

Viruses: What you need to know

Author: Rachael Johnson

Version 2, January 2003

The virus threat is more widely publicised now than ever before and as a result, computer users are largely more aware of the risk and potential implications of a virus infection. However, it is one thing to be aware of the threat; quite another to ensure that your systems are adequately protected.

This guide is intended to

- provide some basic information about viruses,
- outline the central protection mechanisms employed by Computer Services, and
- tell you what you can do to ensure that you are not the weak link in the chain.

1. What is a virus?

A computer **virus** is a self-replicating program, which attaches itself to, or “infects” other programs (by overwriting or modifying them) in order to reproduce itself, undetected, to adversely affect the operation of a computer. Many viruses are relatively harmless and may be present for years with no noticeable effect; others attempt to destroy files and render disks useless. Even the most benign of viruses can cause significant problems in terms of disk and memory space occupied, as well as the waste of time and effort in detecting and removing them. Generally speaking, in order for a virus to become active and to spread, the program to which the virus is attached must be launched. However, there are increasing numbers of viruses (Trojan horses in particular) which exploit vulnerabilities in web browsing and other software, in order to copy and execute themselves on a computer with no user intervention required.

Some viruses are described as **Trojan Horses**; that is, files that claim to perform a useful legitimate function but which also contains malicious, destructive code. In one sense, all viruses are Trojan Horses, since they act by attaching themselves to a useful program. The key difference between the two is that a Trojan Horse does not reproduce, therefore must be spread intentionally.

There is a third type of virus, known as a **worm**. Virus-like in its action, the chief difference with the worm is that it is designed to propagate itself across networks, rather than depending upon user behaviour to allow it to spread further than the user’s machine. Sircam is a good example of a worm, as is Bugbear:

<www.sophos.com/virusinfo/analyses/w32bugbeara.html>

Worms pose an increasingly common threat to computer systems, as can be seen from the Sophos Top 10 latest virus threats statistics:

<www.gold.ac.uk/infos/cs/anti-virus/>

2. Types of virus

2.1 Boot sector virus

A boot sector virus is stored in the boot sector of hard disks and floppy disks, this type of virus loads into memory when the PC is switched on or booted from an infected floppy. A common example is the *Anticmos* virus:

<www.sophos.com/virusinfo/analyses/anticmos.html>

2.2 File or parasitic virus

A file virus attaches itself to executable files in DOS or Windows and infects other executables. Some, such as the Win95_CIH virus, become memory-resident and affect other programs as they are run. An example of an executable file virus is FunLove:

<www.sophos.com/virusinfo/analyses/w32flcss.html>

These types of viruses often spread as email attachments. The AMAViS email scanning software operated by the Computer Services stops many of these viruses from entering College email every day:

<www.gold.ac.uk/infos/cs/tools/virus.php>

2.3 Macro virus

Macro viruses infect a machine when a file containing the infected macro (commonly a Word or Excel file) is opened. An example of a Word macro virus is *Replug-F*:

<www.sophos.com/virusinfo/analyses/wm97replugf.html>

Find out more about macro viruses and precautions to take, in our separate section dedicated to the subject.

2.4 E-mail “virus”

This is a misnomer used to describe the “chain mail” and hoax virus phenomena, which urges the user to forward the message to as many people as possible. It is not a virus, in that it does not replicate itself, but it is responsible for concern on the part of the user, time-wasting and unnecessary use of bandwidth. Hoaxes also fall into this category. One of the most successful hoaxes in recent times is *jdbgmgr.exe*:

<<http://www.sophos.com/virusinfo/hoaxes/jdbgmgr.html>>

3. How does my computer become infected?

A computer may become infected by a virus in the following instances:

- Receiving an e-mail with an infected file attached, which you download to your computer **and run**.
- Downloading an infected file from the Internet **and running it**.
- File sharing of infected files on computer networks or floppy disks
- Booting a computer with an infected boot disk.
- Browsing affected Internet sites using old, vulnerable browser software

Increasingly we are faced with the threat of “malware” (i.e. malicious code) disguised in files other than executable files or macros, such as html and related extensions. The types of files which need to be incorporated into daily scans are now much more numerous.

4. How do viruses work?

A virus attaches itself to a file, usually an executable application. Viruses don't generally directly attack data files, although data files can contain embedded executable code such as macros, which are very susceptible to attack. Microsoft Word and Excel files sent as e-mail attachments or shared on departmental drives should therefore be treated with as much caution as an executable program downloaded from the Internet, regardless of the identity of the originator.

Viruses are usually operating system-specific. For example, a virus such as WIN95_CIH is specific to Windows 9x PCs, *except* in the following circumstances:

1. A Word document (or Microsoft Excel spreadsheet) infected with a macro virus can affect your Word documents on both PC and Mac systems. Some macro viruses are known to infect both Windows 9x and Windows 3.x systems.
2. If you are running PC emulation software on a Mac for Windows 95 emulation, such as Soft PC or Virtual PC, any software running under this emulation is vulnerable to Windows 95 virus attack.

For further information on viruses in relation to Macintosh systems, visit:

<www.sophos.com/support/faqs/savmac.html>

It is impossible to generalise further about how viruses work, as their actions are so varied; some merely display text messages on launch, while others attempt to rewrite the machine's BIOS and thus render the machine useless. For further information on virus definitions, see <www.sophos.com/virusinfo/>

5. How do I tell a virus hoax from a genuine threat?

Hoaxes generally take the form of warnings circulated by e-mail, which typically warn of dire consequences if you do not follow the circulated instructions, and where the recipient is urged to forward the news to everyone they know. Viruses cannot generally infect plain text files (such as e-mail): the real risk is involved in downloading an infected file attachment. The chances are that e-mails of this type are hoaxes, but how do you differentiate between a hoax and a potential threat?

What do I do if I receive a virus warning?

1. DON'T forward it to everyone you know. This is annoying and largely pointless; the only outcome being unnecessary scare-mongering and use of bandwidth.
2. Check out any of the huge number of comprehensive, on line hoax listings available on the Internet, for example:
<www.sophos.com/virusinfo/hoaxes/>
<www.kumite.com/myths/>
3. If you cannot find any reference to the named suspect file in question, look at the Sophos website for further information. If you find that there is an e-mail in circulation with an infected file attached, please contact the Computer Services Helpdesk (ext. 7555 or e-mail *helpdesk*).
4. If you are unsure how to proceed, suspected hoax messages should be sent to

Rachael Johnson for further advice.

6. How do I protect my PC from virus infections?

- **Keep backups**

The importance of backups to your regular working practice cannot be stressed too strongly for all sorts of reasons, including theft, fire and sudden unexpected hardware failure, in addition to destructive virus attacks. Please ensure that you have a copy of all your important data files in a location other than your local hard disk, at all times. Of course, it is very important that you take steps to ensure that your backups are not infected with viruses! The Computer Services recommends the use of CD-RW drives for making backups. Macintosh users use a Zip drive as their local backup facility of preference.

- **Make full and effective use of your anti-virus facility.**

Please see Computer Services Guide V2.2, "Sophos Anti-Virus - Guide for Users" <www.gold.ac.uk/infos/cs/guides/v202.pdf> for full details.

- **Treat e-mail attachments with caution.**

The Computer Services operates software which scans incoming College email (that is, all email containing *gold.ac.uk* in its address) for viruses before it reaches your inbox. The software, *AMAViS*, is very effective: details of the viruses stopped can be found at: <www.gold.ac.uk/infos/cs/tools/virus.php>

However, there remains the possibility that very new viruses may pass through these defences if they circulate widely before the virus definition files are updated to detect them. Therefore it remains incumbent on the user to maintain vigilance in dealing with any executable programs attached to an email message.

You should also be aware that an e-mail can carry a virus in HTML and Visual Basic scripting, in much the same way as a virus may be distributed in macro code. To protect yourself from this type of threat, turn off the script execution capability of your browser or word-processor.

- **Disable automatic launching of programs from e-mail and web browsers**

If available, ensure that the option to launch or execute and programs received as e-mail attachments or downloads is turned off. Most of the viruses which are detected on College computer systems are either brought in from home on floppy disk or other media, or else they are downloaded inadvertently using old, insecure web browser software. To see the viruses stopped on College PC systems, visit:

<www.gold.ac.uk/infos/cs/tools/ichack/>

- **Ensure that your software applications are set to disable macro execution**

Ensure that your word processing and spreadsheet applications are set to disable macros in e-mail attachments. To find out how to do this, see the section on Macro viruses.

- **Beware floppy disks**

Floppy disks must be treated with caution - if you are sharing files with a colleague on floppy disks, always run through your anti-virus program before copying any files to your local disk. Sophos' Intercheck client will automatically scan all files before it will allow you to access them. It is generally not advisable to make a habit of

booting your computer from a floppy disk, although that is not to say that you should not keep a start-up disk available for emergencies - just check it for viruses before it is used. Do not leave floppy disks in the disk drive where they can accidentally be used to start the computer when you next switch it on. If it contains a boot sector virus, your machine will become infected.

7. College Anti-Virus Software

Anti-virus software is only as good as the regularity with which it is updated. College anti-virus software is centrally updated every few days in order to keep vulnerability to new viruses to a minimum. The College standard anti-virus software is Sophos Anti-Virus (SAV) for Windows. All College PCs are configured to automatically receive Sophos via the network. Updated virus definition files are regularly copied down to your PC, to ensure that your machine receives the maximum protection from newer virus strains. For further details of Sophos as used on College PC systems, please see:

<www.gold.ac.uk/infos/cs/guides/v202.pdf>

8. What do I do if I find a virus?

The chances are that SAV will locate and disinfect any viruses present. SAV will alert you if a virus is discovered. A report is sent to the Sophos Administrator when a virus is discovered.

If you are worried that you may still have an active virus present on your system and have followed the procedures laid out in this article and in Guide V2.2, please contact the Computer Services Helpdesk for further information and support.

9. Macro viruses

9.1 What are they?

A macro is a series of commands used to perform an application-specific task, which can either be recorded as a series of keystrokes or written in a specialist macro language. A macro virus is a self-replicating macro, stored in a macro within a document or template, whose payload may involve destructive actions regarding the integrity of your data or, more dangerously, it may involve minor data changes which can render spreadsheet figures wildly inaccurate. Macro viruses are often stored in the normal or global template and thus infect every document you open. Whilst macro viruses were once application-specific, there is a disturbing new trend of cross-application viruses being developed. This is largely due to the fact that macro programming languages, such as VBA, are used extensively in a wide variety of popular Microsoft products. There are also cross-platform macro viruses in the wild.

9.2 How prevalent are they?

Macro viruses constitute a very popular threat to computer users. Consistently appearing at the top of the prevalence tables published by anti-virus vendors, macro viruses are so widespread for a number of reasons:

- Widespread use of macro scripting languages lead to cross-platform and cross-application macro viruses. Macro viruses are also easier to write than file viruses.
- Macro viruses are very easy to spread. All you need to do to become infected with a macro virus is to open an infected e-mail attachment or shared file.

9.3 How can I protect myself?

There are several things you can do to protect yourself from the threat of macro viruses.

- Set your e-mail application and web browser to check before launching programs. Mulberry, the standard College mailer for Windows 95/98, is defaulted to ask the user before launching applications to run attachments.
- Ensure that your suite of office applications (such as MS Word, Excel, PowerPoint) are set to the highest level of macro security, which will automatically disable all macros unless they come from a user-defined trusted source. Users of Office Pro 2000 installed by Computer Services can be assured that the highest level of macro protection is the default option. If you would like to check, go to the *Tools* menu, select *Macros, Security*. The *Security Level* tab contains the relevant information.
- And finally, the golden rule is NEVER open an e-mail attachment before having it virus-checked. Mulberry is defaulted to download all attachments to n:\download: the College Anti-Virus software has a ready-made task available to scan this area, so please use it!

10. Virus News

Information on the latest viruses and hoaxes can be found at:

<www.gold.ac.uk/infos/cs/anti-virus/>

11. Further Reading

If you would like to know more about computer viruses, please see the list of links below for further information.

<www.sophos.com/virusinfo/whitepapers/videmys.html>

<www.sophos.com/sophos/docs/eng/comviru/viru_ben.pdf>

<www.sophos.com/virusinfo/articles/safehex.html#users>

<www.sophos.com/virusinfo/articles/glossary.html>