected with Brain Virus
PC Tools Deluxe R4.11
-----------------------------Disk View/Edit Service----------------------------
Absolute sector 00000, System BOOT
Displacement ----------------- Hex codes ------------------  ASCII value
0000(0000)  FA E9 4A 01 34 12 01 02 27 00 01 00 00 00 00 20  ziJ 4
0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F  Welcome to
0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20  the Dungeon
0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20  (c) 1986 Basit
0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74  & Amjad (pvt) Lt
0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20  d.
0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20  BRAIN COMPUTER
0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49  SERVICES..730 NI
0160(00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41  ZAM BLOCK ALLAMA
0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20  IQBAL TOWN
0192(00C0)  20 20 20 20 20 2020 20 20 20 20 4C 41 48 4F 52   LAHOR
0208(00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38  E :430791,443248
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,280530.
0256(0100)  20 20 42 65 77 61 72 65 20 6F 66 20 74 68 69 73  Beware of this
0272(0110)  20 56 49 52 55 53 2E 2E 2E 2E 2E 43 6F 6E 74 61  VIRUS.....Conta
0288(0120)  63 74 20 75 73 20 66 6F 72 20 76 61 63 63 69 6E  ct us for vaccin
0304(0130)  61 74 69 6F 6E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ation...........
```

Figure 1.



```
                     Map of Brain-Infected Floppy Disk

PC Tools Deluxe R4.11
---------------------------Disk Mapping Service-------------------------------

Entire disk mapped                                               80% free space
                   Track     1    1    2    2    3    3   3
                   0    5    0    5    0    5    0    5   9

Double sided       Bhhhhhaaaaa.............................
                   Fhhhhhaaaaa.............................
          Side 0   Fhhhhhaaaaa.............................
                   Dhhhhhaaaaa....X........................
               ----Dhhhhhaaaa.....X........................
                   Dhhhhaaaaa.....X........................
          Side 1   hhhhhaaaaa..............................
                   hhhhhaaaaa..............................
                   hhhhhaaaaa..............................

                           Explanation of Codes
                      . Available          a Allocated
                      B Boot record        h hidden
                      F File Alloc Table r Read Only
                      D Directory          X Bad Cluster
```

Figure 2.

or IO.SYS and MSDOS.SYS under MS-DOS.

The virus is contained in the boot sector and three contiguous clusters. A map of an infected disk is shown in *Figure 2.*

The virus, residing in high memory, interrupts any disk READ request. If that request is not for the boot sector or non-floppy drive, the virus reads the boot sector of the disk. It examines the fourth and fifth bytes for "1234," that are stored as 34 12, the signature of the Brain. [See *Figure 1.*]

If that signature is not present on the floppy disk, the virus infects the disk and then proceeds with the READ command. If the disk is already infected, the virus does not reinfect the disk but instead continues with the READ. Also if the disk is write-protected, the infection will be terminated.

Normally the virus, in its attempt to infect a disk, will] search for three consecutive clusters it can mark as "bad." If there are no blank clusters, the virus will not infect the disk. However, if there is only one blank cluster and it is neither of the last two clusters on the disk, the virus will select the one blank cluster and overwrite the next two clusters and mark all three as bad.

A Poor Man's Filter

A simple, inexpensive method to protect a disk from becoming infected by the Brain virus is by checking if the virus is resident in memory. This can be done by any of several utilities that show the contents in memory. However one can prepare a simple virus detector by following these simple steps.

[1] Format a floppy disk with or without a system.

[2] Use DEBUG.COM, PC Tools or The Norton Utilities to edit the boot sector. The first line of the boot sector appears as:

EB 34 90 49 42 4D 20 20 33 2E 32 00 02 02 01 00

[3] Since the Brain examines the fifth and sixth bytes for its signature, change those bytes to the signature of the virus, 1234. Below is an altered first line of a boot sector:

EB 34 90 49 34 12 20 20 33 2E 32 00 02 02 0100

To find out if the Brain is in the system, place this altered test disk in drive B. After the system prompt, A, type: DIR B: to obtain a directory of the test disk. If the system is infected by the Brain virus, the following message will appear on the screen:

Not ready, error reading drive B

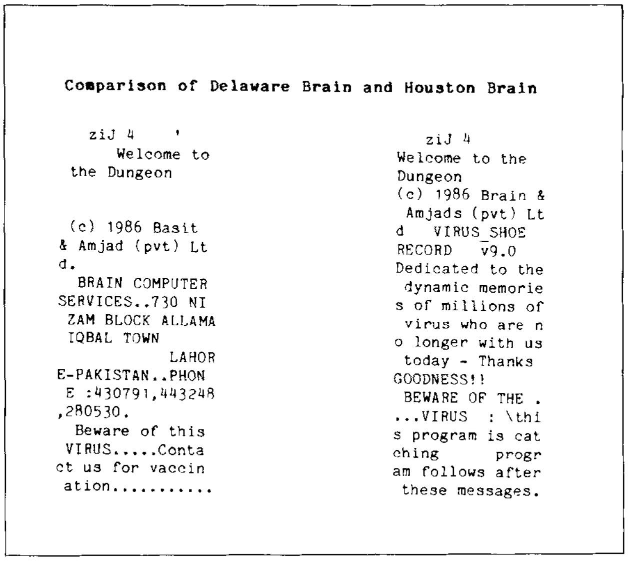
Abort, Retry, Ignore?

The disk with the altered boot sector will work only on a non-infected system.

Some Variations of the Brain

Since the Brain first appeared at the University of Delaware there have been many variations reported at different locations. Early in November 1988, for example, one such version infected about 300 computer library disks at the School of Business at the University of Houston. How many disks, owned by students and faculty, that might have been infected is difficult to determine.

Professor Shafique Pappa of the University sent us a copy. In comparing this version with the original found at the University of Delaware, we found that someone had edited the boot sector message. Similar to the other variations we received earlier, the active code of the virus was not altered. In all respects, except the boot sector message, the two disks were identical.



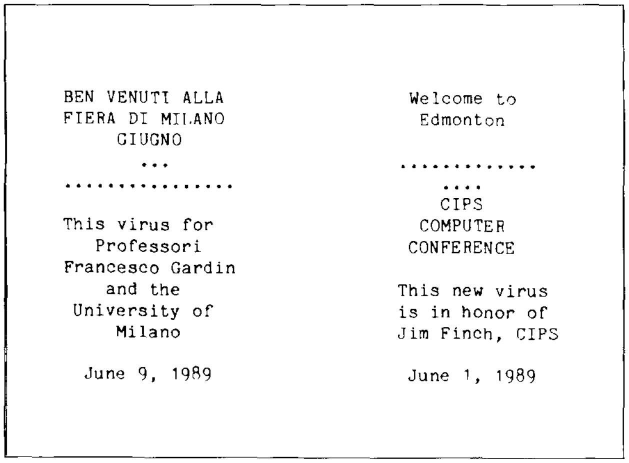
```
Comparison of Delaware Brain and Houston Brain

   ziJ 4    '                        ziJ 4
      Welcome to                    Welcome to the
  the Dungeon                       Dungeon
                                    (c) 1986 Brain &
                                     Amjads (pvt) Lt
  (c) 1986 Basit                    d   VIRUS_SHOE
 & Amjad (pvt) Lt                   RECORD   v9.0
 d.                                 Dedicated to the
   BRAIN COMPUTER                    dynamic memorie
 SERVICES..730 NI                   s of millions of
  ZAM BLOCK ALLAMA                   virus who are n
  IQBAL TOWN                        o longer with us
              LAHOR                  today - Thanks
 E-PAKISTAN..PHON                   GOODNESS!!
  E :430791,443248                   BEWARE OF THE .
 ,280530.                           ...VIRUS  : \thi
   Beware of this                   s program is cat
  VIRUS.....Conta                   ching       progr
 ct us for vaccin                   am follows after
  ation...........                   these messages.
```

Figure 3.

A comparison of the boot sector message found in the original version of the Brain [left] and the University of Houston's copy [right] is shown in *Figure 3.* We wonder why did the author of the new version retain the original copyright notice?

We often use a 'version' of the Pakistani/Brain virus when we demonstrate a number of computer viruses during our speeches. The ASCII portion of this virus is easily modified. By preparing a dedicated virus we can emphasize the ease with which anyone can alter an existing virus. Two of these modified versions of the Pakistani/Brain virus are shown in *Figure 4.*

Late in 1988 we received a set of public domain programs on a special disk with a supplier's label that we recognized. The disk had been sent from a different city in a disk mailer without a sender's return address. Checking the disk we found that it was infected with a mutation of the Pakistani/Brain. Unlike the original Pakistani/Brain virus this one's code was altered so that it infected the C drive, the hard disk. How many



```
BEN VENUTI ALLA             Welcome to
FIERA DI MILANO              Edmonton
    GIUGNO
     ...                  .............
................              ....
                              CIPS
This virus for              COMPUTER
  Professori               CONFERENCE
Francesco Gardin
   and the                This new virus
 University of            is in honor of
    Milano                Jim Finch, CIPS

 June 9, 1989              June 1, 1989
```

Figure 4.

individuals in an office environment would examine the disk prior to making a backup copy?

For almost two years we have examined each disk prior to making a backup. We use PC Tools or the Norton Utilities to obtain a 'map' of a disk and search for bad clusters, a favorite hiding place for some types of viruses We also examine the boot sector to determine if it is 'clean' and does not contain a computer virus. We also read each .BAT and text file using PC Tools or the Norton Utilities and not the standard DOS commands. This is the minimum procedure before we accept a disk to run on our system.

Lehigh or COMMAND.COM Virus

The Lehigh or COMMAND.COM virus was discovered at Lehigh University in Bethlehem, PA late in November 1987. It was found at the start of a school recess and some students had already gone home with infected disks.

At Lehigh University's Computer Center they issued microcomputer program disks to students in the same manner as a library loans books. These disks are to be used for do homework assignments on the machines in the university's microcomputer laboratory or even at the student's home or dormitory.

The students who worked at the Computer Center's checkout counter found that an increased number of disks were returned by students because the disks failed to boot. It was also noted that it was not possible to obtain a copy of the disk's directory under DOS. Furthermore, at the university's microcomputer laboratory that is open to all students, the student assistants in charge of the laboratory found that they had an increased number of hard disk crashes.

When the student assistants examined the remaining disks in the loan library they were surprised to find that there was too recent a date for the COMMAND.COM program when a disk directory was viewed on the screen.

As a result they compared the COMMAND.COM program on the suspected library disks with the one on the source DOS disk. They used the DOS debug program to obtain an assembly language listing of both [a] an original protected version and [b] the suspect COMMAND.COM programs. Thus they were able to isolate the virus.

The Basic Virus Routine

The following is a pseudo-code representation of the Lehigh virus developed by Kenneth Van Wyk of Lehigh University:

```
begin
 IF AnotherDishlsBeingAccessed THEN
  IF (TheOtherDiskIsNotInfected AND
     TheOtherDisklsBootable) THEN
       CopyVirus
       Increase(Counter)
       IF HardDisk THEN
            StoreCounterOnDisk
       IF Counter = 4 THEN
            DestroyOriginal
end
```

How the Virus Worked

Although this attack is analyzed in terms of microcomputers, it is apparent that a very similar technique could be employed with mainframes.

1. The virus code was originally implanted in COMMAND.COM, a systems file that is essential for a DOS computer to boot. It is similar to the IPL [initial program loader] of a mainframe. COMMAND.COM is also used periodically for other microcomputer applications.The virus code was stored in a stack within COMMAND.COM. Therefore, the length of the file was not changed In addition to locating itself in the stack space, the virus had inserted a 'jump' instruction at the beginning of COMMAND.COM so that it was directed to the embedded virus whenever the program was called.

2. When a microcomputer is booted with an infected disk, the altered version of COMMAND.COM remained in memory.The virus code therefore was present in the infected microcomputer's memory.

3. The virus intercepted the standard DOS function requests at interrupt 21H. A number of functions are performed at this interrupt; for example, this interrupt is used to output characters to the screen. The virus waited for either an "execute program" or "find first file" request by a user, such as DIR, TYPE, etc. that are very frequently used.

4. Once one or these functions was requested, the virus code was activated. First the virus checked to see whether the disk being accessed was bootable, that is, contained a copy of COMMAND.COM. If it did, the virus copied itself onto the disk and then incremented a counter. In a two-floppy disk system, the counter remained in memory; in a hard disk system the counter was stored on the hard disk. Although a reboot reset the counter to zero in a two-floppy disk system, the same was not true with a hard disk system.

5. When the counter was equal to or greater than 4, the second part of the virus was called to start its destructive work. This second part of the virus used the DOS interrupt 26H (absolute disk write) to write a series of zeroes to the first 32 sectors of the parent disk, or the hard disk if there was one in the system.Writing over these sectors wipes out the disk's boot tracks and the directory tables, thus rendering the disk useless.

Although a very skilled programmer might be able to recover some of the disk's data, it is doubtful that this procedure is worth the effort.The time would be better spent in reformatting the disk and loading the backups.

How the Lehigh Virus Operates

The Lehigh virus, as it is commonly known, is a virus that attacks only COMMAND.COM, and spreads itself by becoming resident in memory, along with the normal COMMAND.COM, and later infecting other disks (usually floppies).

The virus signature consist of the last word (two bytes) of the infected COMMAND.COM file, and contains the value 65A9h (0a9h, 65h)

When COMMAND.COM is loaded, the virus initialization code allocates a block of memory, copies the virus code there, saves the current INT 21 vector both in memory and in the INT 44 vector, and points the INT 21 vector at the resident virus code. Control is then returned to the normal COMMAND.COM. It should also be noted that invoking a command shell (which many programs do to process commands or let the user use a DOS command) will install the virus again, so that multiple copies are active. Be warned, however, that the memory allocated for the virus will go away with the command shell, but the INT 21 and INT 44 links will not, so that another program re-using the memory will crash the system.

To infect further COMMAND.COM's, the virus watches functions 4BH (load program) and 4EH (find first matching file) of INT 21H. When it finds either function, it takes the drive letter of the passed filename or the current default disk, if the passed filename does not contain a drive letter, and checks for COMMAND.COM on that disk. If it exists, and does not have the signature, it is infected with the virus and the infection counter is incremented. When the counter reaches 4 and the boot disk is not a hard disk and the last infected disk was A or B and the last infected disk is not the current disk, two things happen:

[1] 32 sectors worth of data are written from the ROM segment (the OFE00h segment) to disk, trashing the boot sector, FATs, root directory, and some data.

[2] A 'string' from the ROM segment is sent to the screen. The DOS call then proceeds normally.

Known Bug:

- The direction flag is not cleared before a string primitive (MOVSB), so that its correct operation is not guaranteed.

Comments:

The virus assumes that COMMAND.COM will always end in data (stack?) space that may be safely over-written. If it is truly safe to over-write it, why is it included in the file instead of simply using the memory after the end of the file (since its value does not matter, that fact that it is random memory is irrelevant)?

The virus also assumes that COMMAND.COM will always start with a 3-byte JMP to some initialization routine. Microsoft and/or IBM and/or COMPAQ and/or... do not guarantee this, so this will probably fail under some (possibly future) version of DOS. — **Bill Kenny**

Postscript

The university's computer center alerted students and faculty members to the possible danger. Van Wyk also sent out a warning on the BITNET communications network to alert other universities of the virus danger. In our talks with Kenneth van Wyk he noted that:

- the virus code was about 346 bytes long, located between 59AF and 5B09,
- an unsuspecting student probably picked up the virus from a bulletin board; the reason for sending the BITNET warning message to other universities, and
- the virus was developed by someone with "a very very sick mind."

Fortunately, the virus programmer made several mistakes.

First, standard DOS functions were used to copy the virus code. This caused the write date of the COMMAND.COM file to be changed. A professional would have covered his/her tracks and avoided changing that date which served to alert those who did the autopsy.

Second, the virus writer never checked to determine if a write protect tab was used on a disk. Thus, if an unsuspecting user tried to obtain a directory of a protected disk, a DOS "write protect error" would appear on the screen. This should alert a user to suspect that something was wrong. Many inexperienced users probably would have removed the protect tab and continued, not knowing what was happening.

Furthermore, in testing the virus it was found that it could not compromise security such as a file set to read only. Because of this a well set up local area network [LAN] would probably be safe from this virus.

The Israeli Viruses

In December 1987 the Hebrew University of Jerusalem discovered that its microcomputers had been infected with a virus. They found that a program that had often been run in the past was suddenly too large to fit into memory. Upon closer examination the computer specialists under Yisrael Radai of the Computation Center of the University found that every time an .EXE program was executed, its size increased by 1808 bytes. The .COM programs increased in size as well but there was only a one-time increase.

As the computer center staff and a group of students from the Computer Science Department of the

University searched tor the virus they encountered a new phenomena. Not only had the virus increased the size of executable programs but within 30 minutes after the microcomputer's memory was infected, all processing was dramatically slowed. Further investigation revealed that when the virus had infected the memory and the date of the computer system was any Friday the 13th starting in 1988, any program that was being executed was erased from the disk. These findings were based on analysis of the virus and verified by actual experimentation.

How the Jerusalem Virus Operates

This virus is a general executable infector, capable of infecting both .COM and .EXE files. It notes the type of file being infected [see bugs noted below], and places it in the appropriate location. It sets the appropriate links, if any, to execute the virus first. This virus also installs itself as a TSR. to extend DOS with additional functions.

The virus signature is two-fold, one part of which does not work well. First, the virus must find if the resident portion of the virus is already installed. It does this by calling DOS INT 21H with function 0E0H. If the virus is not installed, the return in AH will probably still be 0E0H [possibly varies with DOS version]. If installed, 0300H is returned in the AX register [AH = 03H, AL is not checked upon return]. The other part of the signature is a five character string, "MsDos," as the last 5 bytes of the program. Due to a programming lapse, however, this does not hold true for .EXE files [see bugs noted below].

If the virus is already resident, the original program is executed. If it is not resident, the virus moves itself down to the start of memory after the PSP and takes over the INT 21H vector. Next it checks the current date:

- If the year is 1987, it does nothing.
- If the year is not 1987 and the date is Friday the 13th, it sets a flag to be destructive instead of infecting the program.
- If the year is not 1987 and the date is not Friday the 13th, it takes over the clock interrupt, INT 8H, to cause 'harmless' mischief. It then searches the environment for the name of the executing program, and does a load and execute program call on it. Since the virus is hooked into INT 21H already, it will not try to install itself again. When it returns from this call, it finishes installing itself as a resident program.

As a resident program, the virus has several functions:

[1] Serves as a signal not to install itself again.

[2] Provides functions for the virus to work properly.

[3] Infects other programs.

[4] Performs appropriate 'mischief.'

To infect other programs, the virus takes over function 4B00H of INT 21H. When this function is called, it checks to see if the requested program is COMMAND.COM. If it is COMMAND.COM, it leaves the program untouched. If it is not COMMAND.COM, the virus checks the last letter of the filename extension. If it finds an M or m, it assumes a .COM file and performs that infection. Otherwise it infects the called program as an .EXE file. It then checks the last 5 bytes of the file. If they are "MsDos," the virus signature, it leaves the file alone; otherwise it infects it. During infection, the file's time, date, and attributes are preserved. After it is done, the virus calls the original INT 21H vector to perform the actual loading and execution.

If it finds that the "Friday the 13th" flag is set, instead of executing the program the virus deletes it. Then it passes the name to DOS, which will return a notice that the program cannot be found.

If the clock interrupt, INT8H, is taken over, each 'tick' decrements a counter that is initially set to just under 30 minutes. When the counter expires, the virus first scrolls part of the screen, messing up whatever is displayed, and then at every 'tick' (18.2 times a second) performs a large number of useless operations, slowing down the system.

Known Bugs

- The virus assumes that DS contains a meaningful address after a load and execute call. This may be true for some DOS versions, but is far from guaranteed for all.

- In the virus DOS functions 0DDH and 0DEH, it assumes that the direction flag is cleared upon entry, but this is not guaranteed.

- It assumes that .COM and .EXE extensions are used exclusively and that they are meaningful. This is wrong since they are merely DOS conventions. A program name passed to the load and execute function may have any name, with or without an extension. Also the file type [.COM and .EXE] is determined by the .EXE signature bytes at the start of the file, not the filename extension.

- The virus uses multiple prefixes on a MOVSB instruction [both REPZ and a CS: segment over-ride] without disabling interrupts. On both the 8086 and 8088 processors when an instruction with multiple prefixes is interrupted, the address of the last prefix is pushed to the stack and not the first prefix. Thus when returning from the interrupt only the last prefix is present when the instruction starts executing again. This leads to erratic behavior if not a system crash.

- It also changes the stack with interrupts ON. Some early 8088 processors had a bug which permitted interrupts after a change to a segment register. An interrupt in the middle of changing SS and SP therefore uses an invalid stack.

- It assumes that the name of the current program can be found in the environment but this is true only under DOS 3.0+

- In the virus DOS function 0DEH [move and execute an .EXE file] which is never called by this virus, the virus sets the stack pointer to an area beyond the end of the TSR. If this function is called the stack can destroy the information in the next memory control block.

- The virus assumes that the filename passed to the load and execute program function has a maximum of 65 bytes. Although any length name may be passed, DOS will use a maximum of 64.

- The author of the virus apparently forgot to set the signature during .EXE file infection. This will cause multiple infections of .EXE files.

Note: Despite this extensive bug list, this is one of the most interesting viruses we have examined because of its ability to infect both .COM and .EXE files. — **Bill Kenny**

Reports about the Virus Attack

Because information about the Friday the 13th virus was limited outside of Israel, news reports were too often based on hearsay. Some papers treated the virus as a joke, a student prank. At the other extreme were those stories that reported the attack by a killer virus.

A front page story in The New York Times on January 31, 1988 reported that the virus was apparently intended as a weapon of political protest. The author

[3] The author of The New York Times article also attributed a quotation to us that we never mad. In that article he wrote that we reported that the Brain Virus contained a random demand for $2000. We had told the author in an interview that we had heard reports about the virus but had not seen it. In our conversation he noted that he heard that the Pakistani virus authors had asked the 'victims' to write to them. The author, knowing that we had taught many foreign students, asked if we could guess how much payment might be requested. We noted that some students might ask for $200, some might ask for $2 000 and others $20 000.

Since we knew the author for several years and since we had a tape of our telephone interview we did not write to the author but telephoned him. We know the job of putting rapidly gathered notes together to write a story and could appreciate his making an error. Having worked for newspapers in the past we did not request printing a correction. Even if the newspaper did so, it might appear hidden somewhere in the paper many days later

What is disturbing is that most of that article has appeared in print in newspapers and magazines all over the world. Probably more serious is the fact that future researchers in this field will pick up inaccurate and/or incomplete parts of the story and include these quotations with appropriate footnotes. Some authors of recent books have already done so — HJH of that article, in reply to Mr. Radai's letter, wrote that he "was too quick to assume too much about this virus, its author, and its intent."[3]

Because of The New York Times story the virus has often been called the PLO virus. Yet, according to Mr. Radai all users had been alerted and to his knowledge no files were actually deleted on Friday 13, 1988.

Other Viruses Found

Three other viruses were found at Hebrew University during their computer virus search. One was a variant of the Friday the 13th or Jerusalem virus.

The Friday the 13th virus attacked both .EXE and .COM programs. However, it did not attack COMMAND.COM, thereby permitting the system to continue operating. The variant of this computer virus is identical to the widely-known Friday the 13th virus but with two small exceptions:

[1] The signature had been changed from "sUMsDos" to "URI2V21."

[2] The do-not-infect-this-program name routine had been changed from:

"COMMAND.COM" to "MMMMMMM.ZZZ."

In the version of this variant that we have examined, the only other differences are in the infected (host) program and the 'leftover' values in the variables, which do not affect the action of the virus.

The April Fool Viruses

The other two viruses discovered have been called the April Fool viruses or the April 1st virus. One infected .EXE files and the other .COM files.

The April 1st EXE virus when activated checks the current date. If it is April 1st, the virus decrypts a string contained within the virus and displays the message on the screen:

"APRIL 1ST HA HA HA YOU HAVE A VIRUS"

After the message is displayed the system enters an infinite loop with the interrupts off causing the system to crash.

The April 1st COM virus is virtually identical except that infects .COM files. Also if the year is 1988 or later and the date is between January 1st and March 31st, the COM virus displays the following message on the screen:

"YOU HAVE A VIRUS !!!"

But if the year is 1988 or later and the current date is April 1st, this virus acts the same as the EXE virus in that it displays the message:

"APRIL lST HA HA HA YOU HAVE A VIRUS"

and entering an infinite loop, the system hangs and requires a cold boot to restart the system.

We have some variants of both of the April 1st viruses. Not having access to the original Israeli versions we are uncertain which are the original and which are later variants. In one the virus executable name is "VIR$$VIR.EXE;" in another the name is "TMP$TMP.EXE." Furthermore, one has a version number of "3.00" and another's version number is "2.01."

How the April 1st EXE Virus operates

This April 1st virus is a general .EXE infector, which works by installing itself as a resident program to extend DOS with additional features. It will not install itself if the April 1st.COM virus is installed.

The virus uses 'two' signatures, one of which is an additional DOS function. If the additional function (0DEH) exists, the original program executes, and there is no return from the DOS call. If the function does not exist, the call returns, and the virus installs itself. The other part of the signature is the virus placing the value 1984H in the checksum field of the .EXE header. This is as (un)likely as any other checksum value [1 in 65536 or lower, as some linkers do not set the checksum field]. and makes a reasonable signature.

If the virus is not resident, the initial call to the virus DOS function fails, which causes the virus to install itself. It takes over the INT 21H vector, then finds the name of the current program in the environment, and does a load and execute program call to DOS. This second call does not try to install itself as INT 21H already points to the virus. When the program exists, the virus finishes making itself resident.

The virus, during installation, checks the current date. If it is April 1st, the virus decrypts a string which it displays on the screen:

"APRIL lST HA HA HAYOU HAVE A VIRUS"

It then enters an infinite loop with interrupts off and crashes the system.

If the year is 1980 or 1988 or after and the date is a Wednesday after April 1st, the virus takes over the system timer tick INT 1CH. When the count reaches about 55 minutes, the virus goes into an infinite loop crashing the system. Also, the counter is not zeroed when an infection takes place, so each later infection has a shorter 'time fuse'.

To infect other programs, the virus takes over function 4B00H of INT 21h. When this function is called, the virus program checks if the requested program has the extension EXE. If it is EXE and the checksum in the program header is not 1984H, the file is infected. The infection program uses a temporary file, TMP$$TMP.EXE, to create the infected file. After the infected program is built into the TMP$$TMP.EXE file, the original file is deleted. The temporary file is then renamed to the original file with the original time and date.

An interesting quirk is the virus containing code to deal with the situation of a return from a TSR DOS call, a situation that cannot exist.

Known Bugs

- Like the April 1st COM virus, the direction flag is never cleared.
- Also as in the case of the COM virus, the one assumes that the name of the current program can be found in the environment, true only under DOS 3.0+. —**Bill Kenny**

How the April 1st COM Virus Operates

This April 1st virus is a general .COM infector, which works by installing itself as a resident program to extend DOS with additional features.

The virus uses two 'signatures', one of which is an addition DOS function. If the additional function (0DDH) exists, the original program executes, and there is no return from the DOS call. If the function does not exist, the call returns and the virus installs itself. The other part of the signature is the first two bytes of a text string, "sURIV", which is checked for during infection of subsequent files.

If the virus is not resident, the initial call to the virus DOS function fails, which causes the virus to install itself. It takes over the INT 21H vector, finds the name of the current program in the environment, and does a load and execute program call to DOS. This second call does not try to install itself, as INT 21H already points to the virus. When the program exists, the virus finishes making itself resident.

To infect other programs, the virus takes over function 4B00H of INT 21H [load and execute program]. When this function is called, it checks to see if the requested program has the extension .COM. If the program name is not COMMAND.COM, the program is scanned for the 2-byte signature string "sU". If it passes all these tests, the file is infected. The infection uses a temporary file, TMP$$TMP.COM, to create the infected file. After the infected program is built into the TMP$$TMP.COM file, the original file is deleted and the temporary file renamed to the original file and maintains the original time and date.

After infecting a file, the DOS date is examined. If the year is earlier than 1988, or the date is later than April 1st, the requested program executes normally. If the year is 1988 or greater and the date is earlier than April 1st, the virus displays the message:

"YOU HAVE A VIRUS!!!"

and executes the requested program normally. If the year is 1988 or greater and the date is April 1st, the virus displays the message:

"APRIL lST HA HA HA HAYOU HAVE A VIRUS"

and goes into an infinite loop that crashes the system.

Known Bugs

- The direction flag is never cleared, although the program assumes auto-inc [flag cleared] for string primitives.
- The program assumes that the name of the current program can be found in the environment, which is only true under DOS 3.0+.
- The drive information passed to the just-infected program in the AX register is the information for the original infected program, and does not correspond to the command line entered.
- When the name of the program being called for execution is copied into a local buffer, only 63 characters are copies. The passed name may be any length, but only 64 are significant.
- When searching the file name for the extension, it is assumed that a period will be found. The name passed to DOS function 4B00 may be anything, and a period is not guaranteed.
- It is assumed that the extension is significant [determines file type]. The .COM extension is a DOS convention, and may contain a file in the .EXE format. The true way to tell file type is to check for an .EXE signature at the start of a program.
- When allocating a memory block to infect a program, it is assumed that the allocation will succeed. If the memory is not available, low memory [corresponding to the error code] will be over-written, probably crashing the system. —**Bill Kenny**.