VIRUS ANALYSIS 1

Finnish Sprayer: Electronic Graffiti

Mikko Hyppönen
Data Fellows, Finland

Virus writers have sometimes been compared to people who create graffiti. It is as difficult to find a rational motive for vandalising other people's property with sloppy spray-paintings as to understand the rationale behind creating a harmful computer program. Whatever the reason, it is unfortunate that both of these activities remain popular. In the case of Finnish Sprayer, one can see a person who perhaps combines both of these pursuits - the 'artist' scrawls his electronic graffiti over the entire contents of an infected hard drive.

This virus was first found in Finland in December 1993, and has quickly spread throughout the country. It was not long before it was found in Sweden, Russia and Estonia, and it may well have spread even further.

Installation

Finnish Sprayer is a fairly typical boot sector virus which infects floppy boot sectors and hard disk Master Boot Sectors (MBS). It employs stealth methods to conceal its presence, and contains two destructive trigger routines.

The virus stores the original boot sector and its own code on the last three sectors of either the active hard disk partition or a diskette. When a PC is booted from an infected disk, the virus code is executed, and either installation or hard drive infection begins.

Its first action is to load the second sector of its code from disk. After this, it relocates all of its code to the top of the conventional memory area and continues the execution from there, decreasing the available memory by 5K. The reason for reserving this large area is unclear - the virus only requires 1K of memory to function, making it likely that this is a simple arithmetical error.

The next part of the virus code is also rather unusual: it checks whether or not the operation of moving the second part of the virus code to memory has been successful. This is done by searching for the letters 'Ai' in the area into which it believes it has loaded the code. If this marker is not found, the virus will try to overwrite the first sector of the hard disk with random data, and reboot the machine.

This destructive routine does not work because of a programming error, but it is obviously meant to be executed if a read error occurs during the virus' installation phase, or if the second part of the virus code is corrupted.

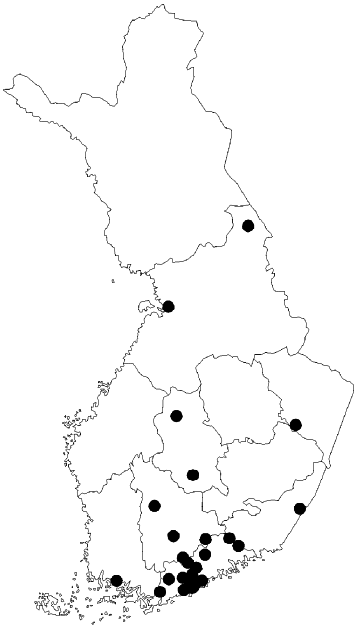
Propagation

The virus is now ready to infect the MBS of the hard disk. It loads the MBS to memory, and analyses the partition information. The virus then searches for its own infection marker: the letters 'Ai' in offset 45h of the MBS. If the computer is already infected, the virus code exits, and lets the normal boot process continue.

If the machine is uninfected, the active partition is located, and its file system type is identified - only partitions using a known DOS file system are infected. This kind of checking is rare among boot sector viruses, and means that the virus will not infect PCs running other operating systems (e.g. *OS/2* and *Windows NT*).

If the hard disk is found suitable for infection, the virus moves the original partition information to the correct place inside the viral code and writes an image of its first sector to the MBS. The virus calculates the location of the end of the active partition and copies the original MBS and the second part of its own code to the last two sectors. Any data contained within these sectors is overwritten.

The virus then executes the original boot sector. It does not stay active after the initial infection (i.e. when a previously uninfected computer is booted from an infected diskette), and will only function when the machine is booted from an infected hard disk.



The Finnish Sprayer virus has been reported throughout Finland, with most incidents concentrated in the south of the country. Reports are indicated by black dots.

Stealth

Once the hard disk is infected, the virus code will be executed during every boot-up. Its operation is similar to that of the floppy disk boot code, but after initialisation it makes a date check, and collects the original Int 13h vector for later use. Finnish Sprayer then installs its own Int 13h handler by modifying the interrupt table in low system memory to point directly to the virus code.

The virus' Int 13h handler starts by checking the called function. If this is not a disk read, the virus passes the call on to the original Int 13h handler, otherwise a rudimentary check is made to ascertain whether the call is directed to a fixed disk or a floppy drive. This information is used to branch program flow.

In the case of a read from hard disk, the virus checks whether it is a request to read the MBS. If so, the register values will be replaced with the head/cylinder/sector values of the original MBS and control is passed to the original Int 13h handler. The BIOS routines then complete the stealth operation by reading the original MBS to memory, and returning it to the calling function.

The virus does not stealth the last two sectors of hard disks, and does not stealth floppy disks at all. If the intercepted Int 13h call is a read from a floppy disk, the virus checks whether or not the disk is already infected. If it is not, the virus inspects the 'total number of sectors' field in the boot sector in order to to ascertain the diskette type.

The virus recognises the four common types of diskette: 360KB, 720KB, 1.2MB and 1.44MB. If the disk's structure does not match any of these, the virus will not infect it. Non-standard (for example, FDformatted) 180KB and 2.88MB floppies are never infected. If the virus recognises the disk type, it writes its own code to the boot sector and overwrites the two last sectors of the floppy with a copy of the original boot sector and the remainder of its code.

Activation

During every boot-up from the hard drive, Finnish Sprayer will check the real-time clock date. If the date is 25 March, the virus will activate, overwriting random sectors on the active partition. The random number is generated by using non-initialised registers as destination values and entering a loop, which calls the BIOS disk write function, decrementing the head value after each write.

After this destructive routine, the virus changes the screen background to grey and displays the text:

```
FINNISH_SPRAYER.1. Send your painting +358-0-
4322019 (FAX), [Aija]
```

Since this text is encrypted with a XOR 50h operation, it is not visible inside the virus code. The phone number is that of the Finnish House of Parliament, which received dozens of faxes on activation day this year. After the display routine, the virus hangs the machine by entering an infinite loop. It should be noted that since real-time clocks are generally available only on AT machines and above, this routine will fail on older machines. On such computers, the virus will never activate. Finnish Sprayer also contains the following unencrypted text, which is never shown:

```
Tks to B.B, Z-VirX ..... [Aija]
```

This string is also used as part of the virus' self-recognition signature. Incidentally, the trigger date of 25 March is also the 'name day' of Aija (a girl's name) in Finland.

Conclusions

The coding style of Finnish Sprayer varies between different parts of the virus. This might indicate that the author has incorporated parts of older viruses into its make-up, although no obvious similarities with other common viruses exist. Another explanation is that this virus might be the work of a number of different people, working as a team.

Finnish anti-virus organisations have followed the Finnish Sprayer incident very closely, which has made it possible to compile remarkably accurate statistics. Some of this information is shown on the map on the facing page.

During March 1994, Finnish Sprayer was reported to have activated on approximately two hundred PCs in Finland alone. The total number of infected machines rises to several hundred, possibly even one thousand. This is quite amazing, since the virus was first found only a few months ago. Such new viruses are becoming increasingly common - for the ill-prepared PC user, the 'writing is on the wall'…

Finnish Sprayer

Aliases:	Aija.
Type:	Memory-resident boot sector virus.
Infection:	Hard disk Master Boot Sectors and floppy boot sectors.
Self-recognition in Memory:	None.
Self-recognition on Disk:	Letters 'Ai' at offset 45h in boot sector.
Hex pattern:	49B8 0103 33DB CD13 0E07 B801 0333 DBB9 0100 B600 CD13 5AC3
Intercepts:	Int 13h for stealth and infection.
Trigger:	Displays message and overwrites part of active partition on 25 March.
Removal:	Under clean system conditions, return original boot sector to its original place. Alternatively, overwrite viral code using the DOS command FDISK/MBR.