Viruses, Trojans and Worms...

Tips for Safer Computing

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

In the mid-1980s two brothers in Pakistan discovered that people were pirating their software. They responded by writing the first computer virus, a program that would put a copy of itself and a copyright message on any floppy disk copies their customers made. From these simple beginnings, an entire virus counter-culture has emerged. Today new viruses sweep the planet in minutes and can corrupt data, slow networks down, or harm your reputation.

What is a virus?

A virus or worm is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses can have harmful effects. These can range from displaying irritating messages to stealing data or giving other users control over your computer.

How does a virus infect computers?

A virus program has to be run before it can infect your computer. Viruses have ways of making sure that this happens. They can attach themselves to other programs or hide in code that is run automatically when you open certain types of file. Sometimes they can exploit security flaws in your computer's operating system to run and to spread themselves automatically. You might receive an infected file in an e-mail attachment, in a download from the Internet, or on a disk. As soon as the file is launched, the virus code runs. Then the virus can copy itself to other files or disks and make changes on your computer.

Trojan horses

Trojan horses are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions. For example, DLoader-L arrives in an e-mail attachment and claims to be an urgent update from Microsoft for Windows XP. If you run it, it downloads a program that uses your computer to connect to certain websites, in an attempt to overload them (this is called a denial of service attack).

Trojans cannot spread as fast as viruses because they do not make copies of themselves. However, they now often work hand-in-hand with viruses. Viruses may download Trojans which record keystrokes or steal information. On the other hand, some Trojans are used as a means of infecting a computer with a virus.

Worms

Worms are similar to viruses but do not need a carrier program or document. Worms simply create exact copies of themselves and use communications between computers to spread (see the "Internet worms" section). Many viruses, such as MyDoom or Bagle, behave like worms and use e-mail to forward themselves.

A brief history of viruses

1950s Bell Labs develop an experimental game in which players use malicious programs to attack each other's computers.

1975 Sci-fi author John Brunner imagines a computer "worm" spreading across networks.

1984 Fred Cohen introduces the term "computer virus" in a thesis on such programs.

1986 The first computer virus, Brain, is allegedly written by two brothers in Pakistan.

1987 The Christmas tree worm paralyses the IBM worldwide network.

1988 The Internet worm spreads through the US DARPA Internet.

1992 There is worldwide panic about the Michelangelo virus, although very few computers are infected.

1994 Good Times, the first major virus hoax, appears.

1995 The first document virus, Concept, appears.

1998 CIH or Chernobyl becomes the first virus to paralyse computer hardware.

1999 Melissa, a virus that forwards itself by e-mail, spreads worldwide. Bubbleboy, the first virus to infect a computer when e-mail is viewed, appears.

2000 Love Bug becomes the most successful e-mail virus yet. The first virus appears for the Palm operating system, although no users are infected.

2001 A virus claiming to contain pictures of tennis player Anna Kournikova infects hundreds of thousands of computers worldwide.

2002 David L Smith, the author of Melissa, is sentenced to 20 months in prison by US courts.

2003 The Blaster worm spreads itself across the Internet via a security weakness in Microsoft software. Together with the Sobig e-mail virus, it makes August 2003 the worst month ever for virus incidents.

2004 The creators of the Netsky and Bagle series of worms compete to see which can have the greater impact.

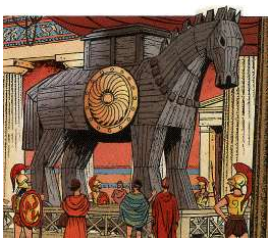
The most recent "malware" reported to Sophos can be found at:
www.sophos.com/security/top-10

What can viruses do?

Viruses used to play pranks or stop your computer working, but now they compromise security in more insidious ways. Here are the things that viruses can do.

- Slow down e-mail. Viruses that spread by e-mail, such as Sobig, can generate so much e-mail traffic that servers slow down or crash. Even if this doesn't happen, companies may react to the risk by shutting down servers anyway.
- Steal confidential data. The
- Bugbear-D worm records the user's keystrokes, including passwords, and gives the virus writer access to them.
- Use your computer to attack websites. MyDoom used infected computers to flood the SCO software company's website with data, making the site unusable (a denial of service attack).
- Let other users hijack your computer. Some viruses place "backdoor Trojans" on the computer, allowing the virus writer to connect to your computer and use it for their own purposes.
- Corrupt data. The Compatable virus makes changes to the data in Excel spreadsheets.
- Delete data. The Sircam worm may attempt to delete or overwrite the hard disk on a certain day.
- Disable hardware. CIH, also known as Chernobyl, attempted to overwrite the BIOS chip on April 26 1999, making the computer unusable.
- Play pranks. The Netsky-D worm made computers beep sporadically for several hours one morning.
- Display messages. Cone-F displays a political message if the month is May.
- Damage your credibility. If a virus forwards itself from your computer to your customers and business partners, they may refuse to do business with you, or demand compensation.
- Cause you embarrassment. For example, PolyPost places your documents and your name on sex-related newsgroups.

Where are the virus risks?



Viruses can reach your computer via all the routes shown here.

CDs and floppies

Floppy disks can have a virus in the boot sector. They can also hold infected programs or documents. CDs may also hold infected items.

Programs and documents

Programs and documents can be infected with viruses. When you share them with other users, by putting them on your network or intranet, or by sending them out, the infection can spread.

E-mail

E-mail can include infected attachments. If you double click on an infected attachment, you risk infecting your machine. Some e-mails even include malicious scripts that run as soon as you preview the mail or read the body text.

The Internet

You may download programs or documents that are infected. Security vulnerabilities in your operating system can also allow viruses to infect your computer via the Internet connection, without your having to do anything at all.

Which files can viruses infect?

Viruses can attach themselves to any code that runs on your computer: programs, documents, or the files that start up the operating system.

Boot sectors

When you switch on your computer, it accesses a part of the disk called the "boot sector" and runs a program that starts the operating system. The earliest viruses replaced this boot sector with their own, modified version. If the user started up their computer from an infected disk, the virus became active.

Programs

Some viruses infect programs. When you start the infected program, the virus is launched first. This type of virus appeared early in virus history but still poses a threat, as the Internet makes it easy to distribute programs.

Documents

Word processing or spreadsheet applications often use "macros" to automate tasks. Some viruses take the form of a macro that can spread from one document to another. If you open a document that contains the virus, it copies itself into the application's startup files and infects other documents you open with that application.

E-mail viruses

Many of the most prolific viruses are e-mail-aware: they distribute themselves automatically by e-mail. Typically, e-mail-aware viruses depend on the user clicking on an attached document. This runs a script that can forward infected documents to other people. The Netsky virus, for example, searches the computer for files that may contain e-mail addresses (e.g. EML or HTML files), and then uses the e-mail program on your computer to send itself to those addresses. Some viruses, like Sobig-F, don't even need to use your e-mail browser; they include their own "SMTP engine" for sending mail. E-mail viruses may compromise your computer's security or steal data, but their most common effect is to create excessive e-mail traffic and crash servers.

E-mail attachments

Any attachment that you receive by e-mail could carry a virus; launching such an attachment can infect your computer. Even an attachment that appears to be a safe type of file, e.g. a file with a .txt extension, can pose a threat. That file may be a malicious VBS script with the real file type (.vbs) hidden from view.

Can I get a virus just by reading e-mail?

You don't have to open an attachment to become infected via e-mail. Just viewing your mail is a risk. Some viruses, such as Kakworm and Bubbleboy, can infect users as soon as they read e-mail. They look like any other message but contain a hidden script that runs as soon as you open the e-mail, or even look at it in the preview pane (as long as you are using Outlook with the right version of Internet Explorer). This script can change system settings and send the virus to other users via e-mail. Microsoft issue patches that eliminate this security weakness and others like it. To find out which patches you need, visit: windowsupdate.microsoft.com. To keep informed about future patches, you can subscribe to a mailing list at: www.microsoft.com/technet/security/bulletin/notify.asp

Internet worms

You may be at risk whenever you are connected to the Internet, even if you don't open suspicious e-mail.

Can I get a virus from a website?

Web pages are written in HTML (Hypertext Markup Language). This cannot carry a virus, although it can call up programs or files that do. You cannot be infected by visiting an HTML page unless there is a security vulnerability on your computer that allows a program to run and infect you. Internet worms can travel between connected computers by exploiting security "holes" in the computer's operating system. The Blaster worm, for example, takes advantage of a weakness in the Remote Procedure Call service that runs on Windows NT, 2000 and XP computers and uses it to send a copy of itself to another computer. As the worm spreads, it creates a lot of traffic on the Internet, slowing down communications or causing computers to crash. This particular worm also later uses the computer to deluge a Microsoft website with data, with the aim of making the site inaccessible. Microsoft (and other operating system vendors) issue patches to fix security loopholes in their software. You should update your computer regularly by visiting the vendor's website.

Backdoor Trojans

A backdoor Trojan is a program that allows someone to take control of another user's computer via the Internet. A backdoor Trojan may pose as legitimate software, just as other Trojan horse programs do, so that users run it.

Alternatively – as is now increasingly common – a virus may place a backdoor Trojan onto a computer. Once the Trojan is run, it adds itself to the computer's startup routine. It can then monitor the computer until the user is connected to the Internet. Once the computer is online, the person who sent the Trojan can run programs on the infected computer, access personal files, modify and upload files, track the user's keystrokes, or send out Spam mail. Well-known backdoor Trojans include Subseven, BackOrifice and Graybird, which was disguised as a fix for the notorious Blaster worm.

Cookies

When you visit a website, it can place a small data packet called a "cookie" on the computer. This enables the site to remember your details and keep track of your visits. Cookies do not pose a threat to your data. However, they do threaten your confidentiality. If you prefer to remain anonymous, use the security settings on your browser to disable cookies.

Spyware

Spyware is software that enables advertisers to gather information about a computer user's habits. Spyware programs are not viruses (you cannot spread them to other computers) but they can have undesirable effects. You can get spyware on your computer when you visit certain websites. A pop-up message may prompt you to download a software utility that you "need", or software may be downloaded automatically without your knowledge. The spyware then runs on the computer, tracking your activity (for example, visits to websites) and reports it to others, such as advertisers. It can also change the home page displayed when you start your Internet browser, and can use a dial-up modem to call 0900 (premium rate) phone numbers. Spyware also uses memory and processing capacity, and can slow or crash the computer. Software is available that detects known spyware programs and enables you to remove them.

Adware and PUAs

Adware displays advertising - such as pop-up messages - which affects user productivity and system efficiency. Although many people view adware as undesirable, it is also a key component of a business model that can bring value to consumers in exchange for receiving advertisements.

PUA is a term used to describe an application that is not inherently malicious, but is generally considered unsuitable for the majority of business networks. Potentially unwanted applications include adware, dialers, remote administration tools and hacking tools.

Can mobile phones get a virus?

Mobiles can be infected by worms that spread themselves via the mobile phone network, although at the time of writing the risks seem limited. In 2004, the first mobile phone worm was written. The Cabir-A worm affects phones that use the Symbian operating system, and is transmitted as a telephone game file (an SIS file). If you launch the file, a message appears on the screen, and the worm is run each time you turn the phone on thereafter. Cabir-A searches for other mobile phones nearby using Bluetooth technology, and sends itself to the first it finds. This worm proves that infection is possible, but it was not released onto a public network.

There are also conventional viruses that send messages to mobile phones. For example, TimoA uses computer modems to send text (SMS) messages to selected mobile numbers, but in cases like these the virus can't infect or harm the mobile phone. Until now, the risks for mobile phones have been few. This could be because they use many different operating systems, and because the software and device characteristics change so rapidly.

Does Bluetooth carry risks?

Bluetooth technology for mobiles, computers and other devices could open the way for viruses, breaches of security or pranks. Bluetooth technology allows computers, mobile phones and even video recorders or fridges to locate nearby devices and to establish links with them transparently.

Bluetooth has already been exploited by a mobile phone worm, which uses it to find nearby phones to which it can forward itself. Technologies based on Bluetooth, e.g. Jini, also enable remote control of services. Bluetooth and Jini are designed so that only trusted code can carry out sensitive operations – but such technologies open up the possibility that malicious code could interfere with services. Bluetooth-enabled phones can also be used to locate other phone users nearby and send them unexpected –and sometimes offensive – messages. You can protect yourself against all sorts of Bluetooth threats – whether from malicious programs or from unwanted messages by turning off the "visible to others" Bluetooth setting in your phone.

Can palmtops get a virus?

Palmtops or PDAs provide new opportunities for viruses, but so far virus writers have shown little interest. Palmtops or PDAs run special operating systems – such as Palm and Microsoft PocketPC. These are vulnerable to malicious code, but so far the risks seem low.

There is only one virus written for Palm, and one Trojan horse, but neither seems to have been released. Virus writers prefer to target desktop systems, perhaps because they are more popular and allow viruses to spread rapidly via e-mail and the Internet. The real risk at present is that your palmtop will act as a carrier. When you connect it to a home or office PC to synchronise data, a virus that is harmless on the palmtop could spread to the PC, where it can do harm. To avoid this risk, follow our "Tips for safer computing" and always run anti-virus software on your desktop computer.

How anti-virus software can help

Anti-virus software can detect viruses, prevent access to infected files and often eliminate the infection.

Virus scanners

Virus scanners detect, and often disinfect, the viruses known to the scanner. Scanners are easily the most popular form of anti-virus software but they have to be updated regularly to recognise new viruses. There are on-access and on-demand scanners. Many packages offer both. On-access scanners stay active on your machine whenever you are using it. They automatically check files as you try to open or run them, and can prevent you from using infected files. On-demand scanners let you start or schedule a scan of specific files or drives.

Heuristics

Heuristic software tries to detect viruses – both known and unknown – by using general rules about what viruses look like. This software doesn't rely on frequent updates. However, heuristics can also be prone to false alarms.

Who writes viruses?

If your computer, or your network, is hit by a virus, the first thing you're likely to say is "Why do people write these viruses?" Virus writers sometimes want to spread a political message, or to disrupt companies of which they disapprove (many viruses and worms have criticised or targeted Microsoft, for example). They can also break into other users' computers, or gather e-mail addresses, and then sell that information to spammers.

However, virus writers are more often motivated by the notoriety that their exploits can gain them. Virus writers tend to be male, under 25 and single. Their self-esteem is bound up with the approval of their peer group, or at least of a small electronic community. Virus-writing, like graffiti art, is a kind of performance that wins the writer status. Viruses also give their writers powers in cyberspace that they could never hope to have in the real world. No doubt that is why virus writers choose names inspired by heavy metal music or fantasy literature, which thrive on similar illusions of prowess and potency.

Is virus writing always wrong?

Most of us take it for granted that viruses are simply a bad thing, but is that necessarily true?

Proof-of-concept

Sometimes people write viruses to prove that a new kind of virus is possible. These are known as proof-of-concept viruses. They don't usually have any effects and shouldn't be released onto other users' computers.

Virus research?

Virus writers like to claim that they are doing research. Yet viruses are often poorly written, they are released at random on unsuspecting users, and there's no way to collect the results. This can hardly be called research. Many viruses are "harmless" or take the form of jokes. Others alert us to security flaws in software. Some people argue that viruses could even be useful, e.g. by distributing bug fixes. Unfortunately, the idea of harmless viruses doesn't stand up to scrutiny.

First, viruses make changes on users' computers without their consent. That is unethical – and illegal in many countries –whether the intention is good or bad. You shouldn't interfere with somebody else's computer, any more than you would borrow their car without telling them – even if you did change the oil. Secondly, viruses don't always perform as the author intends. A badly written virus can cause unforeseen problems. Even if it is harmless on one system, it may be harmful on others. Thirdly, viruses spread indiscriminately: the writer has no control over who receives them.

What to do if you come under virus attack

"Don't do anything. Have a cup of tea or coffee - don't start bashing away at the keyboard before you've determined what you ought to do. In my experience, a lot of virus damage is actually damage done by people doing things before they've made sure of what they ought to do, which is another way of saying panic. So, don't panic".

Dr Alan Solomon - one of the world's foremost computer virus experts

Preventing viruses

There are simple measures you can take to avoid being infected or to deal with viruses if you are infected:

- Make users aware of the risks. Tell everyone that they are at risk if they open e-mail attachments, download files from websites, or swap disks.
- Install anti-virus software and update it regularly. Anti-virus programs can detect and often disinfect viruses. If the software offers on-access virus checking, use it.
- Use software patches to close security loopholes. Watch out for "patches" for your operating system. These often close loopholes that make you vulnerable to viruses.
- Use firewalls. A firewall can prevent unauthorised access to your network and also prevent viruses sending out information.
- Keep backups of all your data. Keep backups of all data and software, including operating systems. If you are affected by a virus, you can replace your files and programs with clean copies.

Tips for safer computing

Apart from using anti-virus software, there are plenty of simple measures you can take to help protect yourself and your company against viruses and worms. Here are our top tips for trouble-free computing.

Don't launch unsolicited programs or documents

If you don't know that something is virus-free, assume it isn't. Tell people in your organisation that they should not download unauthorised programs and documents, including screensavers or joke programs, from the Internet. Have a policy that all programs must be authorised by an IT manager and virus-checked before they are used.

Don't use documents in .doc and .xls format

Save Word documents as RTF files and Excel spreadsheets as CSV files. These formats don't support macros, so they can't spread document viruses. Tell other people to send you RTF and CSV files. Some document viruses disguise the format so to be totally safe, use text-only files.

Use software patches to close security loopholes

Watch out for security news and download patches. Such patches often close loopholes that can make you vulnerable to viruses or Internet worms.

IT managers should subscribe to software vendors' mailing lists such as that at: www.microsoft.com/technet/security/bulletin/notify.asp.

Home users who have Windows computers can visit: windowsupdate.microsoft.com, where you can scan your PC for security loopholes and find out which patches to install.

Block files with double extensions at the gateway

Some viruses disguise the fact that they are programs by using a double extension, such as .TXT.VBS, after their filename. At first glance a file like LOVE-LETTER-FOR-YOU.TXT.VBS looks like a harmless text file or a graphic. Block any file with double extensions at the e-mail gateway.

Block unwanted file types at the e-mail gateway

Many viruses now use VBS (Visual Basic Script) and Windows scrap object (SHS) file types to spread. It is unlikely that your organisation needs to receive these file types from outside, so block them at the e-mail gateway.

Subscribe to an e-mail or SMS alert service

An alert service can warn you about new viruses and offer virus identities that will enable your anti-virus software to detect them. Sophos has a free alert service. For details, see www.sophos.com/virusinfo/notifications

The Government also provides a free e-mail and SMS alert service: IT Safe – a rapid alerting service that tells computer users about serious Internet security problems. It aims to provide both home users and small businesses with proven, plain English advice on protecting computers, mobile phones and other devices from malicious attack. For more information visit: www.itsafe.gov.uk

Have a separate network for Internet machines

Maintain separate networks for those computers that are connected to the Internet and those that are not. Doing so reduces the risk that users will download infected files and spread viruses on your main network.

Use firewalls and/or routers

A firewall admits only authorised traffic to your organisation. A router controls the flow of packets of information from the Internet.

Configure your Internet browser for security

Disable Java or ActiveX applets, cookies, etc., or ask to be warned that such code is running. For example, in Microsoft Internet Explorer, select:
Tools|Internet Options|Security|Custom Level and select the security settings you want.

Make regular backups of all programs and data

If you are infected with a virus, you will be able to restore any lost programs and data.

Change your computer's bootup sequence

Most computers try to boot from floppy disk (the A: drive) first. IT staff should change the settings so that the computer boots from the hard disk first. Then, even if an infected floppy disk is left in the computer, it cannot be infected by a boot sector virus.

Write-protect floppies before giving to other users

A write-protected floppy cannot be infected.

Anti-Virus Software

A selection of anti-virus software packages is listed below. There are many others and, over the Internet, there are programs that can be downloaded free of charge but most have a limited applicability since the only effective anti-virus program is one that is updated at least once a month. Microsoft advise that you should have at least one commercial virus-detection program and use it regularly to check your computers for viruses. Be sure to obtain the latest virus signature files for your program when they are available, because new viruses are created every day:

- Sophos Anti-virus
  www.sophos.com
- eTrust EZ Antivirus
  www.my-etrust.com
- Norton AntiVirus
  www.norton.com/smallbiz/index.html
- Panda Antivirus Small Business Edition
  www.pandasecurity.com/smbusiness.htm
- Outpost Firewall Pro
  www.agnitum.com
- McAfee VirusScan
  www.mcafee.com
- Trend PC-cillin Internet Security
  www.antivirus.com
- Process Guard
  www.diamondcs.com.au
- E-mail Server Anti-Virus - GFI MailSecurity
  www.gfisoftware.com
- Trend Micro NeatSuite
  www.trend.com
- Kaspersky Small Office Security
  www.kaspersky.co.uk/
- AVG Internet Security
  www.avg.co.uk

Recommended Reading

A selection of anti-virus books is listed below:

- Malicious Mobile Code: Virus Protection for Windows, by Roger A. Grimes, published by O'Reilly UK, Hardcover - 28 August, 2001
- E-mail Virus Protection Handbook: Protect Your E-mail from Trojan Horses, Viruses, and Mobile Code Attacks, published by Syngress Media, paperback - 1 October, 2000.
- Bigelow's Virus Troubleshooting Pocket Reference, by Ken Dunham, paperback.
- Malware: Fighting Malicious Code, by Ed Skoudis, paperback October 2003.
- Network Security for Dummies, by. C. Chey, paperback November 2002
- Computer Viruses Demystified, by Paul Oldfield (ed.), 2003

Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

Acknowledgement

© Copyright 2004, is acknowledged of information provided in this document by SOPHOS plc. Since the 1980s SOPHOS has been recognised as one of the world's leading developers of anti-virus products, protecting 20 million business users worldwide.

For more information please contact:
SOPHOS Plc
The Pentagon
Abingdon Science Park
Abingdon
OX14 3YP
UK
Web: www.sophos.com
E-mail: customerservice@sophos.com

Publication issued or updated on:
27 January 2012

Ref: 91