Computer Viruses on New Operating Systems: Windows 95, Windows NT and OS/2

Dr. Jan Hruska

Part # tr00087t/960518

Abstract

A large majority of viruses today are written for DOS running on IBM PCs and compatibles. The advent of new 32-bit operating systems and their eventual widespread use will have a major impact on the type of future viruses. This report discusses the impact of the current crop of about 8000 DOS viruses on the new operating systems, looks at the new cross-platform macro viruses and analyses some security implications of easy networking.

Introduction

In the last few years both Microsoft and IBM have been trying hard to bury DOS and introduce new, GUI-based 32-bit operating systems. Windows NT and Windows 95 from Microsoft as well as OS/2 and Warp from IBM are steadily taking over from DOS as the workstation operating systems, with the former organisation enjoying a somewhat bigger success. Unlike DOS, these operating systems (referred to as 'the new OSs') are relatively recent and the information on how to write programs for them is still hard to get. Furthermore, software development tools (especially for Microsoft operating systems) are much more expensive than software development tools for DOS. Lastly, writing software for 32-bit operating systems is simply more difficult than writing software for DOS, so it is not altogether surprising that system-specific viruses for the new OSs are still rare.

New OSs system-specific virus count on 1st May 1996:

• OS/2:	3
• Windows 95:	1
• Windows NT:	0

Most of the existing viruses are DOS viruses and with the exception of the latest macro viruses such as WinWord.Concept, it is the DOS viruses which will be causing problems in the near future.

What are the virus-related problems in new OSs?

Problem 1: Carrying the DOS baggage

New OSs are all capable of executing 32-bit applications, but at the moment there are relatively few 32-bit applications in existence. To solve this problem, all three of them support not only 16-bit applications, but also DOS applications. Not even Microsoft has dared to deprive the users of the hated DOS command line box.

The emulation of DOS functions provided by the new OSs is rather good, so that a large majority of existing DOS applications will run happily. Herein lies the first problem, since the set of applications which will execute includes most viruses. Any virus which does not attempt to reach too deep into the operating system and trigger the security features provided by the new OSs, will replicate and probably successfully execute its payload.

Trials conducted by Virus Bulletin show that under Windows 95, Jerusalem, for example, replicates without any difficulty in the DOS box, infecting files as they are executed, but does not, unsurprisingly, infect Windows 95 executables correctly. Furthermore, when Windows 95 is booted from an infected disk, it will continue to work correctly. If 16-bit disk access is selected, most boot sector viruses will spread to other floppy disks, while when 32-bit access is selected, the viruses will not spread.[3]

Similar results for replication of parasitic viruses in the command line box under Windows NT and OS/2 have been reported by Fred Cohen.[5]

The current crop (Fig. 1) of some 7500 parasitic DOS viruses as well as some 400 multi-partite DOS viruses (while replicating parasitically) will continue to plague the new OSs, sometimes causing damage by executing their payload, sometimes causing damage while trying to infect and sometimes stealing resources by replicating across networks.

Problem 2: Non-standard disk layout

A large majority of infections by viruses in-the-wild (about 80%, Fig. 2) are due to viruses which are capable of infecting the boot sector (boot sector viruses and multi-partite viruses). The infection happens when the PC is (accidentally) bootstrapped from an infected floppy disk. The disk does not have to be a system disk in order for the virus to infect the PC.

It is important to note that the virus executes before the operating system on the hard disk which means that the virus is free to write to the hard disk unhindered. The virus loads into memory and using BIOS calls attempts to infect either the master boot sector or the DOS boot sector on the hard disk, depending on the virus type. In most cases, the virus will also try to grab some more space on the disk in order to store the rest of its code as well as the original boot sector. Virus writers have adopted different strategies on where to find this extra space, ranging from using absolute sectors 2 onwards on track 0, head 0 of the hard disk (New Zealand, Joshi etc.) to simply assuming that the last two sectors on the disk will not be used (Form).

The problem lies in the fact that the virus' idea of what areas on the disk are free on a PC running DOS does not correspond with the actual situation on a PC with one of the new OSs installed. The result, of course, is a muddle, with either the virus overwriting a part of the operating system or the operating system overwriting a part of the virus. The former causes data corruption while the latter causes the system to become unbootable and can cause data corruption. Windows NT for example, uses the space on track 0 head 0 (which is free on DOS-based PCs) and the infection by almost all boot sector viruses will render the system unbootable at best and irreparably damaged at worst.

Should the operating system manage to boot after the virus has gone memory-resident, the virus will almost certainly not be able to spread further and infect other floppy disks. Windows 95 is an exception if 16-bit disk access is used. The majority of DOS boot viruses effectively become non-replicating damaging Trojan horses as far as the new OSs are concerned. Their lifecycle stops after they have (probably) caused damage.

Viruses such as Form which look for and infect the active partition DOS boot sector on the hard disk cause particular problems with the OS/2 boot manager. This is effectively an active partition on its own, without either having the structure of a normal DOS partition or appearing as a logical drive after booting. Form will happily infect this partition, will not replicate to other floppies, but the detection and removal of the virus has to be done by addressing the disk at absolute sector level, not logical.

Multi-partite viruses in a boot sector will infect PCs and cause similar problems to boot sector viruses, but will probably not replicate further. However, if

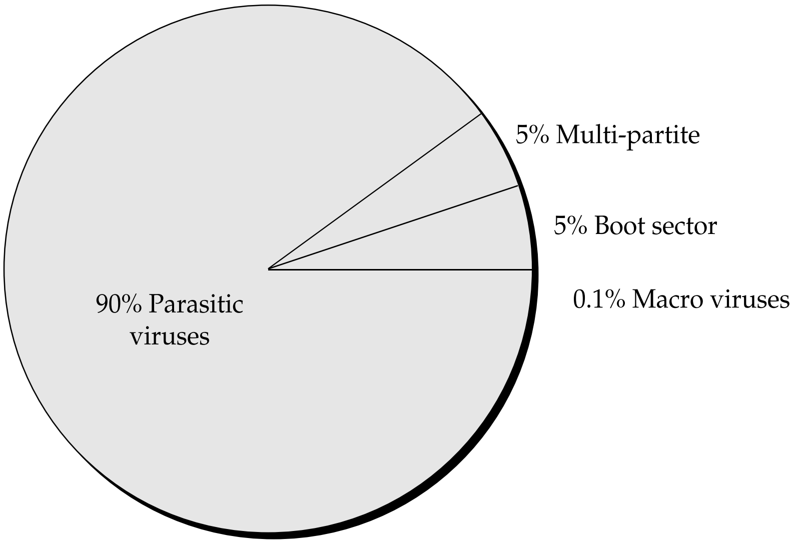

Fig. 1: Known viruses by type, May 96

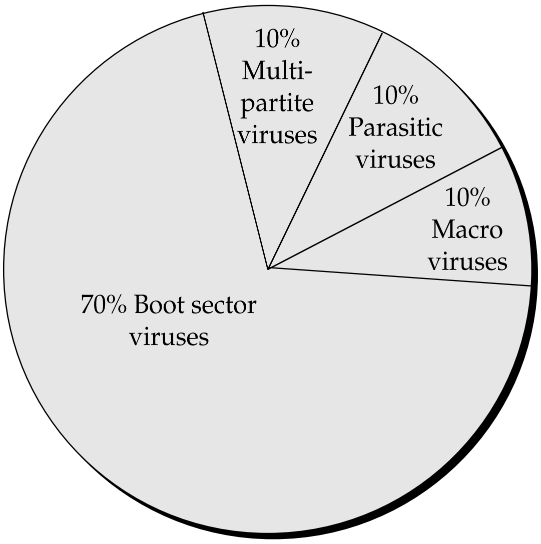

Fig. 2: Virus infections in the wild, May 96

they infect the PC while carried in a program file, they will probably succeed in replicating to other DOS executables, while the infection of the master boot sector and the DOS boot sector will be prevented by the security provided by the new OSs.

What can be done to minimise the likelihood of damage to new OSs from viruses with a boot sector component? The main defence is simple, almost free and grossly neglected by PC users: turn off the floppy boot in the PC setup.

No floppy boot=No boot virus problems

This facility is available under most modern BIOSs, but the keystrokes to execute setup after booting vary between systems. On modern Compaqs, for example, F10 after reboot will run setup and the option to check is 'Disable floppy disk drive boot ability' in the 'Security options'. Note that this is a fundamentally secure facility, unlike the 'Prevent hard disk boot sector writing' option offered by some manufacturers as a measure against boot sector viruses.

The clean booting of machines protected with this simple measure is still possible (execute setup, cancel the option and reboot).

Problem 3: Good connectivity

One of the main features of the new OSs is the ease with which computers can be linked together and share resources. Point and click and you could just as easily be sharing information with a person in another country as with a person sitting next to you.

It should come as no surprise that this great benefit opens up a security loophole in a very similar way that the spread of infectious diseases such as Aids has been greatly enabled by fast and frequent travel. Of course, today's modern medicine has more than compensated for this, preventing massive epidemics of the middle ages by clinical means. Nevertheless, when confronted with an incurable and deadly biological virus such as Ebola, the best epidemic control is isolation and curtailment of travel to and from infected areas.

The virus spread over expanding networks of the future will be fast and we can expect large numbers of PCs to be affected in each outbreak. At the Virus Bulletin conference 1995 in Boston in September a show of hands has indicated not only that a large number of organisations in the US were affected by the WinWord.Concept virus (between 5% and 10% of participants had had infected computers), but also that the number of PC in an average infection was much higher than the number of PCs infected during a normal parasitic or boot sector virus. The virus also reached them very fast (it was reputedly created in July 95).

There are a number of reasons why this was the case. Firstly, virus scanners did not (do not?) check all files for reasons of speed, and even if they did, most did not recognise WinWord.Concept at that time. Secondly, the virus spreads in Word template files which were considered by most users as non-executable and incapable of carrying viruses. Thirdly, the virus has been incorporated on at least three high-circulation CDs. Fourthly, and probably most significantly, Word templates and documents saved as templates are widely distributed and shared over networks within organisations. The average number of infected machines per organisation is usually in the hundreds.

Problem 4: Cross-platform application compatibility

One of the major benefits of the so called open systems is the ease with which documents and applications can be moved between different operating systems running on different hardware. This, unfortunately, conceals a major security loophole which provides virus authors with wonderful new and exciting opportunities.

WinWord.Concept[1,6] was the first virus encountered in the wild which exploited this. It relies on the fact that the structure of Microsoft Word documents is identical under Windows, Windows 95, Windows NT and Macintoshes. Word has its own programming language, WordBasic, which allows easy definition of macro sequences. The AutoOpen macro is executed transparently whenever a document is opened by Word and provides the means of infecting the environment as well as spreading the virus.

The virus replicates under all operating systems and hardware which run the English version of Microsoft Word versions 6 and 7. WinWord.Concept is the first example of a PC virus encountered in the wild which is capable of operating on different hardware and different operating systems.

The concept of macro viruses can be ‘ported’ to other applications as long as they support a reasonably powerful macro language. The technique of using macros to write viruses is not new (it was first predicted by Prof. Harold Highland in 1989 using Lotus 1-2-3 as an example) but it is surprising that it took the virus-writing community so long to recognise its full potential and release the first macro virus into the wild.

The future

Increased popularity of new OSs will invariably bring wider availability of development information which will trickle down to the virus-writing underworld. It is only a matter of time before viruses written for the new OSs start to appear in quantities similar to DOS viruses. The question is not ‘whether’ but ‘when’.

Conclusions

New OSs are only marginally less vulnerable to viruses than DOS. It will take time before system-specific viruses reach the glut levels currently observed in DOS viruses. The main barrier at the moment seems to be the relative difficulty in getting information about various operating system internals as well as the relatively high price of development tools.

Good DOS emulation offered by the new OSs provides a fertile breeding ground for parasitic and multi-partite DOS viruses in DOS boxes. DOS viruses with a boot sector component do not replicate in most circumstances under new OSs but often have catastrophic effect on them due to a non-DOS disk structure. Disabling the booting from floppy drives is a simple, but often ignored measure against such damage.

Easier connectivity and wide use of networks facilitates the spread of viruses. Cross-platform viruses such as WinWord.Concept have made virus scanning more difficult and time-consuming, while virus-writing is now accessible to anybody capable of pointing and clicking the mouse.

Bibliography

1. What a (Winword.)Concept, Sarah Gordon, Virus Bulletin, September 1995

2. Windows 95 virus, Underground Technology Review, American Eagle Publishing

3. Windows 95: Even Better than the Real Thing?, Virus Bulletin, October 1995

4. Viruses on Windows NT, Ian Whalley, Virus Bulletin, March 1995

5. Why 32-Bit Desktops Need Virus Protection, Fred Cohen, Datamation, 15 July 1995

6. Macro Viruses and Viruses in Microsoft Word, Paul Ducklin, Sophos Technical Report, March 96