Computer Viruses - The Breadth of the Problem

Karen Richardson, Sophos Plc, Oxford, England

Part # tr00004p/940301

Karen Richardson is the Marketing Manager for Sophos Plc, a software house specialising in computer security. Sophos is the UK's leading supplier of anti-virus software, training and consultancy.

1. Introduction

Information technology systems are increasingly being threatened by computer viruses. Too few people contemplate the potentially disastrous effects of the disruption to their computer systems caused by a virus attack.

Personal Computers (PCs) are particularly vulnerable to virus attacks, because the programs on PCs are relatively unprotected. A number of specific viruses have become well-known, including *Brain*, *New Zealand*, *Jerusalem* (Friday 13th, 1813), *Cascade* (1701, 1704), *Datacrime*, the *4K* virus and others. The number of viruses is currently increasing at a rate of about 2 per day.

2. Virus side-effects

Virus side-effects (or the virus 'payload') are normally the first contact between the infected user and the virus. Not surprisingly, they are also the part which is most interesting for the majority of users.

They are normally the easiest part of the virus to program. They are also the easiest part to change. There have been several examples of mutated viruses which had their side-effects completely changed from the original (e.g. *Cascade-format* and *Cascade*).

Virus side-effects range from annoyance (such as the bouncing ball in the *Italian*), data modification (like the *dBASE* virus) to data destruction (*Michelangelo* virus). The side-effects are completely open to the imagination of the programmer.

When the first viruses appeared, their side-effects were on the whole confined to annoyance, which prompted several people to treat **all** viruses as innocuous, and as dangerous as a pet cat.

Unfortunately, recent viruses are more like hungry tigers; fine behind bars in a zoo, but rather less so in the wild.

3. Virus carriers

Any medium which can be used for transmission of executables is a potential carrier of **parasitic viruses**. Any medium which can be used to bootstrap the PC can also be used to carry **bootstrap sector viruses**. **Multi-partite viruses** can be carried on any medium which can carry parasitic or bootstrap sector viruses.

The PC becomes infected with a **parasitic virus** when the user executes an infected program. The system becomes infected with a **bootstrap sector virus** when bootstrapped from an infected medium. **Multi-partite viruses** infect either when the PC is bootstrapped from an infected medium or when an infected program is executed.

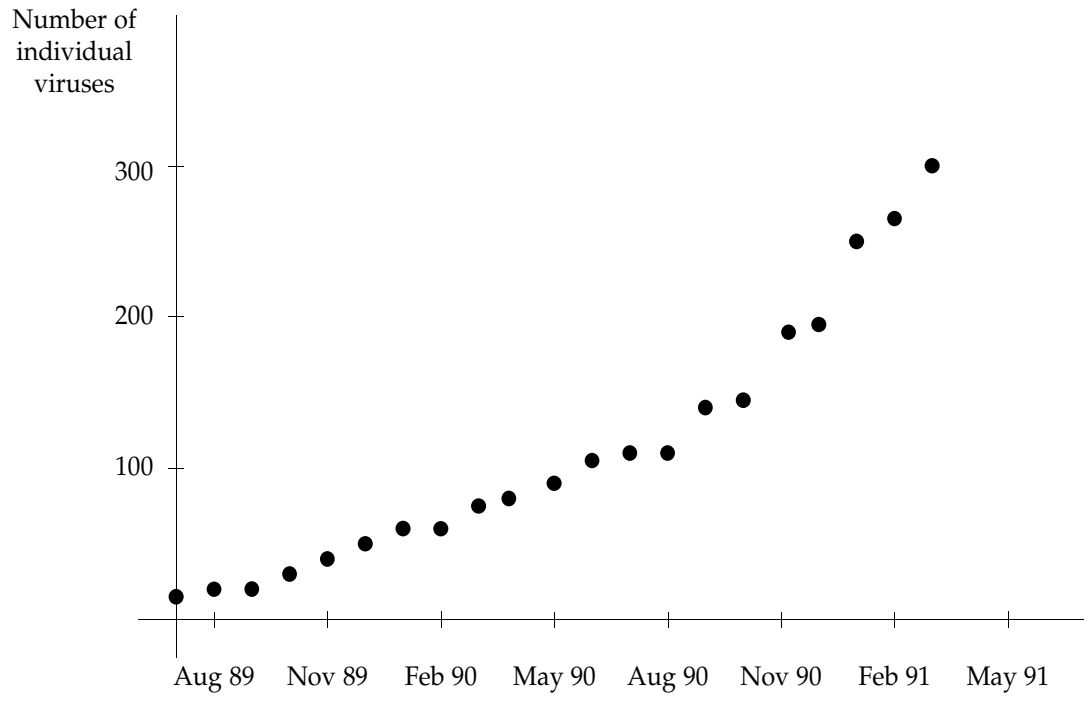
As a rule, if the medium can be used to bootstrap the PC, it should be considered capable of carrying bootstrap sector viruses and multi-partite viruses, as well as parasitic viruses. If the medium cannot be used to bootstrap the PC, it can only carry parasitic viruses and multi-partite viruses.

4. Virus infiltration rules and methods

Some user actions have been shown to carry a high risk of spreading viruses. The following list of routes and methods of virus infiltration has been assembled by analysing real-life cases in which organisations and individuals became infected.

4.1 Pirated software

It is easy to copy software and in most countries it is illegal to do so. Games are probably the most commonly pirated software and they tend to move between PC users at a far greater speed than 'serious' pirated software. For this reason, they are also most prone to picking up a parasitic virus on the way.



Growth in the number of separately identifiable viruses in the early days

4.2 Bulletin boards

Bulletin boards normally provide the means of downloading and uploading software which is classified either as 'public domain' (free for all) or 'shareware' (copy freely, but pay if you use it). Most reputable boards are run under the close supervision of the SYSOP, the SYStem OPerator, who is at great pains to ensure the integrity of the software available from the bulletin board. Unfortunately, it is almost impossible to analyse all traffic on a bulletin board and, hence, bulletin boards carry a risk of virus propagation.

4.3 Shareware

Shareware is an attractive concept developed in the USA. The software carries the traditional copyright, but anybody is encouraged to copy it and pass it on to others. If anybody ends up using it, he is under moral obligation to send a small sum (usually $20 to $50) to the author. Unfortunately, shareware distribution is not without problems. Although most authors send 'the latest version' once payment has been received, users end up trying (and using) the original version obtained from a friend of a friend of a friend. By the time one receives 'the latest version', the computer may be infected many times over with any viruses the original software picked up on the way.

4.4 Floppy disks supplied with magazines

Some computer magazines supply floppy disks containing free software with every issue. On a number of occasions the disks were found to carry complete viruses or sections of virus code:

- Personal Computing Vol. 3 No. 1, *Database Publications*, March 1990, *New Zealand* mutation, unknown number of copies
- PC Today Vol. 4 No 4, D*atabase Publications*, August 1990, *Disk Killer* (inactive), 40,000 copies
- PC-WORLD Benelux, 9th November 1990, *IDG Communications*, *Cascade*, 16,000 copies

Virus risks associated with this form of software distribution are similar to shareware.

4.5 Public domain software

Unlike shareware, public domain software is completely free for anybody to use. Unfortunately, it suffers from the same distribution risks as shareware, with the added disadvantage that there is often nobody to supply 'the latest version'.

4.6 Shared PCs (PC at home)

A surprisingly large number of infections in business PCs occur through the use of home

computers for company work. In one case an executive's 14-year old son used his father's home PC to play games downloaded from bulletin boards (unbeknown to his father). The executive, having brought home a report to finish, unwittingly took an infected disk back to work the next morning and in turn, infected his office PCs with the *New Zealand* virus.

4.7 Service engineers

A lot can be done to prevent viruses from infiltrating organisations through this route. All diagnostic disks used by service engineers should be write-protected, or, even better, the customer should have a set of his own write-protected disks.

At least one large computer company has expressly prohibited its service engineers from carrying any floppy disks. All disks used on the customers' PCs, including diagnostics, must be supplied by the customer or come shrink-wrapped from the factory.

4.8 Shrink-wrapped software

Shrink-wrapped software normally refers to commercial software packages which come in a shrink-wrapped sealed container - usually for legislative purposes rather than anti-virus measures. By breaking the seal, the user implicitly agrees to abide by the manufacturer's terms and conditions. There is also a good chance that the software has not been tampered with from the time it left the manufacturing plant.

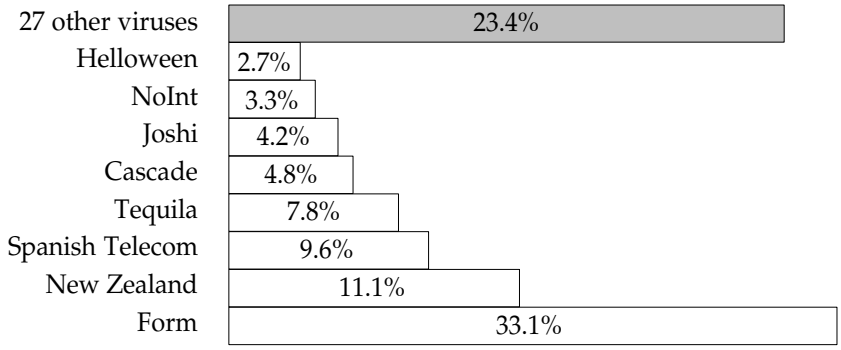
There have been a few cases of shrink-wrapped software containing viruses (mainly on floppy disks supplied with hardware originating from Taiwan). Major software companies operate stringent QA (Quality Assurance) procedures in order to prevent virus propagation into production software. Although there is always a chance that shrink-wrapped software may contain a virus, the probability, in practice, is extremely small.

5. Viruses and networks

Simple networks normally allow several users to access the central file server, which is treated as a big shared disk. Anybody can write to it and access any directory. Such systems offer no security in general, as well as no security against viruses. If a user's PC becomes infected with a parasitic virus and the user executes a program residing on the file server, the program on the file server will become contaminated. Any other user executing that program from then on will infect his own PC.

Few networks in use today are as primitive as that. Most offer some degree of protection against writing to designated areas, such as the directory containing executables. Some of the best security features at present are offered by *Novell NetWare* which provides four different aspects of network security: the **login procedure**, **trustee rights**, **directory rights** and **file attributes**.

- The **login procedure** requires all users to identify themselves by a username and a password.
- **Trustee rights** are granted to each user by the 'network supervisor' and allow each user various actions such as reading from files, writing to files, creating files, searching directories etc.
- **Directory rights** (read, write, open, close, delete) are set separately and can be used to limit the access to certain directories such as those containing executables.



Virus reports from 1st January 1993 to 30th June 1993 (332 reports)

- **File Attributes** (read-only, read-write, share) can be set separately.

This means that even if a user's PC becomes infected, the infection cannot spread to the file server. This security **does** break down if the network supervisor's PC becomes infected. **Care should be taken to use network security features, as they may not be enabled by default.**

6. Virus numbers and types

In October 1993 there were some 3200 different viruses in existence. New viruses are currently appearing at the rate of 2 per day (Fig. 1). It is interesting that despite the large numbers of viruses known to researchers, about 75% of all reported infections are due to 8 viruses, and of which more than a third are due to only one virus (*Form*) (Fig. 2).

7. Future trends in virus writing

It is extremely difficult to predict the trends in virus-writing popularity and the style and methods used by future viruses. Some of the best researchers in the field have had to swallow predictions which they made only months before.

It is likely that the popularity of virus writing will increase, as the techniques become better known. The avalanche started by the publication of Ralf Burger's book 'Computer Viruses - A High Tech Disease' is continuing and a number of bulletin boards carry 'hackable' virus source code. The number of individual viruses has been approximately doubling every 6 months for the last two years and this is likely to continue for some time before saturating.

More and more stealth viruses which are difficult if not impossible to detect by using scanning anti-virus software, will undoubtedly appear. Sparse infection and non-recognition of files already infected will be combined to produce viruses undetectable by scanning software.

It is somewhat easier to speculate about the side-effects of future viruses. Virus side-effects can be divided into four categories:

- Innocuous effects
- Data destruction
- Data modification
- Security breaches

It is almost certain that side-effects which emulate suicide (such as disk formatting in *Datacrime*) will remain comparatively rare, since virus potential for spreading terminates with the activation of the side effects.

Data modification is much more likely to remain the predominant side effect of viruses in the future. Gradual corruption of the FAT (as in *Nomenklatura*) closely resembles a bug in application software or an intermittent disk failure. It is unlikely to be attributed to a virus, which is thereby given a much longer period to multiply and spread before being 'caught'.

A number of viruses do not have any side-effects whatsoever (apart from replication). They are probably research platforms for studying the speed of multiplication in the wild and the virus potential for carrying a much more lethal cargo in the future.

Whereas the number of viruses and the analysis of their structure may be of academic interest, the number of *actual infections* is much more important from the practical point of view. Firm data on the number of infections is difficult to collect for a variety of reasons which range from the unwelcome publicity, to the absence of an international reporting or report-consolidating organisation. The *Computer Crime Unit* of the *New Scotland Yard* in London (Tel. 071 230 1177) started collecting virus attack reports in March 1991, with the aim of producing reliable statistics about the extent of the virus problem.

Viruses have nothing to fear. Their future is assured.