Danger zone

The proliferation of email and the internet has created a fertile breeding ground for computer viruses. Terence Green advises on ways you can **protect and survive.**

Recent high-profile virus attacks such as Happy99, Melissa and Chernobyl have put the spotlight on the virus threat and this time it isn't a Michelangelo-style marketing exercise. New working practices mean new threats require a more sophisticated approach than simply scanning for viruses.

Back in 1995 the virus threat came on floppy diskettes. In 1999 executable viral code is transmitted via document exchange and email because fewer people use floppies, more people use email, and more computers are interconnected via networks and the internet.

Boot and file viruses are no longer responsible for the majority of virus incidents but they are still active. The Chernobyl virus which hit the headlines in April is a Windows 95-specific file infector usually spread via floppy, although it can also be found on CDs. IBM even managed to ship a batch of infected Aptiva PCs. Boot sector and file viruses spread slowly by comparison with mail-borne viruses. Melissa infected over 100,000 computers within two days of its first release.

As viruses need human intervention to propagate, they exploit both human nature and the way we work. The latter has led to the rise of macro viruses. The vast majority of desktops run Windows, over 80 percent run Microsoft Office, and many have email. In April 1999 the top ten viruses reported to Sophos, an anti-virus software vendor, included six Microsoft Word macro viruses, one Excel macro virus, one Office 97 macro virus, one Win32 file infector (Happy99) and one Windows 95 file infector (Chernobyl).

Clearly, the widespread adoption of Windows and Office creates fertile ground for macro viruses, but they still depend heavily on human nature. Happy99 is a worm which infects Win32 (Windows 9x and Windows NT) files. Specifically it modifies a Windows system file, enabling it to attach itself to every outgoing mail message.

Contents

Happy99 plays on human nature. Many people, receiving an attachment entitled 'Happy99' in January 1999, opened it expecting to see a new year greeting. Instead, they infected their systems and passed it on. Melissa is a macro virus with a twist: it infects Word documents but also uses Microsoft Outlook (but not Outlook Express) to send infected mail to addresses listed in the user's address book. When someone receives a message carrying Melissa as an attachment, they feel safe in opening it as it appears to come from someone they know.

The macro virus threat is hard to defeat. Anti-virus scanners are best deployed against known viruses. If they try too hard to identify possible new viruses, they run the risk of raising false alarms and being disregarded. Microsoft software developments have a factor in the 'success' of macro viruses: Office 97 includes Visual Basic for Applications, a single macro language for all Office applications.

Melissa was undoubtedly a perversion of the purpose Microsoft envisioned for VBA, but its use of Word and Outlook is entirely consistent with VBA's objectives. Say your company creates a VBA application for expense accounting. When you return from a trip, you email the accounts department and receive a reply with an attachment that opens an expenses form in Word. You fill in the form, and when you close the document it automatically uses Outlook to send a copy to your supervisor for approval. Not very different from Melissa at all.

The dangers inherent in macros have been obvious ever since Concept, the first Word macro virus, appeared in 1995, accidentally released by Microsoft on a CD distributed to developers. But Microsoft has not found it easy to control the power of macros. Office 97 has a feature called macro virus protection which provides a simple on/off switch for macros. By default, when Office 97 is installed, the ability to run macros is disabled. If the user then opens an attachment containing a macro, Word throws up a warning message about the potential for macro virus infection and requires the user to place a tick in an 'Enable Macros' check box before it will run the embedded macro in the document.

Illustration by Ken Laidlaw

In effect, Office 97 provides little or no real protection against a macro virus infection. Users who work in offices which make use of VBA macros will either turn macro virus protection off permanently or become so inured to clicking the Enable Macros switch whenever they open a document with an official macro, that they'll hardly hesitate before opening an attachment like Melissa which purports to come from someone known to them.

Human nature ensures that the simple on/off switch in Office 97 simply doesn't provide enough control over macros. At the very least there should be three positions – off, off for unauthorised macros, and on for authorised macros; and this is what Microsoft has implemented in Office 2000 with digital certification for macros.

By upgrading to Office 2000 a company can enable digitally signed macros for execution while preventing all other macros from running. This is better, but not perfect. The digital signing scheme requires a certain amount of administration for which a small- to medium-sized company might not have the skills or time. It also will not work unless Microsoft Internet Explorer 4.0 or higher is installed, so companies using Netscape Navigator or Internet Explorer 3 or earlier won't be able to use signing.

What's more, the scheme can still be circumvented by users who change their security options, and users who don't alter their security options are still faced with the Enable Macros warning when they open a document with an embedded macro; so we're back at square one where human nature enables an attack like Melissa to succeed.

Mail-borne attacks are a significant threat but increasing use of the internet exposes us to other dangers which can be activated simply by viewing a web page. In this case the user isn't required to perform any action other than visiting the page in order to activate the malicious code.

Increasing use of the internet EXPOSES US TO OTHER DANGERS which can be activated simply by viewing a web page ... just visiting the page activates the malicious code

One of these has recently been dubbed the Russian New Year attack, but it has long been discussed on net newsgroups. If you use your browser to view a web page containing an Excel or Word document, the browser will attempt to open the relevant application if it is installed on your PC. This opens the way for a malicious web page to introduce a macro virus into your system and it happens without any 'enable macros?' warning.

In a similar vein, JavaScript, VB Script, Java, and ActiveX code embedded in web pages has the potential to cause harm without any user action. In theory Java code operates in a security 'sandbox' which prevents it from operating outside the user's browser, but a number of instances of bugs in Java which exposed security holes have been discovered in the past. ActiveX is more of a problem because it can do anything on your computer. In theory, ActiveX code offers the security of digital authentication, but this only identifies the person or organisation ostensibly responsible for the code and says nothing about their intentions or their ability to write bug-free code.

How to protect your system

The multifarious threats discussed here all depend in some way on introducing code which executes on your computer. The solution is simple — prevent unauthorised code from executing. But how? Simply relying on anti-virus scanning is insufficient. Scanners can't offer complete protection against new, unknown viruses, against complex macro viruses, against encrypted attacks.

Nor can you rely on the built-in protection in Microsoft software because you can't change human nature. Yes, if you never open attachments, you've eliminated one potential source of infection. But the fact remains that people do open them.

Since the problem mainly exists on Microsoft software, why not switch to another supplier? It has some validity as a solution, but it's really too much to expect 90 percent of desktops and 80 percent of office-suite users to switch in order to counter a potential risk. And if they did, so would the virus authors. The prevalence of Microsoft macro viruses is as much a function of the size of its user base as of its vulnerability.

The best answer is a combination of methods. How much you need to spend on a solution depends on the size of your organisation and the level of exposure. The aim should always be to simplify and automate. The less each user is required to do in order to maintain security, the less likely they are to circumvent it.

To begin with, you should have a comprehensive and tested backup and recovery plan. You should set the BIOS boot setting so that PCs can't boot from the default 'floppy diskette first, hard disk second'. Boot sector viruses are relatively rare, but this action will ensure that they can't affect you. There are very few reasons these days to boot from a floppy diskette and it's a simple matter to enable floppy boot only when you have to. Naturally you should scan the bootable floppy for viruses before using it.

If you're committed to using Microsoft Word and you tend to receive messages with attachments, you might want to use the Microsoft Word Viewer which you can download from the Microsoft website. The Word Viewer allows you to view documents without activating any embedded macros, and you can cut and paste the contents to another word processor.

Windows and Office users should enable macro virus protection in applications and the security options in browsers. Always keep up to date with security advice. Some sites to watch are:

- **Microsoft Security Advisor**
www.microsoft.com/security
- **Microsoft Office Update**
officeupdate.microsoft.com
- **Windows NT BugTraq**
ntbugtraq.ntadvice.com
- **Windows 98 Central**
www.win98central.com

Always apply recommended security patches and updates for Office and for Internet Explorer and Netscape Navigator.

Do scan for viruses but do not rely on a single anti-virus scanner. Use at least two, and update them regularly. Most anti-virus software and general security software vendors offer gateway systems which will scan for viruses and malicious documents. Alternatively, Mimesweeper <www.mimesweeper.com>, a highly recommended gateway, scans incoming and outgoing content and is usually used in conjunction with one or more virus scanners.

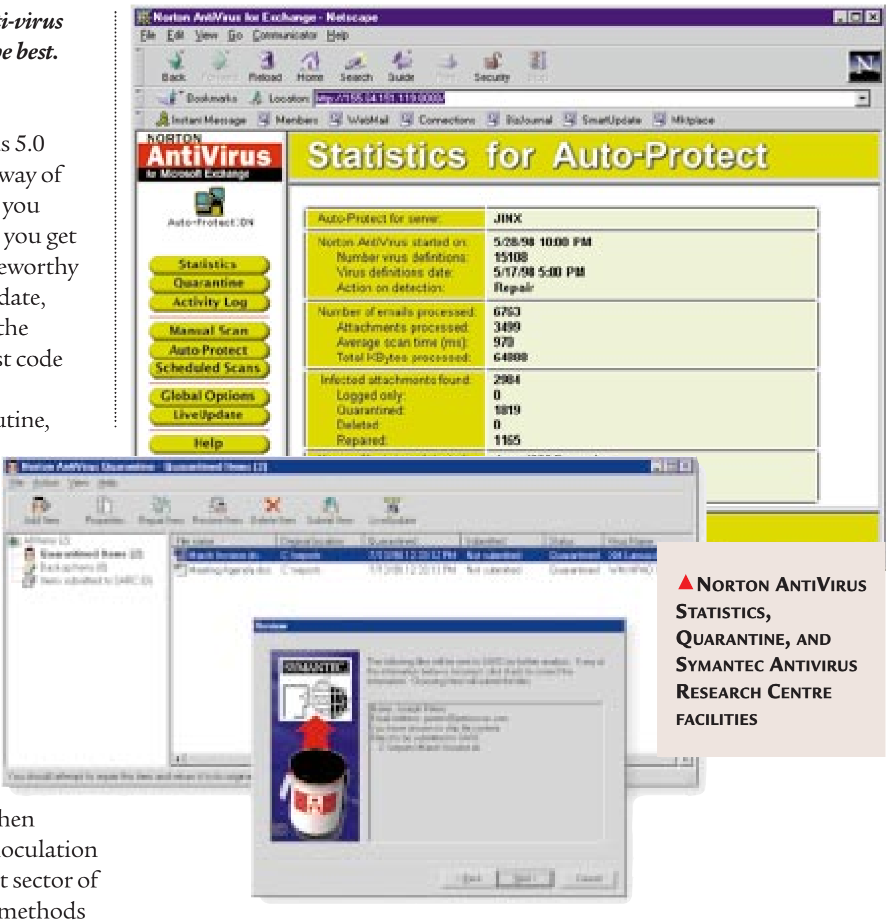
There are a number of tools which offer better protection. Reflex DiskNet <www.reflex-magnetics.co.uk> has a comprehensive set of functions which prevent unauthorised executables from running. Finjan <www.finjan.com> supplies a range of 'Surfin' products which control the behaviour of what it calls 'mobile code' — that is, ActiveX, Java, JavaScript and VB Script. The tools from Reflex and Finjan are particularly useful when you actually need to run mobile code and can't afford to simply switch off Java or ActiveX execution in your browsers.

You also need to ensure that viruses and other malicious executables don't enter the system from inside via CDs and floppy diskettes. Don't rely on employee sanctions: accidents can and do happen. Again you can turn to a solution like Reflex DiskNet which will only allow authorised floppy diskettes and other removable disks to be used. DiskNet is actually a collection of several tools which, in addition to the services already mentioned, can also be used to set up a list of authorised macros which are allowed to run while all others are prevented from executing.

As they say on CrimeWatch, don't have nightmares! But do be careful out there.

Vanquish **that virus!**

Virus scanners should be a part of any anti-virus defence strategy. Here we review five of the best.


Norton AntiVirus for Exchange - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Quarantine
Activity Log
Manual Scan
Auto-Protect
Scheduled Scans
Global Options
LiveUpdate
Help
Norton AntiVirus Quarantine - Quarantined Items
SYMANTEC
Review
Back Next Cancel

Statistics for Auto-Protect

Auto-Protect for server:	JINX
Norton AntiVirus started on:	5/28/98 10:00 PM
Number virus definitions:	15108
Virus definitions date:	5/17/98 5:00 PM
Action on detection:	Repair
Number of emails processed:	6763
Attachments processed:	3499
Average scan time (ms):	970
Total KBytes processed:	64888
Infected attachments found:	2984
Logged only:	0
Quarantined:	1819
Deleted:	0
Repaired:	1165

▲Norton AntiVirus statistics, quarantine, and Symantec Antivirus Research Centre facilities

■ Symantec Norton AntiVirus 5.0

During installation of Norton AntiVirus 5.0 you set various parameters to adjust its way of working to your own system. It also lets you create an emergency boot disk for when you get a virus in memory. One of the most noteworthy characteristics of this version is Live Update, an automatic utility which connects to the Symantec website to download the latest code to combat new viruses.

Another novelty is the quarantine routine, which lets you isolate suspicious files in a secure section of the PC until they can be repaired. However, you can still send sample files to the Symantec Antivirus Research Centre to see if they can come up with a solution. This dispatch of files worked well in our tests but we were less impressed with the technical support we received. The Research Centre reported that the files we sent were not infected. In fact, we had sent a file infected with the Ithaqua virus.

Norton AntiVirus uses signatures when scanning for viruses, and also uses an inoculation utility which detects changes in the boot sector of the hard disk. Used together, these two methods should stop any boot sector virus attack, whether the virus is known and documented or not.

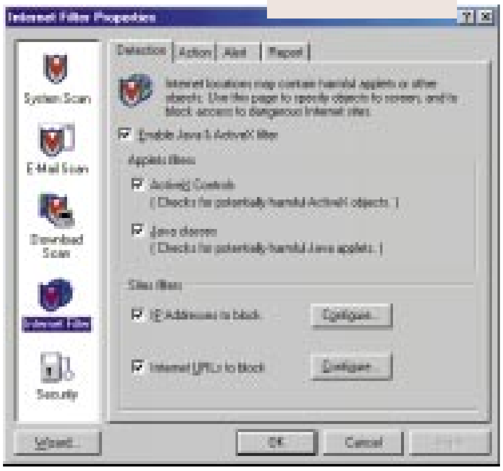
The strength of Norton AntiVirus lies in its detection of known viruses, along with a system of alarms that activate when a suspicious process starts to execute. However, certain utility software may set off false alarms as it accesses the hard disk. Performance was only average in our tests, and the package showed evident weakness in finding and destroying bat and mIRC viruses.

Overall this is an average product that does its job but does not incorporate any of the new technologies. Although it uses the internet to update itself, it doesn't pay enough attention to the net as a route for viruses to reach the user's PC. Virsuses are only detected when the writing to the hard disk begins.

■ McAfee VirusScan

At the beginning of the year Network Associates shook up the anti-virus market when it bought both McAfee and Dr. Solomon's. Using the best of the newly acquired engines from Dr Solomon's, combining it with the power of McAfee and Anyware and the interface of McAfee, Network Associates has created a powerful new anti-virus package, although it is still using the McAfee VirusScan name.

The program offers two ways of working. Normal mode offers very few options, but Advanced mode is where we find the new features. In Advanced mode you can send reports over the net, carry out a heuristic scan for macros and files, and exclude files and directories from any analysis. VirusScan is the only package able to detect viruses by analysing data from all communications ports, and in our web test it detected and destroyed all the malicious Java applets and ActiveX controls. The other products we looked at couldn't detect the ActiveX viruses, and none were able to analyse them at a protocol level as VirusScan does.



☑ Enable Java & ActiveX filter

Applets filters

☑ ActiveX Controls
(Checks for potentially harmful ActiveX objects.)

☑ Java classes
(Checks for potentially harmful Java applets.)

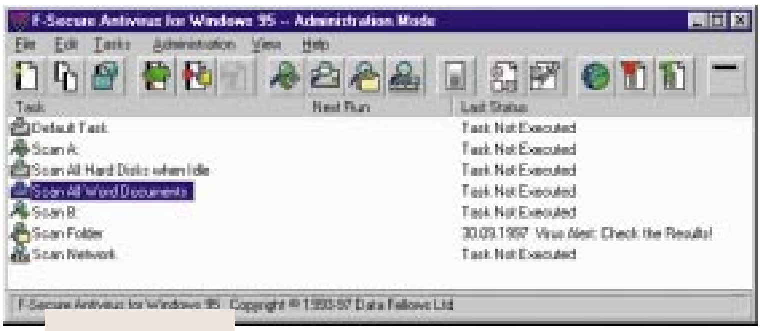
Sites filters

☑ IP Addresses to block

☑ Internet URLs to block

▼In our web test, McAfee VirusScan detected and destroyed all the malicious Java applets and ActiveX controls

➔



Task	Next Run	Last Status
Default Task		Task Not Executed
Scan A:		Task Not Executed
Scan All Hard Disks when Idle		Task Not Executed
Scan All Word Documents		Task Not Executed
Scan B:		Task Not Executed
Scan Folder		30.09.1997 Virus Alert: Check the Results!
Scan Network		Task Not Executed

F-Secure Antivirus for Windows 95 Copyright © 1993-97 Data Fellows Ltd

▲F-Secure's two search engines give better detection rates but do slow down the analysis process

Another remarkable aspect of this package is its analysis of compressed files. It was the only one we saw that could detect viruses inside compressed files, such as zip and lzh files, and is undoubtedly one of the most solid and balanced products tested here. Its detection rate equals or exceeds Dr. Solomon's and it uses the new technologies that Solomon's lacks. The only weak point was the technical support, especially how they responded to the challenge we posed them to find the Ithaqua virus in an infected file.

■ Dr Solomon's AntiVirus Toolkit

Dr Solomon's has long been one of the most respected names in anti-virus packages. However, it looks as if the end of the road could be approaching, following the takeover by Network Associates. The lastest version of VirusScan incorporates the Dr Solomon's engine and Network Associates has added new technologies to it that increase its power.

This leaves Dr Solomon's AntiVirus Toolkit somewhat in the shade, but it is still one of the best anti-virus packages. With its intuitive and simple interface it is easy to use, it works quickly and has a very high detection ratio. In our tests its heuristic engine also came out as among the best. It picks up information about all the files on the system and detects any change in them. The behaviour of the core modules was good, but it could take better account of the internet and the way the new breed of viruses work.

■ F-Secure

F-Secure has two search engines instead of one, F-PROT and AVP. This gives better detection rates but does slow down the analysis process. On the other hand, those two integrated technologies together make one of the best engines alongside Dr Solomon's.

F-Secure uses both engines independently, rather than incorporating the two technologies into a single engine. A file is opened and scanned first with the F-PROT engine and afterwards with the AVP engine, giving two chances for viruses to be detected.

There are problems with this approach. Apart from slowing the process down, both engines have to be updated separately. Another weak point is the interface, which is untidy and unintuitive. But where it suffers most is in its protection of the system from infection via the internet.

In our detection tests the results were good, due to the use of two search engines, especially AVP; but problems arose when scanning large amounts of infected files. To run the Zoo virus and binary viruses tests we had to split the files into smaller groups, as after more than two hours analysing infected files non-stop, an error occurred which forced us to restart the test.

■ Sophos Anti-Virus

Sophos is an easy to use program that allows access to most options with a single click of the mouse, although it has more advanced configuration options that can be reached via menus. Among these is an option to do a quick search, which analyses only the characteristic areas where viruses hide, while a second search carries out a complete scan.

The InterCheck technology of Sophos offers the user active protection in real time both on a standalone PC and on one connected to the internet. Although this package works through a DOS window, our tests showed that it works perfectly. Email and shared files often use compression or encryption in their formats, which makes it impossible to scan their contents, but InterCheck prevents any unknown file formats from being opened, so preventing infection.

On the downside, Sophos cannot scan compressed files; they must first be uncompressed manually, so the program can analyse the content. And as in other instances here, technical support were unable to rightly diagnose the Ithaqua virus we sent them.

VNU Labs

PCW DETAILS

NORTON ANTIVIRUS 5.0
Price *£45.83 (£39 ex VAT)*
Contact *Symantec 0171 616 5600*
www.symantec.co.uk

MCAFEE VIRUSCAN
Price *£24.95 (£21.23 ex VAT)*
Contact *Network Associates 01753 827500*
www.mcafee.com

DR SOLOMON'S ANTIVIRUS TOOLKIT
Price *£79.95 (£68.04 ex VAT)*
Contact *Dr Solomon's 01296 318700*
www.drsolomon.com

F-SECURE
Price *Single-user licence £105.75 (£90 ex VAT)*
Contact *Portcullis Security 0800 694 1098*
www.portcullis-security.com

SOPHOS ANTI-VIRUS
Price *Per user £46.41 (£39.50 ex VAT)*
Contact *Sophos 01235 559933*
www.sophos.co.uk