Computer viruses demystified

Carole Theriault, Technical Author, Sophos Plc
First published: October 1999

SUMMARY

Despite our awareness of computer viruses, how many of us can define what one is, or how it infects computers? This paper aims to demystify the basics of computer viruses, summarising what they are, how they attack and what we can do to protect ourselves against them.

Introduction

In the mid-eighties, so legend has it, the Amjad brothers of Pakistan ran a computer store. Frustrated by computer piracy, they wrote the first computer virus, a boot sector virus called Brain. From those simple beginnings, an entire counter-culture industry of virus creation and distribution emerged, leaving us today with several tens of thousands of viruses.

Many people believe the worst a virus can do is format your hard disk. In fact, this type of payload is now harmless for those of us who back up our important data. Much more destructive viruses are those which subtly corrupt data.

In just over a decade, most of us have been familiar with the term computer virus. Even those of us who don't know how to use a computer have heard about viruses through Hollywood films such as *Independence Day* or *Hackers* (though Hollywood's depiction of viruses is usually highly inaccurate). International magazines and newspapers regularly have virus-scares as leading stories. There is no doubt that our culture is fascinated by the potential danger of these viruses.

Many people believe the worst a virus can do is format your hard disk. In fact, this type of payload is now harmless for those of us who back up our important data. Much more destructive viruses are those which subtly corrupt data. Consider, for example, the effects of a virus that randomly changes numbers in spreadsheet applications by plus or minus 10% at a stockbrokers. Other nasty viruses post company confidential documents in your own name to some of the alt.sex internet newsgroups, an act which can both ruin your reputation and the company's confidentiality.

Despite our awareness of computer viruses, how many of us can define what one is, or how it infects computers? This paper aims to demystify the basics of computer viruses, summarising what they are, how they attack and what we can do to protect ourselves against them.

What is a computer virus?

The difference between a computer virus and other programs is that viruses are designed to self-replicate (that is to say, make copies of themselves). They usually self-replicate without the knowledge of the user. Viruses often contain 'payloads', actions that the virus carries out separately from replication. Payloads can vary from the annoying (for example, the WM97/Class-D virus, which repeatedly displays messages such as "I think 'username' is a big stupid jerk"), to the disastrous (for example, the CIH virus, which attempts to overwrite the Flash BIOS, which can cause irreparable damage to certain machines).

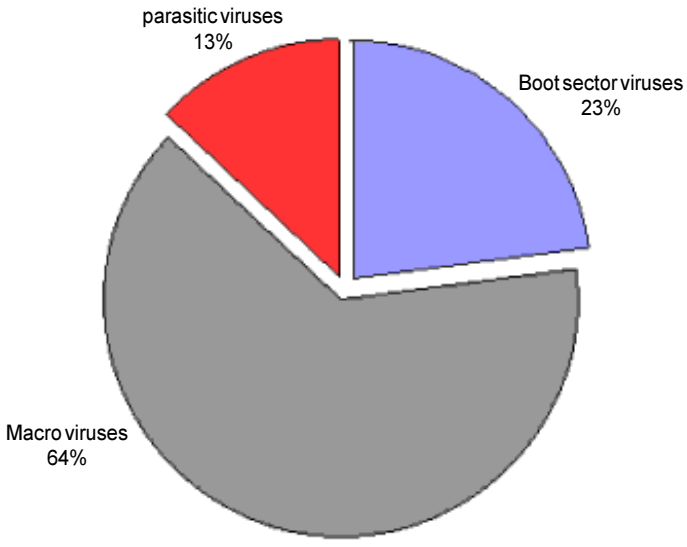
Example of WM97/Class-D virus payload

Viruses can be hidden in programs available on floppy disks or CDs, hidden in email attachments or in material downloaded from the web. If the virus has no obvious payload, a user without anti-virus software may not even be aware that a computer is infected.

A computer that has an active copy of a virus on its machine is considered infected. The way in which a virus becomes active depends on how the virus has been designed, e.g. macro viruses can become active if the user simply opens, closes or saves an infected document.

How infection occurs

Once the virus is active on the computer, it can copy itself to (infect) other files or disks as they are accessed by the user. Different types of viruses infect computers in particular ways; the most widespread types are Macro, Boot and Parasitic viruses.



Sophos Plc virus classification statistics (September 1999)

Macro viruses

Macro viruses are macros that self-replicate. If a user accesses a document containing a viral macro and unwittingly executes this macro virus, it can then copy itself into that application's startup files.

A macro is an instruction that carries out program commands automatically. Many common applications (e.g. word processing, spreadsheet, and slide presentation applications) make use of macros. Macro viruses are macros that self-replicate. If a user accesses a document containing a viral macro and unwittingly executes this macro virus, it can then copy itself into that application's startup files. The computer is now infected—a copy of the macro virus resides on the machine.

Any document on that machine that uses the same application can then become infected. If the infected computer is on a network, the infection is likely to spread

rapidly to other machines on the network. Moreover, if a copy of an infected file is passed to anyone else (for example, by email or floppy disk), the virus can spread to the recipient's computer. This process of infection will end only when the virus is noticed and all viral macros are eradicated.

Macro viruses are the most common type of viruses. Many popular modern applications allow macros. Macro viruses can be written with very little specialist knowledge, and these viruses can spread to any platform on which the application is running. However, the main reason for their 'success' is that documents are exchanged far more frequently than executables or disks, a direct result of email's popularity and web use.

Boot sector viruses

The boot sector is the first software loaded onto your computer. This program resides on a disk, and this disk can be either the hard disk inside the computer, a floppy disk or a CD. When a computer is switched on, the hardware automatically locates and runs the boot sector program. This program then loads the rest of the operating system into memory. Without a boot sector, a computer cannot run software.

A boot sector virus infects computers by modifying the contents of the boot sector program. It replaces the legitimate contents with its own infected version.

A boot sector virus infects computers by modifying the contents of the boot sector program. It replaces the legitimate contents with its own infected version. A boot sector virus can only infect a machine if it is used to boot-up your computer, e.g. if you start your computer by using a floppy disk with an infected boot sector, your computer is likely to be infected. A boot sector cannot infect a computer if it is introduced after the machine is running the operating system.

An example of a boot sector virus is Parity Boot. This virus's payload displays the message `PARITY CHECK` and freezes the operating system, rendering the computer useless. This virus message is taken from an actual error message which is displayed to users when a computer's memory is faulty. As a result, a user whose computer is infected with the Parity Boot virus is led to believe that the machine has a memory fault rather than an disruptive virus infection.

Parasitic viruses

The parasitic virus, because the operating system understands it to be part of the program, is given the same rights as the program to which the virus is attached.

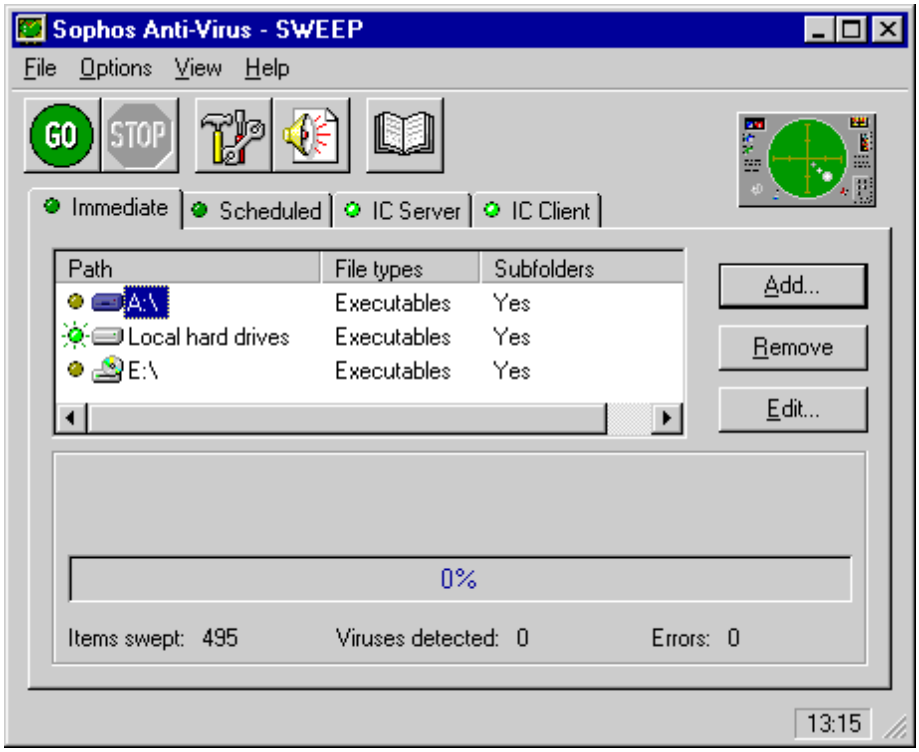
Parasitic viruses attach themselves to programs, also known as executables. When a user launches a program that has a parasitic virus, the virus is surreptitiously launched first. To cloak its presence from the user, the virus then triggers the original program to open.

The parasitic virus, because the operating system understands it to be part of the program, is given the same rights as the program to which the virus is attached. These rights allow the virus to replicate, install itself into memory, or release its payload. In the absence of anti-virus software, only the payload might raise the normal user's suspicions. A famous parasitic virus called Jerusalem has a payload of slowing down the system and eventually deleting every program the user launches.

Prevention

The best way for users to protect themselves against viruses is to apply the following anti-virus measures:

- Make backups of all software (including operating systems), so if a virus attack has been made, you can retrieve safe copies of your files and software.
- Inform all users that the risk of infection grows exponentially when people exchange floppy disks, download web material or open email attachments without caution.
- Have anti-virus (AV) software installed and updated regularly to detect, report and (where appropriate) disinfect viruses.



Sophos Anti-Virus Windows interface

- If in doubt about a suspicious item that your AV software does not recognise, contact your anti-virus team immediately for analysis.

SOPHOS

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • UK
Tel +44 01235 559933 • Fax +44 01235 559935

www.sophos.com