# VIRUS ANALYSIS 1

***Eugene Kaspersky***

## Peter-II - Three Questions of The Sphinx

How much does a user really need to know to operate his IBM PC effectively? Certainly he needs to understand how to use the keyboard, and with the advent of so many graphical interfaces, knowledge of the mouse is also necessary. Basic knowledge about how the computer works also helps - how to use the disks and, most importantly, how to turn the machine off and on. Reading the manuals is also a pretty good idea, so that the applications which are used are understood. Is this enough? Maybe.

What a user needs to know in order to defend his computer from computer viruses is a more difficult question. Should he simply know how to use a virus scanner? Does he need to understand how lots of different viruses work, and exactly how and what objects they infect? It is a difficult question, but I think my answer to it will come as some surprise.

The latest news from the antiviral battle-front is that if the user wants to defend the contents of his computer from viral attack, he should know have an outstanding knowledge of trivia. For example, to be fully prepared, the user should know the names of rock-superstars and their popularity. Unbelievably, this knowledge can be invaluable in the fight against viruses... especially if the computer in question happens to be infected by the Peter-II virus and the date is February 27th.

### The Installation Routine

Peter-II is an ordinary memory-resident master boot sector virus. It is six sectors long (0C00h bytes), made up of five sectors of virus code, and one sector which is used as a data area to store the original boot sector which is replaced by the virus.

The virus is executed when the user boots the machine from an infected disk. Its first action is to decrease the effective size of the system memory (by decreasing the word at the address 0000:0413 by four), read the rest of the virus in from the disk, and copy itself to the memory at address 9F00:0000. This has the effect of reducing the total system memory by 4K.

As the virus is executed before DOS has loaded, the DOS services Get System Time and Get System Date are not available, and the virus has to use other more complex means to ascertain the system date. It does this by directly reading the data stored in the CMOS: the virus outputs the address value into port 70h and reads the result which is returned in port 71h. If the current date is set to February 27th, the virus calls the trigger routine (see below).

If the trigger conditions are not met, the virus reads in the Int 13h vector and stores in within the virus code. It then initialises its own Int 13h handler, and sets the relevant entry in the interrupt vector table to point to it. If the computer has been booted from an infected diskette, the virus now attempts to infect the hard drive. When this process is finished, the original boot sector is executed.

However the virus does not check the contents of memory before installing itself, which can cause the machine to crash in some instances. Consider the case of attempting to boot a machine with an infected hard drive from an infected floppy diskette. The virus is first run from the infected floppy disk, and, after hooking Int 13h, it executes the floppy disk boot sector. If this disk is not bootable the familiar 'Non-System disk or disk error. Replace and press any key when ready' message will be displayed.

At this point, if the disk is removed and a key pressed, the copy of the virus on the hard drive is executed. This hooks the current Int 13h address (which already points to the virus). Therefore the next time an Int 13h interrupt is encountered, the machine will crash.

### Infection and Int 13h Handling

The master boot record is infected during virus loading. The virus reads the original sector and checks the virus ID byte - if the byte at offset 01FDh is equal to BBh, the virus assumes that the disk is already infected, and the routine aborts. If not, the virus saves this sector on the hard drive at sector 6, head 0, cylinder 0 and writes itself into the first physical sector of the hard drive, and to the next four sectors.

The virus monitors all calls using Int 13h to provide an infection mechanism and stealth. Whenever there is a request to read or write to the sectors, the virus substitutes appropriate register values so that it appears that the disk is not infected. If the request concerns the original sector one, the contents of the relocated boot sector are returned/altered. If the request concerns any of the sectors two to seven, the call is passed on to sector eight. This works on most machines, as these sectors are usually filled with zeros.

Unfortunately life is not always so simple. On early*NetWare* servers (versions 2.xx) this space is used for the start of the *NetWare* boot code, and in this case extensive damage will result. Many boot sector viruses use this 'dead space' as storage, and for this reason, viruses of this type on*NetWare* servers almost invariably cause a disaster.

Whenever a floppy disk is used, the virus checks to see whether it is already infected by examining the contents of the disk's boot sector. If the value of the byte at offset 01DFh in the boot sector is 11h, the infection routine aborts.

The virus then checks another section of the boot sector - the byte at the address 0018h. This contains the number of sectors per track on the floppy disk. If the value is not equal to 15 (i.e. if the disk is not a 1.2Mb 5.25 inch disk), the infection routine terminates.

If the disk is deemed suitable for infection the virus attempts to format an extra cylinder at the end of the disk. A normal 1.2Mb disk has 80 cylinders which are accessed by DOS, numbered 0 to 79. Although it is not possible to access tracks outside this range using standard DOS calls, some drive controllers are capable of using these extra cylinders, and the virus takes advantage of this in order to infect the disk without decreasing its storage capacity.

The virus uses these extra sectors to store part of the virus code. The relocated boot sector is stored separately in the last sector of the standard root directory (sector 14, head 1, cylinder 0)

**Trigger**

On February 27th, as described above, the virus calls the trigger routine. This routine is encrypted, and the first step is for the code to be decrypted. Once completed, the routine displays the message:

```
Good morning,EVERYbody,I am PETER II Do not
turn off the power, or you will lost all of
the data in Hardisk!!!

WAIT for 1 MINUTES,please...
```

Then the virus encrypts all the sectors of the physical hard drive: all the words are XORed with the value 7878h. If the machine is switched off at this point, all data on the drive will be lost, and the user will have to restore from a backup. However, it is possible to recover the disk by correctly answering the three questions which the virus displays next:

```
Ok.If you give the right answer to the
following questions,I will save your HD:

A. Who has sung the song called "I`ll be
there" ? 1.Mariah Carey  2.The Escape Club
3.The Jackson five  4.All  (1-4):

B. What is Phil Collins ? 1.A singer  2.A
drummer  3.A producer  4.Above all   (1-4):

C. Who has the MOST TOP 10 singles in 1980's ?
1.Michael Jackson  2.Phil Collins (featuring
Genesis) 3.Madonna  4.Whitney Houston   (1-4):
```

The user should give three correct answers, in this case the virus decrypts and restores the hard drive sectors and types:

```
CONGRATULATIONS !!! YOU successfully pass the
quiz! AND NOW RECOVERING YOUR HARDISK ......
```

and the disk is recovered. If any of answers are wrong, the virus displays:

```
Sorry!Go to Hell.Clousy man!
```

and all the data on the drive is lost.

While this trigger routine doubtless caused the virus author great mirth, the casual disregard for other people's data makes this a rather nasty piece of malicious code. Fortunately, there is no time limit on the questions, so the user can ring up his friends to find the answers! And what are the answers to these 'three questions of the Sphinx'? Easy... Four, four and two.

## PETER-II

| | |
|---|---|
| Aliases: | None known. |
| Type: | Memory-resident Master Boot Sector. Fully Stealth. |
| Type: | Floppy Boot Sector and Hard Drive Master Boot Sector. |
| Self Recognition: | |
| Disk | Checks the byte at the location 01FDh for the value BBh or 11h. |
| Memory | None. |
| Hex Pattern: | `fa0e 1f33 c08e c08e d0bc 007c 2683 2e13 0404 fb0e 07b9 0300` |
| Intercepts: | Int 13h for infection and stealth. |
| Trigger: | Displays three questions and encrypts the contents of the hard drive sector by sector. If the questions are answered correctly the disk is recovered. |
| Removal: | Specific and generic removal is possible. Under clean system conditions, replace original contents of Master Boot Sector from sector 6 (hard drive) or from logical sector 28 (floppy). |