HS v3.2, Boot Virus detection and repair

Contents

1. What is HS?

HS.COM is a small program written to protect against boot viruses. It checks for differences in the boot sectors of your harddisk. It will catch almost any boot virus, notify you of the virus, and cold boot your machine after first having removed the virus. A copy of the infected boot sector is stored for later examination.

I wrote the program because I couldn't find the virus protection setup I wanted. My program executes in less than a second, and generates no output to the screen, as long as no virus is detected.

You will no longer waste your time with boot virus infections!

2. Why use this program?

A) Very fast

B) Easy to install

C) Catches almost any boot virus

D) Small (less than 4 Kb.)

E) Works with stealth viruses

F) Automatic removal of detected viruses

G) Do not need to be upgraded often

H) Inexpensive

3. Compatibility

HS supports:

PC's and PS/2's

DOS 3.2 > 6.0

DR-DOS 6.0

OS/2 2.0's Boot Manager

Windows NT's FlexBoot

(It will not work under OS/2 or Windows NT, but with their possibility of booting more than one operating system! Like DOS & NT or DOS & OS/2. So it is possible to use HS when booting DOS from these systems.)

4. Installation

1) Make sure your machine is virus free

2) Copy HS.COM to your harddisk

3) Run HS /M [Savefile]

Where Savefile is an optional filename for the file containing a copy of the original Master Boot Record and the DOS Boot Record of the active drive. Default name for the Savefile is C:\BOOT.HS

4) Insert a line like:

path\HS.COM [Filename]

near the top of your C:\AUTOEXEC.BAT

Or, if you have DOS 4 or newer, a line like:

Install=path\HS.COM [Filename]

in your C:\CONFIG.SYS

5) Run the path\HS.COM [Savefile] from the command line to check that everything works.

6) Reboot your machine to check that it boots without problems. This is especially important if you try to invoke HS.COM from your C:\CONFIG.SYS file. This will i.e. not work very well with DR-DOS 6.0!

7) If everything works smoothly, without any error messages, you are through with installing HS.

8) If there is a problem you can try to solve it by checking out the explanation of the error messages described later in this document, or you can contact me by E-Mail. See end of document.

5. Features

*) /M [Savefile]

The /M option have to be used the first time you run HS, and again each time you have repartioned your harddisk, or installed a new version of any operating system you are running on your computer. Like when you upgrade to a newer version of DOS.

*) When a difference in one of your boot sectors is found, HS will assume it is a boot virus. It will notify the user, and ask for a key press from the user as a confirmation that the user want to get rid of the virus. It will cold boot the machine after having removed the virus, as well as dumped the infected boot sector to the file C:\INF.HS.

*) At any time you can do a:

Type C:\INF.HS

to get information about past infections.

If no infections have occurred since HS was installed on the machine, no C:\INF.HS file will exist. The file contains a header with time & date of detection, and type of infector (MBR or DBR). Below the header are all the infected boot sectors stored (Max. 13).

*) If you reach 13 infections you will be asked to insert a write-enabled, and pre-formatted, diskette in drive a:, and the file C:\INF.HS will be copied to the diskette, and removed from your harddisk. A request, for you to send the diskette to me, will appear on the screen. Then your machine will cold boot after you have pressed a key. By sending me the diskette with the INF.HS file, I will have a greater chance of improving my program. However, most people will never reach 13 boot virus infections.

*) HS has only three components:

```
HS.COM              ; The program
BOOT.HS [Savefile]  ; Copy of the MBR/DBR
INF.HS              ; Dump of infected boot sectors
```

*) HS uses only direct calls to the ROM disk BIOS, and never interrupts, when reading the boot sectors on your harddisk. Because a virus can trap interrupts and trick programs requesting information about the contents of the sectors where the virus resides. Direct calls to "Read Only Memory" can't possibly be trapped by a virus, so HS should never be tricked by a stealth virus.

*) The Savefile (C:\BOOT.HS by default) will always be checked for validity, so if it is destroyed or tampered with, the user will be notified, and HS will not try to use it.

*) If you forgot to disable HS in your C:\CONFIG.SYS or C:\AUTOEXEC.BAT before you ran FDISK and made changes to the partition table, HS will ask you if you just repartioned your disk, and if you reply positive it will give you a chance to boot from a certified virus free system diskette and update the Savefile of HS by doing a HS/M [Savefile].

6. How good is HS?

HS v3.2 has successfully detected and removed all viruses I have tested it against. I don't have all known boot viruses (far from it!), so I can't claim a 100% detection, because it is not tested against all known viruses, on all possible machines, running all possible configurations. Also new viruses are created every day, so it is NOT possible to prove a 100% detection of all viruses or, in this case, 100% detection of all boot viruses. But I don't know of any boot virus that will not be successfully detected and removed by HS, and it should be quite difficult to write a virus that bypasses it. However, in theory, it is possible.

7. Error messages, and other messages from HS.COM

Unknown partition table format, aborting!

None of the four entries in the partition table is set active, making it a non-standard format which HS will not try to handle.

Unknown DOS boot record format, aborting!

No IO.SYS or IBMBIO.COM filename was found in the boot sector. These filenames are always present in MSDOS or PC-DOS boot sectors. If you use any other boot sector, as Windows NT's FlexBoot or OS/2 2.0's Boot Manager does, HS will try to make a valid Savefile anyway. This will fail if the double word at offset 1F8h in the boot sector is non-zero.

HS.COM v3.2

Check integrity of MBR & DBR using previously saved information.

Syntax: HS [/M] [Savefile]

Savefile	File containing copy of original MBR & DBR
/M	Make copy of MBR & DBR

This message appears on the screen if you type HS/? or similar
---

Error tracing BIOS entry point, probably VIRUS in memory
Incompatible DOS, HS will not run!

This message should only appear if you are infected by a virus, or if you are running some Control Access Packages (Like DiskSecure or SafeMBR). Try booting from a virus free system diskette and run HS /M [Savefile] again.

File not found!

HS can not find the Savefile you specified on the command line or in your CONFIG.SYS or AUTOEXEC.BAT.

Unable to read/write Savefile or C:\INF.HS, system unprotected!

Either HS is unable to create a valid Savefile or INF.HS file, or it is unable to read one of these files. Out of disk space may lead to such an error. Check if the files are on your harddisk and that they are available to HS.COM.

Read/Write error on harddisk, system unprotected!

A call to the BIOS disk routines (Int 13h) failed. This should never happen. It may indicate an harddisk error. Retry the command. If it still does not work you should get expert help.

Only Partition table in MBR has changed!
Did you just repartition your harddisk ? (Y/N)

If the partition table (Offset 1BEh-1FEh in the MBR) was the only area in the Master Boot Record to change, and Int 13h is not trapped, HS will assume that the user has done changes to the partition table. HS assumes you forgot to update the Savefile and will give you a chance to do it. If you have no knowledge of any such changes you should either reply NO or get help from a person with knowledge of system software and computer boot viruses.

Insert a certified virus free system diskette, cold boot with it,
and rescan the harddisk for any viruses. If no viruses are found
you can run HS /M and boot from the harddisk again.

Press any key to cold boot...

This message appears if you reply YES to the previous asked question.

?BR Infector
Press a key to clean up virus or
turn off your PC and get expert help!

A similar message will be shown on screen if HS finds that sector one of harddisk one (MBR), or the active partition's boot sector on that harddisk, has changed since the creation of the Savefile that was specified on the command line or, in your CONFIG.SYS or AUTOEXEC.BAT (C:\BOOT.HS if no Savefile was specified). This normally means that a boot virus has infected your machine and has been detected by HS. It will be removed when the user confirms this action by a single press of a key.

New copy of MBR and DBR made

After successfully creating HS's Savefile you should receive this message.

Savefile tampered with, system unprotected!

If the Savefile has been damaged or changed in any way you will get the message shown above.

Please insert a pre-formatted, write enabled, diskette in Drive A:

And press any key...

When you have had 13 boot sector infections on your machine, after HS was installed, it will ask you to insert a diskette so it can copy the C:\INF.HS file to the diskette (to A:\INF.13). The C:\INF.HS file will be deleted. It has reached its maximum size, and HS will create a new C:\INF.HS upon the next boot sector infection. If you wish to preserve the infection log contained in the C:\INF.HS file, which was moved to the A:\INF.13 file, you could do a TYPE A:\INF.13>Filename.Ext, or a TYPE A:\INF.13>PRN to get the report printed.

Please help us in the fight against viruses!

Send the diskette to:

Henrik Stroem
Stroem System Soft
Husebyveien 58c, 7078 Saupstad
Trondheim, Norway

Press any key...

For me to continue improving my program I need to study more viruses. It also helps to know which viruses are common, and where they have been detected. So by sending me the viruses you get infected by, you are helping me. Thanks!
---

8. Disclaimer, Licensing, Prices, Address

Disclaimer

The author takes no responsibility for unwanted effects from the use of HS.COM, or any of its components!

Licensing

This program is NOT freeware! However non-commercial users are free to use it on their home machine. This means that if you have one computer at work, and one computer at home, you may use HS to protect your home computer, without paying me anything, but you may not use HS on the computer you have at work. So in order to use HS on a computer owned by a company, the company have to buy a site-license! This site-license is reasonable priced and is valid for all computers owned by that particular company, department, institute or whatever. Upgrades can be obtained by FTP. If you want me to send you a diskette with the latest version, by mail, it will cost additional $20. This particular product does not depend on regular upgrades, because it is not signature-based. New versions will contain new features, and bug fixes if any bugs are found. The current site-licenses are valid for versions 3.x of HS. The major version number (currently 3) will change approximately every 12 months. If you have any questions you may contact me either by mail or E-Mail.

Prices

Non-commercial users	= Free
Single commercial user	= $15
Company with less than 10 machines	= $75
Company with less than 500 machines	= $175
Company with less than 1000 machines	= $350
Company with less than 2000 machines	= $700
Company with less than 4000 machines	= $1400
Company with more than 4000 machines	= Contact the author

All prices are in US dollars. Machine counts above 10 are approximate.
You receive an invoice upon ordering. The invoice is valid as a site-license when it has been paid.

Address

Henrik Stroem, Stroem System Soft
Husebyveien 58c, 7078 Saupstad
Trondheim, Norway
E-Mail: hstroem@flipper.pvv.unit.no