No. 52, Mar 1998

THE COMPUTER CORNER

Is Windows 95 a Virus?

- by Stan Kaplan, WB9RQR
105 Martin Drive
Port Washington, WI 53074-9654
(414) 284-9346
WB9RQR @ N9PBY.EN63BI.WI.USA.NA
skaplan@mcw.edu

According to Robert Slade (Guide to Computer Viruses, 2nd ed., Springer, New York, 1996), a computer virus is:

> "an entity that uses the resources of the host to spread and reproduce itself without informed operator action"

and Slade emphasizes the word **informed**. Well, gals and guys, guess what? According to this definition, Windows 95 is a virus.

If you put a floppy disk in a Win95 machine and copy a file to it using the "Send To" function called up by a right click of the mouse button, it of course sends a copy to the floppy and thereby alters the file structure of the floppy with your consent. But get this: it also changes the boot sector of that floppy, without informing you of the fact and without your consent.

One of my favorite web sites is http://www.annoyances.org, where Win95 bugs and annoyances are published, along with fixes and work-arounds. While browsing this site in December 1997, I found one reference to behind-the-scenes altering of floppies inserted in a Windows 95 machine. I could not believe that Microsoft would build into its software an unauthorized change of the computer owner's floppies, so I did some experiments to see for myself. It is true!

Here is how I proved it. First, I examined the boot sector of 3½-inch HD floppies (1.44 Mb), which were either freshly formatted or brand new (Sony HD, IBM preformatted). Norton's DISK EDITOR was used to read and print the boot sectors. The disks that I prepared were formatted in several machines with different operating systems, as follows: MS-DOS 6.22, PC-DOS 7 (IBM), MS-DOS 7 (formatted from the DOS that Windows 95 sits on) and Windows 95 itself (formatted directly from My Computer on the Desktop). The following table shows just the OEM ID section (8 bytes long) of the boot sector of each disk (the rest of the boot sector is not relevant).

	NEW SONY	MS-DOS 6.22	PC-DOS 7	MS-DOS 7	WIN95
OEM ID:	IBM 3.3	MSDOS5.0	IBM 7.0	MSWIN4.0	)+W%=IHC

Then, I put a new Sony disk (with the OEM ID: IBM 3.3) into my Win95 machine and used the Send To function to copy a single file to it. Afterward, I examined the boot sector and found the following:

	NEW SONY
OEM ID:	(k")+IHC

Clearly, Win95 altered the boot sector. Just to confirm it, I put a PC-DOS 7 disk (the boot sector read IBM 7.0) into the Win95 machine and copied just one file to it. The boot sector then appeared thus:

	PC-DOS 7
OEM ID:	(ip!sIHC

Again, the boot sector was altered. However, when I exited from Win95 into the MS-DOS 7 operating system and used the COPY command to copy a file to a Sony disk, the boot sector was unchanged.

Win95 supposedly changes the boot sector to prepare the floppy in some way for long filenames. However, it does this even if the owner has not selected the long filename option, which is true in my case.

Well, so what if Win95 changes the boot sector without permission? Can it really make any difference? You bet it can. If you have boot disks from certain versions of MS-DOS or other operating systems (PC-DOS, DR-DOS) and you access them from Windows 95, it can make them unusable. Some copy-protected disks can be completely ruined by putting them in a Win95 machine. Indeed, any pre-Win95 software disk that inspects it's own validity can be ruined by accessing it in a Win95 machine. Beyond that, it also means that the distribution disks that come with any software you buy on floppies is altered the moment you use them for installation, without your informed consent, by your lovely new Win95 computer.

The answer? One approach is to write-protect any floppy you don't want altered before putting it in your Win95 computer. However, you should know that this step is not foolproof because some floppy drives (even new ones) have defective write-protect mechanisms, allowing them to ignore the write-protect tab. A better ploy is to avoid installing software from distribution disks. Use DISKCOPY to make copies of them, preferably in an older, non-Win95 machine. Then use the copies to install the software. However, even DISKCOPY in an MS-DOS 6.22 machine will alter the serial number of the copies. Use Norton's DUPEDISK for an absolutely perfect, byte for byte image copy of a disk. Even from MS-DOS 7 (the operating system under Win95), DUPEDISK will make a perfect copy, with not one byte altered from the original.

This is another incentive to set up your Windows 95 machine to routinely boot into MS-DOS 7, if for no other reason than to format disks (a format from MS-DOS 7 did not alter the boot sectors in my tests above). However, don't forget to create and edit a workable AUTOEXEC.BAT and CONFIG.SYS if you don't have them, so you can do more than just execute the FORMAT internal command. No. 39 in this series (Feb '97), HOW TO OPEN AND SHUT THE WINDOWS IN 95, gave details on the way to boot directly to DOS in your Windows 95 computer.

I think this is an astonishing finding, and if you are like me, you also resent the covert, unauthorized alteration of your floppy disks. We now need complete disclosure from Microsoft, including a complete explanation of what is coded in that altered OEM ID and how it is used.

Keep learning, keep aware and Happy Computing!