**What is a Boot Sector Virus?**



**What is a Boot Sector Virus? - Definition**

A boot sector virus is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks (some infect the boot sector of the hard disk instead of the MBR). The infected code runs when the system is booted from an infected disk, but once loaded it will infect other floppy disks when accessed in the infected computer. While boot sector viruses infect at a BIOS level, they use DOS commands to spread to other floppy disks. For this reason, they started to fade from the scene after the appearance of Windows 95 (which made little use of DOS instructions). Today, there are programs known as ‘bootkits’ that write their code to the MBR as a means of loading early in the boot process and then concealing the actions of malware running under Windows. However, they are not designed to infect removable media.

The only absolute criteria for a boot sector is that it must contain 0x55 and 0xAA as its last two bytes. If this signature is not present or is corrupted, the computer may display an error message and refuse to boot. Problems with the sector may be due to physical drive corruption or the presence of a boot sector virus.

**How Boot Sector Viruses are Spread and How to Get Rid of Them**

**Boot sector computer viruses are most commonly spread using physical media.** An infected floppy disk or USB drive connected to a computer will transfer when the drive's VBR is read, then modify or replace the existing boot code. The next time a user tries to boot their desktop, the virus will be loaded and run immediately as part of the master boot record. It's also possible for email attachments to contain boot virus code. If opened, these attachments infect the host computer and may contain instructions to send out further batches of email to a user's contact list. Improvements in BIOS architecture have reduced the spread of boot viruses by including an option to prevent any modification to the first sector of a computer's hard drive.

Removing a boot sector virus can be difficult because it may encrypt the boot sector. In many cases, users may not even be aware they have been infected with a virus until they run an antivirus protection program or [malware](https://usa.kaspersky.com/resource-center/definitions/boot-sector-virus) scan. As a result, it is critical for users to rely on continually updated virus protection programs that have a large registry of boot viruses and the data needed to safely remove them. If the virus cannot be removed due to [encryption](https://usa.kaspersky.com/resource-center/definitions/boot-sector-virus) or excessive damage to existing code, the hard drive may need reformatting to eliminate the infection.