Computer viruses - don't click here

PB/INFO/012 (10/06)

Every few months a computer virus outbreak is publicised in the national press. One in every thirty e-mail messages contains a virus. Every computer user should therefore be aware of the danger and take simple steps to protect themselves against it.

What do viruses look like?

A few years ago viruses spread on floppy disks. Now they are most commonly spread by e-mail, with filesharing and other Internet messaging systems also being used. This is a result of the increase in Internet use and the complex functions that have been added to modern e-mail programs. These allow users to send programs and dynamic documents around the world but also let malicious authors spread viruses just as widely and quickly. Viruses most commonly arrive as attachments to messages. To infect the computer the attachment must be run, usually by the user clicking on it. The text of the message usually provides an incentive to do this: money, sex and humour are commonly used as hooks to trap the reader. Unfortunately it is possible to mislead many e-mail programs so the nature of the attachment is concealed. All unexpected attachments, even if they appear to have 'safe' extensions, should therefore be regarded as suspect.

What can they do?

The first thing a virus will attempt to do is to reproduce itself. It may do this by sending infected e-mails to other addresses (often stolen from your address book or recent correspondents list), by writing a file to a local directory or network computer, or by attaching itself to other documents or programs on your computer. One of the most productive methods for a virus to use is to send infected mail to a mailing list to which you subscribe. If you click on an infected attachment, all these activities will appear to others to be done by you.

Some viruses then attempt to steal information from files, for example searching for passwords or credit card numbers; or to destroy information on the computer. In extreme cases this can make the computer unusable. Many viruses also run additional programs that allow other people, anywhere on the Internet, to take control of your computer.

Have I been a victim?

Unfortunately most people learn that they have been victims of a virus only after the reproduction stage, when one of their correspondents tells them they have sent out an infected e-mail. Many viruses display an alert box when infection has succeeded, or cause some other unexpected behaviour. By the time they reveal themselves in these ways it is likely that most of the damage will have already been done.

Some viruses can be successfully removed from infected computers, but others may require part or all of the operating system to be removed and re-installed. If documents or other files are modified or deleted by the virus, then it may not be possible to retrieve their contents. Where passwords or credit card numbers have been sent to others, of course, the damage cannot be undone. One business has estimated the average cost of repairing a single infected PC as £400.

How to stop them?

There are a number of technical measures that can be used to reduce the threat from viruses. Anti-virus programs, if they are kept up to date, do a good job of detecting viruses that are already known. Most of them also identify some forms of suspicious activity, which will sometimes detect previously unknown viruses as well. Anti-virus programs can be run centrally as well as on individual computers – the approach taken by one Janet site can be found in the References section.

Since most viruses are now spread by e-mail, mail servers are another popular location to check for viruses. Given sufficient computing power this can be done using anti-virus software; many viruses can also be detected by simple rules based on the file names or subjects of the mails they send. Unfortunately virus writers are now tending to include random variations, which make this approach less effective. One simple but effective technique is to reject all e-mail attachments of types known to be dangerous; however, this means that legitimate users can no longer send programs, documents and spreadsheets as simple attachments.

The most successful technical solution is to disable the functions that allow viruses to run, notably the ability to execute programs or macros direct from e-mail messages. Removing the Windows Scripting host reduces the virus threat considerably. however the only real solution to the present virus threat is for users to learn not to run them. Technical measures may seem simpler, but education is more effective.

References

Hoax warnings of viruses are often circulated and cause nearly as much disruption as the real thing. A list of the best known was maintained by CIAC.

Vendors of anti-virus software provide a public service in publishing detailed, up to date information about viruses. These include Sophos: http://www.sophos.co.uk/ [1] and Symantec: http://www.symantec.com/avcenter/ [2]

Information about Southampton University's virus scanning project is at: http://www.mailscanner.info/ [3]

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/computer-viruses-dont-click-here

Links
[1] http://www.sophos.co.uk/
[2] http://www.symantec.com/avcenter/
[3] http://www.mailscanner.info/