ISSN 0956-9979 NOVEMBER 1999

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Conference call:** VB'99 speaker Dave Black details the *RCMP's* daily fight against viruses on p.14, while on p.4 an open letter to *Microsoft* is the direct result of a technical panel session in Vancouver. The conference report on p.12 explains it all.

• **Told you so!** Péter Ször predicted at *VB's* conference that something like Infis would come along soon. We analyse this new *Windows NT* virus on p.8.

• **Sweet sixteen:** Our bi-monthly Comparative Reviews continue with *Windows 98*. Sixteen products hope for VB100% awards, starting on p.16.

CONTENTS

COMMENT

Sites for Sore Eyes?

I have long thought that anti-virus software, when made available for download, should be presented as if the downloader were in the worst possible position: with a computer that can't load a GUI operating system and that has only a slow modem with just text-based tools for connecting to the Internet. This is a reasonable assumption; it is standard to recommend a clean floppy boot, and not to use software from the hard drive, when one thinks there might be a virus lurking about.

"… top quality products have both good and bad Web access…"

Moreover, some viruses prevent clean boots into a GUI, and, when restricted to a floppy boot, one isn't likely to be able to use applications like *Netscape* or *Internet Explorer*, but will be reduced to the likes of *Kermit* and *Lynx*: this is the lowest common denominator for a PC that still has 'Net access. If, however, a GUI can be used, loading all those glitzy graphics is not fun when using a slow modem. It is reasonable to assume that, when the user thinks an infection may be present and a graphical browser is being used, the autoloading of images is likely to be disabled.

Unfortunately, many vendors seem to think otherwise. For example, on one vendor's software download page, viewed by *Lynx* (and not much better in *Netscape* without images) one finds this rather unhelpful display (though it's actually on 5 lines), here compressed:

[INLINE] [INLINE] [LINK] [LINK] [LINK] [INLINE]

Some vendors, of course, are better than others. One, in particular, starts out well enough, offering a <Text-only> link on their home page. Following this leads to a text-based index – but when one selects the <Download now> link, the result is a non-text page that, in *Netscape* with autoloading of images disabled, displays only the company logo, copyright information, and several unlabelled graphic icons for selection. Then there are the pages that are tuned to a particular browser, or that make too much use of forms, or worse, that require active content of one type or another to load. Even worse yet, there are those that crash a browser for whatever reason. This is hardly reassuring to the person who thinks they may currently be afflicted by a virus…

The vendor might argue that this matters little, since the victim can contact the IT department, or download on another computer. This, however, ignores the corporate worker at home, as well as the home user. Interestingly enough, some of the vendors who cater only to corporates have particularly well-designed Web pages, from the perspective of being accessible to all comers.

All AV vendors should consider implementing the following. When using the HTML inline IMG statement to place a graphic, use the ALT attribute to associate 'meaningful' text with that image. Offer text-only links, particularly from pages that lead to the download section. Avoid active content – the industry says that it is potentially a Bad Thing, so let's practise what we preach. Always make a small package available for download: the text-based browser user may not see that fancy blinking graphic that lets one know it's a 35 MB download. Moreover, if the user has to boot from floppy and, for example, is infected with Monkey, they will have to download to a floppy – the hard drive will not be accessible.

Do more quality assurance testing on all Web pages, with particular attention to the download ones and all pages that lead to these pages. This QA testing should include many different browsers, and should check to make sure there is no HTML code designed for one particular browser.

The correlation of Web accessibility with product quality, as measured by tests such as *VB* Comparative Reviews, seems nonexistent: some poor products have good Web presence – perhaps this is where they devote most of their efforts – while top quality products have both good and bad Web access, if one considers the complete range of possible browsers. I urge those vendors who fail to meet the mark to devote some careful thought to serving those most in need – the individual user who has no access to another machine, has a slow modem, and who is sure only to have a floppy drive. If the process is easy for them, think how much better it will be for everyone else!

Bruce P. Burrell, University of Michigan

NEWS

Vancouver Revisited

VB has a limited number of conference proceedings CDs for sale. They include the previously advertised but unheard contributions from Costin Raiu and Adrian Marinescu from *GeCAD*, Romania. A conference CD costs £150 including VAT. Please contact Jo Peck at the *Virus Bulletin* UK offices; Tel +44 1235 555139, fax +44 1235 531889, or email jo@virusbtn.com. The venue for VB 2000 is to be announced in the January 2000 issue ▮

Look What's Round the Corner

The recently discovered P98M/Corner.A is the first macro virus to infect *Microsoft Project* applications. This virus infects both *Project* and *Word* and can travel between them. When an infected document is opened in *Word 97* or *2000*, Corner checks if *Project* is running. If it is, it gets infected.

The *Word* part of the virus is a simple class infector. It spreads when an infected document is closed. At this point it sets the *Office 2000* security settings to low, disables the 'Tools/Macros' menu and turns off the macro virus protection. Then the virus replicates to all opened documents. Corner is not able to infect *Word 2000* unless the user has first changed the security settings to medium or low. To infect *Project*, the virus adds a new blank project and inserts the virus code to the 'ThisProject' class module.

When an infected document is opened in *Project 98*, Corner infects *Word*, even if it is not running. It opens *Word* and inserts the virus code in the global template's class module 'ThisDocument'. The user will not see *Word* being infected. The *Project* part of the virus is not resident, and it does not infect the global project – it replicates during project deactivation (after an infected project has been opened). An analysis of this virus, which does nothing other than replicate, is planned for next month ▮

Happy gets Happier

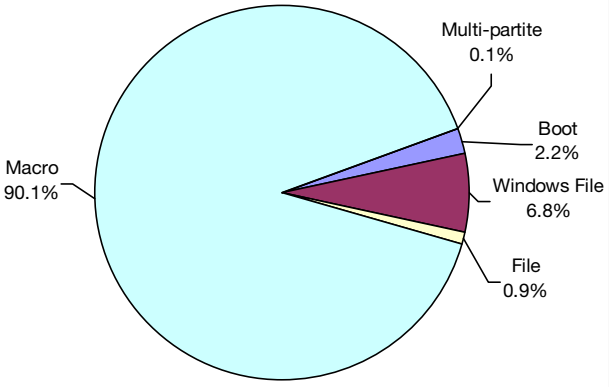
Some 'common' EXE infectors can infect SKA.EXE from Win32/Ska (which the virus attaches to email messages as HAPPY99.EXE). When people receive such a copy of 'Ska', if their scanners are set to 'automatic disinfection', the EXE virus may well be cleaned but the resulting 'Happy99.exe' file is not exactly the same as the 'real' one. As many (most) products detect 'immutable' files like HAPPY99.EXE by CRCs, these scanners then *miss* Win32/Ska, so the user may go on and run it. Fortunately, SKA.EXE cannot be infected with CIH, but recently three separate people have posted HAPPY99.EXE infected with Kriz.4092 to Usenet. The moral? Do not trust automatic disinfection and set gateway scanners to quarantine rather than clean infected attachments ▮

Prevalence Table – September 1999

Virus	Type	Incidents	Reports
ColdApe	Macro	890	23.5%
Class	Macro	721	19.0%
Ethan	Macro	481	12.7%
Pri	Macro	394	10.4%
Story	Macro	301	7.9%
Marker	Macro	263	6.9%
Win32/Ska	File	192	5.1%
Tristate	Macro	69	1.8%
Cap	Macro	54	1.4%
Form	Boot	44	1.2%
Laroux	Macro	41	1.1%
Win32/Pretty	File	41	1.1%
Melissa	Macro	33	0.9%
Freelinks	Script	29	0.8%
Concept	Macro	18	0.5%
Win95/CIH	File	17	0.5%
Appder	Macro	15	0.4%
Footer	Macro	15	0.4%
Thus	Macro	11	0.3%
Muck	Macro	9	0.2%
Npad	Macro	8	0.2%
Walker	Macro	8	0.2%
Others [1]		135	3.6%
Total		3789	100%

[1] The Prevalence Table includes a total of 135 reports across 58 other viruses. A complete summary can be found at http://www.virusbtn.com/Prevalence/.

Distribution of virus types in reports



LETTERS

Dear Virus Bulletin

Open Letter to Microsoft

A technical panel session was held on Friday, 1 October 1999 at the *Virus Bulletin* conference in Vancouver, British Columbia. The panel consisted of *Microsoft's* Larry Tseng, Darren Kessner of *Symantec*, Paul Ducklin of *Sophos*, Nick Fitzgerald of *Computer Virus Consulting Ltd*, *FRISK Software's* Vesselin Bontchev and David Chess of *IBM*. I moderated the session, the main topic of which was 'What should we do to prevent viruses?'.

A lively discussion resulted in several valuable contributions made by both the panellists and members of the audience. Since a large majority of the proposals involved actions on the part of *Microsoft*, I proposed that an open letter be sent to Redmond.

Four main proposals emerged from the discussions:

1) *Microsoft* should provide code signing which would ensure that whenever an application is started, its signed checksum is compared against *Microsoft's* public key and the execution only allowed to proceed if the signature is valid. The overhead in doing this was not judged to be unacceptable.
2) During the installation of *Microsoft Office*, the user should have an option not to install macro capability. The resulting installation would be secure in a similar way that *Word*, *Excel* etc viewers are secure, since they cannot execute macros.
3) *Microsoft* could provide the option of storing macro code in one file and data in another file, for example ABC.DOC being the document and ABC.MAC being the macros belonging to the document. This way the user would have the choice of either sending macros to his correspondent or not.
4) *Microsoft* should be much more open in publishing information on data file formats. This was a request by anti-virus companies who could spend time which they currently use in reverse-engineering *Microsoft* formats in combatting viruses. This could take the form of RFC-style documents.

Jan Hruska
Sophos Plc
UK

Agreeing to Disagree

Jakub Kaminski's objections (see *VB*, September 1999, p.4) to Jeremy's 'good' Aprone virus (suggested in the Letters section of the previous issue) are, of course, well-founded.

Perhaps, though, we should not be too discouraging. The problem is the viral mechanism, rather than the underlying concept. There are possible non-viral implementations which would avoid some of the problems. For instance, a memory-resident utility could work along the lines of:

IF (file is opened for writing)
AND (file is executable)
AND (file is not on exclusion list)
THEN
(checksum original file)
(copy original file to holding area)
[. . .]
IF (file is closed)
AND (file has been modified)
AND (file has been copied)
THEN
(overwrite modified file with preserved copy)
(compare checksums)
(delete preserved copy of original)

It is no panacea (it still does not address the macro virus problem, for instance), but it could be a viable supplement to a scanner. At any rate, there are worse 'solutions' on the market…

David Harley
Imperial Cancer Research Fund
UK

An Axe to Grind?

A year has now passed, but the memory of catching eLeprosy remains still fresh. On a Friday afternoon last November I checked my mailbox and yes, there was the expected email from Sydney, replying to my inquiry about Y2K job opportunities overseas.

Within the reply were two attachments. Upon closing the company profile document why was the VBA debugger suddenly displaying source code? It read 'you are a Big Stupid Jerk' on the 14th of the month between June and December. A quick cut and paste captured the viral code and adrenalin levels rushed skywards.

That entire weekend I attempted to understand the gate-crasher. The alternating comment lines were all the same:

```
"user29/09/98 16:22:40Canon  BJC-4200 on
LPT1:APROFILE3 W6"
```

Were these the previous victim's Registry values? Had they had the infection for six weeks? How many of their clients had similarly received the infected company profile document? And who was this bloke VicodinES and what did /TNN and /CB mean?

AltaVista came to my rescue – The Narkotics Network and CodeBreakers were the answers. As for VicodinES, what to make of him? Obviously a rapidly rising star within the vX underground, an interesting dude to *cyberstalk*, no doubt I mused, just don't tell Al Gore!

Now, to whom to report the incident first thing Monday morning? Alan Candy, a WildList contributor, seemed an obvious choice and Sarah Gordon; she sounded cool.

Before seeing Alan, I rang Sydney, to impress upon them the fruits of the weekend's cybersleuthing. I said 'Listen mate, as fellow victims, if we cannot cooperate on this, the cyberhoons will ride rings around us every time, and by the way I reckon your initial infection was at 16:22 on 29 September 1998, *and* your default printer is a Canon BJC-4200, right?'. The Ozzie bloke had a gush of verbal diarrhoea; 'Yes, sorry mate, we got the infection from our Head Office in London, yes, about six weeks ago. We have been trying to disinfect but have been unsuccessful.'

After hanging up, I thought what a *dork* confirming all that. Alan quickly put the diskette under the *AVP* microscope. 'You've got a Class.D infection here and this is now the second independent reporting that I've received for the WildList. Thanks for coming in, but here, please sign this non-disclosure agreement.'

'No worries, only too pleased to help out. Now how about you phoning Sydney with the news and a disinfectant?' So Alan rang, only to be rebuffed by alarming disinterest. I then asked him to recommend a news reporter who could investigate this sorry cover-up carefully. He suggested Chris Barton, the IT Editor at Auckland's *NZ Herald*. By the time Chris phoned the rot had firmly taken hold. Last December, Chris wrote two excellent albeit subdued articles about Class.D fiascos Down Under.

Meanwhile as the cyberstalking of Mr Vic became my daily ritual and addiction, the numerous requests to liaise with London went unanswered. I obviously needed an eLeprosy cure real bad. Finally, I leave you with these questions:

a) Is this typical of anti-virus deployment within 'professional organisations'? The other victim's main business is Taxation Consultancy and tax departments worldwide remind all taxpayers that ignorance of the law is no excuse!

b) What is the state of anti-virus deployment amongst the millions upon millions of home users who busily cruise the ehighways daily without adequate warrants of efitness?

c) Does *Microsoft* get the last laugh over Mr Vic? Only the previous month I had upgraded *Office 97* to SR-2 thereby inflicting a run-time bug on Class.D (my only other AV protection was an out-of-date *McAfee*).

Brien Barlev
'Millennium Viking'
NZ

Praise Indeed!

What did I think of VB'99 and what did I get out of it? I was very impressed at the largest attendance ever of security professionals at this year's *Virus Bulletin* conference. This is by far the best anti-virus security event for those of us from very large corporate companies. Candid, straight-to-the-point subject matter, helpful open debates and question and answer format, various current and future contents for corporate and technical streams combine to make it the best of its class.

In the years that I have been a part of the conference, whether as a speaker or a delegate, I have always left with a feeling that I have gained highly valuable information that helps mould the direction of company policy and procedures for the future, especially this year's Y2K theme. I have noticed that the *VB* conference has a large international corporate attendance when it is held in the Western hemisphere, while still keeping a sizeable European presence. The personal atmosphere and actual interaction with the world's leading anti-virus industry experts and corporate personalities is priceless.

Shawn Campbell
Global Anti-Virus Project Manager, Ford Motor Company
USA

Positively No VB 100%?

Virus Bulletin is staying timely with the introduction of the requirement of 100% on-access detection in order to receive the VB 100% award and we are glad to see the additional requirement. However, we feel there is still a small requirement missing – false positives.

Easily, I could create a small program, EricAV.EXE, that simply identifies all objects as infected with the 'Ceskie virus'. This program would then receive the VB 100% award and be entitled to the usage of the logos and everything else that comes with acheiving it. Obviously, this would de-value the VB 100% award.

Yes, this is an extreme example, but hopefully clearly demonstrates the point. Achieving VB 100% can be made more meaningful with the additional requirement of no false positives (and considering a false postive test is already performed, I would doubt there are any logistical nightmares associated with the additional guideline).

Virus Bulletin not only provides a valuable service to anti-virus consumers by providing reviews and insights into the virus world, but also forces improvements in anti-virus products from detection to usability. We believe anti-virus vendors should continue to be challenged and held to higher and stricter bench marks. At *Symantec*, we encourage the addition of 'False Positve = No VB 100%'.

Eric Chien
Senior Researcher, SARC EMEA
Leiden, The Netherlands

VIRUS ANALYSIS 1

Freelinks To Infection

Vanja Svajcer
Sophos Plc

Rapid spread is inherent in today's most successful viruses and Worms; to achieve this, they exploit features and protocols used in network communication. WM97/Melissa sends emails with infected attachments to the first 50 contacts from the *Microsoft Outlook* address book. The W32/Ska Worm, more commonly known as Happy99, patches the WSOCK32.DLL in order to utilise email propagation. W32/ExploreZip replies to previously received email messages with an infected attachment and spreads across LANs using *Windows* networking.

Recently, a Worm written in VB Script has hit user machines. One of Marius Van Oers' points in his VB'99 conference paper 'Automating MS Outlook – VB Script' was that the power of VBS should not be underestimated. VBS viruses are not new to the anti-virus community – they are usually very simple and incapable of spreading.

At the time of the conference, we were already aware of a VBS Worm capable of spreading not just by using *Outlook's* automating capabilities but also by using other mechanisms. *Sophos* received only a few infection reports and samples of the Worm during the first weeks of July. The Worm was called VBS/Freelinks, and once we produced detection signatures, we did not expect to see it in the wild. However, a variant did appear a few weeks ago, at the end of September.

Spreading Method(s)

If Melissa spread quickly using only *Outlook's* automation, perhaps we should consider how quickly a Worm like Freelinks might spread? After all, it incorporates three more spreading mechanisms. Obviously, the answer depends on the infection path and how frequently the affected applications are used.

How likely is it that a user would send a VBS file as an email attachment? Moreover, how likely is it that the recipient would execute the attachment? As it happens, in the current climate, not very likely. What if the script is set to create a message automatically which then invites the recipient to execute the attachment? If the attachment is executed, an interesting stealth mechanism might be observed – a payload that conceals the actual function of the attachment might be incorporated into the virus.

Today, email is one of the most popular communication methods. Undoubtedly, a Worm capable of accessing all entries in the email client address book and sending a message of itself as an attachment to them all would indeed soon be considered a 'successful' virus. The author of Freelinks obviously thought so, since this process is incorporated into this Worm. The email message subject is 'Check this' and the message body is 'Have fun with these links'. The name of the attached file is LINKS.VBS. To increase the speed of propagation, the Worm also uses the *mIRC* and *PIRCH* Internet Relay Chat (IRC) clients as well as the *Microsoft* network drive sharing service. It would be a fairly safe bet that the most effective propagation of Freelinks occurs via email attachments.

VBS Code

One of the vulnerabilities of VBS viruses has been the fact that they have not been able to conceal their code. VBS code is not compiled, and the scripting language is easily understandable. A knowledgeable user can open the script with any text editor program, quickly recognise and remove the potentially malicious code. Freelinks and some other VBS viruses use encryption techniques so that the code is not instantly recognisable.

The Freelinks Worm contains two files, LINKS.VBS and RUNDLL.VBS: one is contained within the other in encrypted form with functionality divided between them. When a recipient executes the viral email attachment, the script launches and opens the LINKS.VBS file. It then looks for the string "`sd]Lhbsnr", starting from the fortieth position in every code line. The decryption key can be found at the seventieth position of the line containing the above string. The decryption routine is a simple function that is called on demand each time an encrypted character string has to be used. Depending on the ASCII character number (odd or even), the routine either adds or subtracts the rightmost decimal digit of the key (incremented by 1 to get a plain text character).

The script then queries the *Windows* registry to get the system folder so it can create the RUNDLL.VBS file in it. It also creates the *Windows* registry key:

```
…\Microsoft\Windows\CurrentVersion\Run\Rundll
```

and sets it to 'RUNDLL.VBS', ensuring that the script runs every time *Windows* is started. Up to this point in the infection process, the user still cannot see anything to do with the promised links and may become suspicious. Therefore, the Worm provides links to cloak its presence. It displays the message box shown overleaf.

If the user clicks 'Yes', Freelinks creates a shortcut file pointing to a Web site with explicit adult content. Furthermore, the user can 'have fun' as the Worm continues to run. Using the automation model, it creates a Wscript.Network object and uses it to find any shared network drives mapped to the user's computer.

If a shared drive is found, the Worm copies itself to it. Using a similar automation technique to that used by the Melissa virus, the Worm first attempts to get a handle to *Microsoft Outlook 98* or *Outlook 2000* by creating the Outlook.Application object. If the handle is returned, it uses MAPI calls to find *Outlook's* address book entries. Once found, it creates a new email message, puts the email address of each entry to the Bcc: field and places the message into *Outlook's* Outbox. As with Melissa, the quantity of traffic generated might overload servers, causing them to shut down.

The RUNDLL.VBS file runs every time the OS is started. Using the same decryption method as LINKS.VBS, the script creates C:\WINDOWS\LINKS.VBS to ensure re-infection. RUNDLL.VBS uses Scripting.FileSystemObject to look for *MIRC* and *PIRCH 98* folders. If either of the folders is found, the Worm checks if a MIRC32.EXE or PIRCH98.EXE program exists. A similar process is used for every sub-folder in the Program Files folder.

If MIRC32.EXE is found, the script creates a SCRIPT.INI file which uses the direct client connection (DCC) send function to send C:\WINDOWS\LINKS.VBS to other IRC users. The triggering of the command is done by the ON JOIN event that occurs when a user joins an IRC channel:

```
n0=on 1:join:#:if $me != $nick dcc send $nick
C:\WINDOWS\LINKS.VBS
```

If PIRCH98.EXE is found, an EVENTS.INI file is created which uses a variant of the DCC instruction in order to send the worm to other IRC users:

```
[000-Unknowns]
User1=*!*@*
UserCount=1
Event1=ON JOIN:#:/dcc send $nick
C:\WINDOWS\LINKS.VBS
```

Again, it is only by luck that this Worm does not have a destructive payload. VBS is a powerful scripting language, and it is capable of controlling and automating applications, not to mention almost every aspect of the computer system, including file management. It is not difficult to imagine the damage that could have been caused by the destructive payload of the ExploreZip Worm. Looked at in this way, one could say that infected users were lucky, this time.

Prevention

We saw the first samples of the Freelinks Worm in July, but why did they not spread then? Why the recent outbreak? Is it because more people started to install *Windows 98* or *Microsoft Explorer* versions 4 and 5 so that they were actually able to run VBS scripts? Is it a mere question of luck? The probable answer to both of these questions is 'Yes'. The ability of the viruses to spread may have been increased by its packaging – that is, a message inviting the recipients to have fun with the links.

One reason why the Worm has broken through some anti-virus defence lines may be the result of some AV products not being automatically configured to scan files with the VBS extension. Thus, it may have escaped detection even if the scanners are capable of detecting it [*as verified during this month's Comparative Review, Ed*].

So what can we do to prevent email Worms? Once the Worm is on the desktop, it needs user intervention (opening an attachment), and the user is the one who is ultimately responsible for the decision to launch the attachment or not. Although user awareness following Melissa and W32/Ska attacks has reached higher levels, more is needed to ensure that everyone understands the seriousness of the matter.

Opening attachments and non-trusted programs prior to them being checked in a safe environment should be regarded as a serious security breach. Users should be warned that such actions may lead to actual damage not only to the user's computer, but to the company's entire system. A proper security policy is important and, if properly implemented, can prevent viruses from spreading through internal and external computer systems.

Some companies have already introduced the stripping of all attachments from both incoming and outgoing messages as a part of computer security policy. The applying of regular updates to the virus signature databases and ensuring correct anti-virus program configuration is an essential preventative measure.

Although many companies have started to implement restrictive security policies, there will always be those who will continue to disregard the warnings. We have seen enough big corporations hit by a Worm or a virus in the past to know that they will undoubtedly be hit again. Why? There will always be a handful of users who love to have fun with links!

VBS/Freelinks

Aliases:	WScript/Freelinks.
Type:	Worm.
Spread:	Via email, IRC and across networks.
Files Used:	LINKS.VBS, RUNDLL.VBS, SCRIPT.INI, EVENTS.INI.
Removal:	Remove the Worm entry from the *Windows* registry and delete any Worm file instances. If *mIRC* or *PIRCH 98* clients are installed, delete appropriate script file.

VIRUS ANALYSIS 2

Inside Infis

Andy Nikishin
Kaspersky Lab

Until now, there have only been two 'virus-friendly' operating systems – DOS (and *Windows 3.x*) and *Windows 9x*. Viruses for them are estimated at tens of thousands. *Windows NT* was not in this category. Yes, there are a few viruses that use Win32 APIs to spread on *Windows 9x* and *NT* but, so far, there has only been one *NT*-specific virus, RemoteExplorer. Now we have another – WinNT/Infis.

This is a memory-resident, parasitic, *Windows NT* virus. It only operates under *NT v.4* and is not able to infect files under *Windows 9x*. The virus does not have a payload and does not harm the system. However, it has a bug in its infection routine and corrupts some files while infecting them. When run, the corrupted files put up the standard 'is not a valid Windows NT application' error message.

Memory and Program Infection

Infis remains in memory as a kernel mode driver, which hooks on file opening and writes itself to the end of PE files (Win32 Portable Executable files). The virus infects all PE files with .EXE extensions, except CMD.EXE. It does not check the read-only attribute and cannot infect files with this attribute set. Furthermore, it does not save the original timestamp of the infected file.

Infis sets the file time and date double word stamp in the PE header to -1(FFFFFFFFh) to mark infected files. While infecting a file, the virus increases the size of the last section, writes itself there and modifies the necessary fields in the file header. As a result, when infected PE files are executed, the virus code receives control and runs the installation routine.

This routine copies Infis to the system and registers it there. To do that the virus extracts its 'pure' code (4608 bytes) as a standalone PE EXE file with the name INF.SYS and writes it to the %SystemRoot%\system32\drivers directory. It does not check for the presence of the dropper and writes INF.SYS every time during its activation.

Next, the virus adds 'run-it' commands to the system registry by creating a new Registry key with three values:

```
HKLM\SYSTEM\CurrentControlSet\Services\inf
   Type = 1
   Start = 2
   ErrorControl = 1
```

The 'Type' section value (SERVICE_KERNEL_DRIVER) means that the virus is loaded as a standard *Windows NT* driver. The next value, 'Start', signifies startup type (SERVICE_AUTO_START) and forces *Windows NT* to load the viral INF.SYS file when *NT* is started. The final value, 'ErrorControl' (SERVICE_ERROR_NORMAL), means that if the driver fails to load or initialize, startup should proceed but display a warning message. It is necessary to have administrator rights to create these keys in the Registry.

Thus, the virus dropper is loaded as a system *Windows NT* driver on the next system restart without depending on user account's rights and permission. When the INF.SYS virus dropper takes control the virus allocates a block of *NT* memory, reads its complete copy from the INF.SYS file for further use in the infection routine, and hooks INT 2Eh by patching the Interrupt Description Table.

The INT 2Eh interrupt is completely undocumented, and it is used to call *NT* system functions, including file accesses. The INT 2Eh virus hooker only intercepts the file open function, checking the file name and extension. It then opens the file, checks its format and runs the infection routine. Infis uses the INT 2Eh interface even in *NT* user mode and does not call any Win32 API functions.

This virus cannot run properly under *Windows NT v.4 Service Pack 1*, *Windows NT 3.5x* (all Service Packs) and *Windows 2000* (all betas). This is precisely because of the undocumented nature of INT 2Eh interface.

Recognition in Memory

It is possible to see the name of the loaded virus driver by checking the Devices list or using *NT*'s Diagnostic tool or Registry Editor. Interestingly, the virus driver has a correct unload procedure; it can be stopped easily with the Device Manager 'Stop' button.

You may say 'This is a primitive *NT* virus using old DOS techniques to intercept *NT* events. Why are you threatening us with it?'. You are right. However, this virus is only the first indication of something with terrible potential.

WinNT/Infis	
Aliases:	None known.
Type:	*Windows NT* PE infector.
Intercepts:	Undocumented *NT* internal interface.
Payload:	None.
Infects:	Executable files with EXE extensions (except CMD.EXE).
Removal:	Unload virus driver, delete INF.SYS and restore infected files from backups.

FEATURE SERIES

Macro Viruses – Part 3

Dr Igor Muttik
AVERT Labs, UK

When different macro viruses meet on one user system they may mate. WordBasic copies macros by name. If two viruses have the same macro name one virus may copy a macro belonging to another virus. Then this cocktail may be able to travel with one (or several) macros substituted. Such mated viruses do exist and they replicate happily with the macros 'borrowed' from other macro viruses.

Viruses can also snatch macros from a set of legitimate macros in NORMAL.DOT. For example, there are many known macro viruses which are the result of mating between the ScanProt macro (the anti-Concept macro released by *Microsoft*) and this or that other macro virus.

VBA5/6 viruses also are able to mate. Apart from just two sets of macros being present in one document, they now can merge inside a single module. Most contemporary viruses live in the class module called 'ThisDocument' (or 'ThisWorkbook' for *Excel 97* or *Excel 2000*). If two viruses using the same class module infect one DOC file they can:

1) stop working if they use the same functions (e.g. two functions for 'Document_Open' in one module produce a VBA error)
2) live happily together (e.g. one infects on 'Document_Open', another on 'Document_Close') and spread together, one attached to another
3) produce a mixture, the behaviour of which would depend on which virus' function is used to replicate the cocktail. Such behaviour can be very complex depending on the history – it may devolve to non-replicating samples, lose some modules or functions, etc.

Devolving

Some viruses are badly written and can lose their own macros. For example, the original virus consists of a set: {AutoOpen, FileSave, and FileSaveAs}. If it replicates via AutoOpen the whole macro set is preserved, but if the user invokes FileSaveAs the virus fails to copy FileSave.

The resulting virus – {AutoOpen, FileSaveAs} – is called a devolved macro virus (of course, only if this reduced set is able to replicate recursively, i.e. we have a 'viable devolved virus') and the original virus is known as devolving. A virus can devolve more then once (losing different macros) resulting in many different variants. Such variants are distinguished by attaching a digit to the name, e.g. WM/Rapi.A and WM/Rapi.A1 (the WM/Rapi family is famous for having several devolved variants).

In some cases a devolved virus no longer works and we get a 'non-viable devolved virus'. These do not replicate but anti-virus programs should still be able to detect and clean them as they occur as a result of a viral activity.

Naming

There is an email group called VMacro consisting of the most active anti-virus researchers in the field. They share the identification data (not the virus samples – they are sent more carefully within *CARO*), discussing the family relationship of macro viruses, their names and other issues related to macro viruses.

It was decided that names of macro viruses start with a platform identifier – WM (*Word* Macro for viruses using WordBasic), XM (*Excel* Macro for VBA3), APM (*AmiPro* Macro), A97M (*Access 97* Macro), W97M (*Word 97* Macro), X97M (*Excel 97* Macro), PP97M (*PowerPoint 97*), CSC (*CorelDraw Script*).

Then, the family name (e.g. Wazzu) goes after the slash separator, followed by a dot and a variant suffix (which can be omitted). Variant suffixes start at .A and go through to .Z, then start again at .AA to .AZ, etc. If the virus devolves the index is attached to every variant. For viruses which infect all *Office 97* applications an O97M prefix can be used or multiple prefixes can be grouped in curly brackets {W97M/X97M}. This also applies to multi-partite infectors hitting, say, DOCs and EXEs {W97M/Win95}:

WM/Wazzu.A

WM/Concept.A

WM/Npad.BV

APM/GreenStripe

WM/Rapi.E2

XM/Laroux.B

W97M/Appder.B

X97M/Laroux.JH

O97M/Tristate.A

{W97M/X97M}/Shiver.A

{W97M/Win95}/Coke.22231.A

A97M/AccessiV

CSC/CSV

If the virus is language-specific (e.g. it replicates only under a localized version of *WinWord*) the virus name can be followed by a country designator. Internet abbreviations are used, such as ':De' (for Germany) or ':It' (for Italy). [*This is the final part of the consecutively published series on macro viruses. Ed.*]

OPINION

Ramming It Home: The Universal Generics

Peter Morley
Network Associates Inc

[*Back in the July issue Peter Morley aired his initial views on Generic Repair. Readers are urged to remind themselves of his Tutorial on p.10 before reading this follow-up. Ed.*]

The time is nigh when the flow of 'OFFVs' (old-fashioned file viruses) will almost dry up. Those which do still come will be written in faraway places like Taiwan and South America. Furthermore, one may have to trawl the Bulletin Boards in order to get them.

I reckon it will happen sometime within 18 months to five years from now, and when it does, the anti-virus vendors will take the decision only to process new ones which come from the wild. You will know when it does happen, because the *Virus Bulletin* Pie Chart, which still showed a file virus total of 17.4% in August 1999, will show less than 3%.

When that day comes, our customers will continue to expect their anti-virus products to handle all the viruses thrown at them, particularly if they get an outbreak! It follows that the code which handles these viruses should be subjected to ruthless efficiency reviews, and that all the dead wood should be chopped out whilst detection and repair capability should be left unscathed.

A typical example is the overwriting viruses which have to be dealt with by replacing the original files. As long as we detect them, our customers do not care what esoteric name we call them. They just want to get rid of them, and move on. So, we can save a lot of code by losing all the funny names in addition to all the functions which differentiate between them.

In fact, we have made a token start, on the Trivial.ow viruses, but there is a long way to go before we can report *all* overwriting viruses under a single name. As usual, the proverbial will hit the fan if we cause any false alarms along the way.

Construction Kits

The prime example resulting from the question 'Do we really need to distinguish between them, as long as we can repair them satisfactorily?' is the viruses written using construction kits. Yes, we must repair them, because new variants keep appearing in the wild, because little Johnny played with the kit last Sunday afternoon. However, does it really matter what we call them? The kits I have in mind are IVP, VCL, PS-MPC, and BW.

My first 'Universal Generic' was IVP.GR to detect and repair IVP variants. It worked well, but a number of incidents did occur. For starters, I found it detected and repaired lots of PS-MPC viruses, and lots of VCL viruses too. At that point, there were no complaints about naming.

So, I renamed it Univ.GR5. Then I took out a large amount of code which was no longer needed to detect and repair large numbers of MPC and VCL viruses.

This was a happy start. However, what about all the other viruses it detected and repaired? I had several happy days searching for and removing drivers which I (and quite a few other people, including Alan Solomon) had sweated blood over. The loss of virus names annoyed no-one, with the possible exception of the authors.

The second stage was obvious – write generics to handle as many of the remaining MPC viruses as possible. I had just about finished (or thought I had), when the VKit collection of 15,000 new viruses arrived. Some tidying up, and one additional generic, was required but we survived VKit with a minimum of difficulty.

It was time to be venturesome. A shady area in the code was the Vienna family of viruses. Everyone had made excuses not to change it, and written a separate driver for any new variant! When I made it generic, there was a lot less code!

At the time of writing there are 10 'Universal Generics', but the number will only rise very slowly from now on.

The Big Problem

The big problem with this can be summed up in two words – Generic Misrepair. It occurs when our generic makes use of the virus code, but that virus code has bugs or behaves in a way different from that expected. It is important that we handle this, because virus authors have no tradition of testing their products!

Luckily, the solution is simple. What is required is a separate driver to detect and repair that variant before the generic gets to it.

The prerequisite to all this is knowing which variants would be misrepaired. So, properly planned testing of all new generics is a must. Currently, we think we have got it right. I do not recall a field complaint about Generic Misrepair.

Glitches

One minor incident occurred long before I embarked on the generics project. Many variants of BW and of MPC use the same decryptor, and we detect the decryptor to avoid

having to decrypt before we detect. However, in the BWs, the COM file repair data (usually three bytes) is between the end of the original file and the start of the virus, whereas the MPCs keep the repair data in the virus code.

This resulted in a new MPC virus being identified and repaired as an existing BW virus, so three bytes too many were chopped off! As a result of this old incident, our generics play it safe. Generic repair of some BW viruses now leaves three extra bytes on the end! They have no effect, but I did not like leaving them there.

Full Steam Ahead

Having completed the packages, the next question is obvious – what about all the other drivers which repair several variants of the same virus? Is it not possible to make them generic too? The answer must be 'Yes', so we went right through the database, doing all the easy ones.

There are still a few which need a second look, but we have now reached the point where over half the new viruses we receive in monthly collections, are already detected and repaired correctly. All we have to do for these is:

i) Check the repair

ii) Add them to the count

What about the ones we detect and repair correctly, and never see? They never get added to the count, so you can expect it to be an underestimate from here on.

Strategies for Writing Repair Code

Before the advent of Generic Repair, it seems that two totally different strategies were in common use:

i) Do the repair at the time you first process the virus, if and only if it is a field virus

ii) Do the repair initially, whether it happens to be a field virus or not

My personal preference is strongly in favour of the latter procedure because one makes the first attempt at repair at a time the virus is understood. We have an unwritten rule at *NAI* that if repair is not possible we note why not. We also document any new tools or improvements to existing tools which will make it possible. The net effect is to accelerate the advent of the new tools.

Now generics have come along, it dramatically changes the way we write repair code. There are two new rules:

i) When you process a completely new virus, do it in such a way that the procedure for the next variant of this virus will be easy

ii) When you get the second variant, modify the existing driver and make it as generic as possible. This takes a little extra effort, which is repaid many times over, when later variants need little or no effort

The development of these procedures has been helped by something which at first glance seems irrelevant – the advent of the macro virus. Since that time, the fact that repair is usually essential has signified two things; from the start, all drivers for handling macro viruses have been made as generic as possible, and the rapid development of repair tools has been essential. Together, these two things have had the effect of making both the above procedures easier, by speeding them up.

A Sting in the Tail

When we first received the TMC virus (Tiny Mutation Compiler), which is not encrypted, but is polymorphic all the way, we all tried to do the repair and failed. Recently, some eighteen months later, using just one of the tools developed since, the TMC repair had become possible for both COM and EXE files. It is in DAT 4045 onwards, so if it ever reaches the field, it will be a non-event. More important, however, is the fact that similar viruses will probably not be a problem in the future.

If anyone else has written a repair for this virus, and can show it, I will happily buy him a drink!

Keeping up to Scratch

In an era when a lot of new tools are being added to anti-virus products, it is essential to ensure that adding a new facility does not accidentally invalidate an existing one we all take for granted. With this in mind, we have prepared a small collection of viruses, which exercise many of the common repair techniques.

The guiding principle has been variety, but TMC is in there! This collection is available to any bona-fide anti-virus concern which would like it. It is also available to *bona fide* reviewers who would like to use it for testing repair capability.

Where Does This Leave Us?

Given that here at *Network Associates Inc* we were getting 500 new viruses per month, and that it takes up to three months for a virus to reach us, it would appear that at any time there are about 700–800 viruses out there that we have not seen yet. We handle just over half of them, but that still leaves 300–400 which require attention. That figure is reducing gently.

May I suggest that you read this last paragraph again if and when anyone ever makes that well-known claim to you, 'Our product detects all known viruses'.

The old-fashioned file virus game is winding down albeit several years later than most people (including me) thought it would. However, the Trojan/Malware game is still expanding fast, primarily because of the Internet. As for the macro virus game, it is still growing like crazy, and will continue to do for some time to come.

CONFERENCE REPORT

Canadian Club

Francesca Thorneloe

There was a core impression of tighter unity and better understanding among this year's *Virus Bulletin* conference delegates. In fact, from the start of the event at 9am on Thursday 30 September my first Editorial Address to all the attendees embraced that concept with the subject of sticking together and working as a symbiotic unit. It soon became apparent that I was not alone in my thinking.

First Impressions Last

Conference Manager Jo Peck mentioned in her post-Gala Dinner speech that this was a year of firsts for *VB*. VB'99 was her first opportunity as primary organiser to take control of the conference co-ordination and the result was a slick and seemingly effortless couple of days set amongst the most stunning scenery in the Pacific North West.

It was also Fraser Howard's first conference since coming on board as Technical Consultant for the magazine. Characteristically, he relished the challenge, delivering a universal and candid retrospective of the year, throwing in his confident predictions for the coming Millennium.

Despite this having been *Virus Bulletin's* ninth international conference and tenth anniversary year, for this particular *VB* team it is only the beginning.

Now you see it, now you don't – with *VB* Technical Editor, Jakub Kaminski…

Rocky Mountain High

The venue certainly did its bit to help. The Hotel Vancouver opened its doors to the biggest *VB* conference to date, and we were admirably looked after. Wednesday evening's Welcome drinks reception in the spectacular Roof Room showed off the city of Vancouver to its greatest advantage. Old friends were given a chance to introduce themselves to new faces aided by plentiful and exotic finger foods and local beer and wine. From the off, lively and proactive discussions seemed the order of the day. Debates were often to carry over from presentations into typically British Columbian breakfasts and lunches.

Taking timely advantage of the wealth of experts gathered in one place, extra-curricular meetings such as those for the *ICSA* and *The WildList Organization* took place between sessions. This year also witnessed a marked increase of partners at the event, a welcome development which culminated in as even a match as we have seen on the dance floor on Thursday night. Wives and girlfriends confessed to feeling part of the AV family and the Swimmer baby made an awful lot of friends!

The Gala Dinner and Dance took place in a truly celebratory style. Clutching their champagne flutes, slightly suspicious but good-humoured delegates were issued with black trilby hats and sunglasses on entering the stunning Pacific Ballroom prior to sitting down to a sumptuous five course meal. The Blues Brothers Band took over and, as they say, the rest is history.

United We Stand

The conference itself was seamlessly executed and extremely well-attended. Huge multi-national conglomerates such as *Boeing*, *Shell*, *UPS* and *Ford* rubbed shoulders with Government agencies like *NATO*, *NASA* and the armed forces. Software giants *Microsoft*, *Compaq* and *Intel* were well represented, as were charitable organizations including *Imperial Cancer Research*.

This year's press contingent was the largest so far, with delegates from US, Japanese, German and UK publications registering. Educational establishments sent particpants from a wide selection of schools and universities across America, England, Poland and Denmark.

SARC's Chief Researcher Carey Nachenberg kickstarted the proceedings with the keynote paper on computer parasitology which managed to be simultaneously dynamic and hilarious, serious and premonitory. The audience, technical and corporate, was united in appreciating his humour and his controversial predictions, not to mention his stochastic simulation.

When visa problems prevented the participation of scheduled speakers Costin Raiu and Adrian Marinescu from *GeCAD*, Romania, the unity continued. Sarah Gordon and Richard Ford, *VB* old-timers and always enthusiastically received, appealed to both corporate and technical audiences with their timely and relevant discussion about information sharing into the 21st century.

Speakers' Corner

Having made the difficult and painstaking decision of paper selection back in the spring, we were confident that our speakers – from Dave Phillips, Computer Virus Control Officer for the *Open University* to Dave Black, a Royal Canadian Mounted Policeman – reflected the diversity and

scope of the conference delegates. Topics covered the spectrum from mathematical algorithms to *EICAR* test files by way of Java and network-aware malware.

Old familiar favourites like *IBM Research's* Ian Whalley and *Sophos'* Paul Ducklin were joined by newcomers to the *Virus Bulletin* conference circuit. Two representatives from *Kaspersky Labs*, Andrews Nikishin and Krukov, *Symantec's* Eric Chien and *Data Fellows'* Katrin Tocheva joined Marius Van Oers from *NAI* for the first time on the speaker's podium.

There was something for everyone. Audiences were treated to tutorial-style sessions from *Computer Associates'* Rob Stroud and Christine Orshesky from *i-secure Corporation*, while timely discussions on *Office 2000* were delivered by *Norman's* Righard Zwienenberg and *Symantec's* Darren Kessner. An impromptu technical panel session resulted in a suggested open letter to *Microsoft* published on p.4 of this issue. Vesselin Bontchev's controversial paper 'The WildList – Still useful?' can be found at the following URL: http:www.complex.is/~bontchev/papers/wildlist.html.

There were the usual highlights and gems which give *VB's* conferences their individual flavour. This year's classics included Nick FitzGerald's spontaneous and emotional rant against application designers and Graham Cluley's 'dancing pigs', one of which just happened to be his boss, Jan Hruska of *Sophos Plc*.

Graham Cluley and friends tackle the serious issue of Y2K…

The well-placed and bustling exhibition had its share of firsts too. The big names were all there, joined for the first time by *Sybari Software* and *Panda Software*. Raffles, freebies and demonstrations served to make coffee breaks interactive and entertaining for all.

Always a firm favourite at *VB* conferences, and an opportunity for all the attendees to reunite, the closing speakers' panel session was professionally overseen by *IBM Research's* Steve White. Playing to a full house, Graham Cluley, Sarah Gordon, Péter Ször, Rob Stroud, Carey Nachenberg and Ian Whalley took questions from the floor.

AV heavyweights Jimmy Kuo and Dmitry Gryaznov got the session off to a provocative start with their reactions to the annual enquiry 'will your virus problem be worse or better this time next year?'. The old chestnut of the relationship between virus writers and anti-virus companies also came up, but even this, usually accompanied by hot tempers and flare-ups was friendly in nature and conciliatory in tone.

An exercise in cool. No wonder we asked Steve White to chair the Speakers' Panel session…

Attendees of VB'99 are urged to fill in their assessment forms and post them back to *Virus Bulletin*, so that we can improve on this year's conference. Early records of conference assessment forms already submitted reveal an energetic, comprehensive audience eagerly anticipating VB 2000.

Indeed, CDs of this year's proceedings (see the News page) are still selling fast. Not featured on the CD are Dmitry Gryaznov's technical paper 'Upconversion 2000' and Graham Cluley's presentation, which can be found at the *VB* Web site http://www.virusbtn.com/. Hard copies of Robert Vibert's corporate talk '101 Criteria to Consider for Enterprise-Level Anti-virus' are available by special request from *Virus Bulletin*.

After much consideration and a substantial recovery period, 'Men of the Match' for this year's event have been elected based on the delegate assessment that we have managed to gauge so far. They are, unanimously, key note speaker Carey Nachenberg, Graham Cluley and Péter Ször, the latter presenting the most popular technical paper on 'Memory Scanning under Windows NT'.

Ian Whalley asks 'What happens if I press here?' Carey Nachenberg is keen to find out…

A DAY IN THE LIFE

The Virus Police

Dave Black
Royal Canadian Mounted Police

A veteran computer virus response expert knows it's going to be a bad day when the radio report during the drive to work is about the newest, 'fastest spreading, most destructive' virus ever. Another clue comes when a colleague hands you a newspaper article about the very same virus before you can turn on your PC. Then, before you can pour your first coffee, the phone begins to ring. You have not even checked your email yet!

This was not going to be an average day for me, a Civilian Member IT Security Consultant with the *Royal Canadian Mounted Police*. It was one, however, that would consolidate, in a few short hours, all the typical activity that goes on with a response to a virus incident within the Canadian federal government departments.

I have been researching virus threats and responding to incidents for the past six years, and this particular day the Melissa virus would be handled in the same comprehensive way that the *RCMP* has dealt with viruses over the last decade. This specialised type of work has given us the unofficial tag, the Virus Police.

Inside the RCMP

Why is the *RCMP* involved in this non-traditional line of work? Our role in terms of virus fighting has not been publicized over the years, due partly to the conservative nature of the organization, but also to a well-defined client constituency and no need for an additional workload.

Recent developments and local media reports have highlighted some of the *RCMP's* successes in this particular area and served to emphasize the importance of technical expertise in the police organization. This expertise has developed from years of cooperation with large Canadian federal government departments, which, in turn, has fostered close working relationships and offered a unique perspective on the virus situation in Canada. Unlike the traditional image of the *RCMP's* law enforcement role, the force's Technical Security Branch (TSB) is organized on a functional basis to serve Canadian federal government clients and other police agencies.

The major component of the branch is the Security Evaluation and Inspection Team or SEIT which was formed in 1974 in response to a need for improved security at computer installations where federal government information is processed. SEIT is made up of regular and civilian members, who share backgrounds in various fields of technical specialization. One of the uniquely Canadian advantages to this arrangement is that the entire nation is small enough, population-wise, to manage this role on a centralized basis.

Time and time again, during SEIT security reviews, it has been found that computer viruses are the foremost practical threat to systems and data in Canada. Accordingly, and also within the TSB, the Computer Investigative Support Unit (now the High Tech, Computer Forensics Section) was established to assist other police forces in the investigation of crimes involving computers.

Part of the expertise within the section was based on the early development of a number of low-level DOS hard-drive forensic utilities, which are still used internationally. These tools allowed, for the first time, a direct examination of the physical sectors of a hard-drive. This was especially important for virus analysis work as it provided the ability to read the system's boot sectors. Coincidentally, these tools were developed around the same time as the Michelangelo virus first appeared.

Viruses have quickly been recognized as a very practical threat to computer systems and these two police departmental sections serve to compliment each other in the analysis of suspect (virus) code. Thus, the reputation of SEIT grew as its ability to detect and clean viruses became well-known in Canadian circles.

SEIT Inspections

Over the years, one of the main thrusts of SEIT has been to collect virus incident reports and analyse the numbers – in effect creating a Canadian WildList. These numbers were then used in security awareness presentations and 'Threat and Risk Assessment' projects across the country. Subsequently, along came Mr McAfee and Dr Solomon, providing software for the accurate and automatic detection and removal of viruses.

AV software has now developed to the point where it has become the first tool of defence in Canadian government departments. It is also the first line analysis tool for the Virus Incident Response Team, a sub-component of SEIT.

When I finally sat down to check on Melissa, I tapped into an informal network that has been developing over the last ten years with contacts in various venues around the world, primarily with law enforcement, university and private sector individuals. When there is no actual code to examine, these external sources provide the first links to finding credible information about a new threat.

Lately, the references of choice have been the extremely useful Web sites put out by leading anti-virus companies, notably *Data Fellows*, *NAI*, *Symantec* and Canada's own

Sensible Security Solutions. This initial line of information provides me with a virtual perspective on how widespread (internationally) and malicious the particular virus is.

In fact, the level of detail provided is broad enough to form an opinion on the likelihood of this threat reaching Canadian systems, and a means of detecting its presence. This information is still needed, despite the best efforts of departments to keep their defence tools updated.

Canadian federal government departments depend on the *RCMP* to provide them with factual, timely and non-commercial information about a particular virus. In order to do this, and to substantiate what others are saying, the practice of the *RCMP* has then been to monitor information sources until a report has been received from a Canadian department that it has actually been hit.

The next step is to get them to send the suspect code to TSB for forensic analysis, and then when this and subsequent reports are confirmed, the *RCMP* issue a general virus alert to the client departments. Uniquely, these alerts must be produced in both English and French format to serve Canada's bilingual public sector personnel.

In the case of Melissa, despite third-hand reports of private sector companies being hit around Ottawa and Toronto, no federal departments reported a problem. This was partially attributable to two factors: incompatible software and a high-level of security awareness in departments.

After years of *RCMP* training courses, the departments knew where to go for information. They also knew how to get their anti-virus systems updated with the required patches – provided quickly by the vendor community – which would detect and block the virus. It was noted with some satisfaction that the *Data Fellows* Web site 'Melissa Information Centre' did not report any Canadian incidents.

Mounties and the Media

Another responsibility to deal with is media relations. In the middle of collecting and disseminating all the facts about Melissa, the phone calls started to come in from various media outlets requesting an interview. On that day, I handled enquires from two newspapers, one national magazine, one national television station and conducted a live radio talk-show interview. In reality though it seems that the media was just looking for a soundbite that would add to the hype and hysteria surrounding this virus. Based on the evidence seen and reported on, they did not get what they were looking for.

It should be noted that in order to get first-hand information, the Web sites provided by the various anti-virus vendors are extremely important. This includes both the virus encyclopaedias and the hoax reference sites. While there is a tendency for vendors to hype the situation, and fan the media flames, there is a justifiable need to get the information out as rapidly as possible.

The *RCMP* depends on the various vendors to substantiate the claims of others. In this vein, we urge and commend the voluntary principle of exchanging information and virus code for analysis as quickly as possible.

One phenomenon noted with an incident like Melissa was that the amount of traffic to the useful and normally reliable sites made it difficult to get to the information and downloads we needed quickly. When this happens, we are very appreciative of details located at local sources such as those found at http://www.canada-av.com.

There are also a number of public domain programs or databases which have served useful purposes for the *RCMP* over the past few years. These include Joe Wells' WildList, Project VGrep, Magic Bullet and any DOS-based tool written to handle a particular virus (eg. Kill_CIH and Killmonk). Project VGrep in particular provides a means of fielding enquires from people all across the country using different anti-virus products.

Crimes and Misdemeanours

One of the usual questions asked during the heat of an incident is whether the *RCMP* will attempt to track down the virus writer(s). This is not within the mandate of TSB and, unfortunately, viruses do not leave fingerprints. Then there is the matter of jurisdiction. From a Canadian Criminal Code perspective, it is not illegal to write virus code.

It becomes a crime under section 430.1.1, where deliberate (intent to cause) damage to a computer can be proven, under a mischief-to-data clause. Violators can be found guilty of an indictable offence and face up to ten years in prison, or they can be found guilty of an offence punishable on summary conviction (fined). There is a cross-reference under this section to section 342.1, where computer hackers are typically prosecuted.

Unlike other crimes the *RCMP* investigate, viruses are not yet seen as high priority and virus writers do not usually confess. The courts, however, are starting to recognize the need to prosecute these offences, and I was accepted as an Expert Witness on Computer Viruses in a provincial court trial in 1998. As the awareness of viruses and their harmful potential increases, the penalties will get stiffer.

From the TSB's perspective the mandate, in terms of viruses, is to get reliable threat information into the hands of security practitioners as quickly as possible. The most efficient way of preventing damage is to know where to get the most up-to-date information and to prepare a proper defence in a proactive way .

The *RCMP* will continue to be involved with the fight against viruses. Success will depend on the continual development of internal expertise and international companies or individuals providing real-time and accurate information in order to assist with law enforcement efforts, as on the fateful day that Melissa struck in Canada.

COMPARATIVE REVIEW

WOW! Wide Open Windows

Six months on from the last *Windows 98* Comparative, the time has come again to take a look at the products for the pre-*Windows 2000* operating system.

Sixteen products were submitted for review, the only notable absentees being *Trend Micro* (who have not submitted since March), and *Panda Software* (who intend to start submitting at the start of next year).

Test-sets and Procedures

Three essentially identical machines were used for testing, the details of which can be found at the end of this review. As usual for *VB* Comparatives, the timed tests were all performed on a single machine, isolated from the network. The only change made to the familiar *VB* tests was the introduction of *PowerPoint* files into the clean OLE2 set and the file set used in the overhead tests.

All products were presented with the customary *VB* test-sets – that is, the Polymorphic, Standard, Macro and In the Wild (ItW) sets. The ItW set, with its boot and file virus components, was aligned to the August 1999 WildList, which was announced a couple of weeks prior to the product submission deadline (31 August).

The overall WildList is reduced somewhat from that used in the previous Comparative. Concurrent with the decrease in the prevalence of boot sector viruses, only 33 made up the boot sector test, compared to the 84 that were present this time last year. Other departures include the file viruses Green Caterpillar, Quicky.1376, Raadioga, Spanska.1500 and Tai-Pan.666. On the macro virus front, farewells are due to WM/NiceDay.A, WM/Wazzu.F and XM/Laroux.FC to name but a few. The only new appearances in the ItW set were macro viruses, and included W97M/Chack.H, W97M/Melissa.I, X97M/Laroux.CF and W97M/Ethan.B.

No changes to the Polymorphic test-set were made this time, but the Standard and Macro test-sets were updated with a selection of viruses. Of particular interest is the addition of Visual Basic Script (VBS) viruses for the first time in *VB* tests. On this front, VBS/Freelinks, VBS/Happy and three variants of VBS/First were included. A few sightings of VBS/Freelinks (see p.6 for analysis) in the wild were noted at the start of July.

The standard method of assessing the overhead of each of the on-access scanners was used once more. The time taken to copy a set of 200 files between directories on a local hard disk was measured with the scanners in each of its various configurations. The file set consisted of 200 files totalling 25.9MB, containing a mixture of executables, *Word*, *Excel* and *PowerPoint* documents. The scanning speed of each of the on-demand scanners was measured for scanning both executables and OLE2 (*Word*, *Excel* and *PowerPoint*) files. These timed scans also serve as false positive tests, since both of the file sets are clean.

The detection rate percentages printed in each of the product summaries are those for on-demand scanning, unless otherwise indicated – 'o/a' being on-access.

Aladdin eSafe Protect v2.1 (1/9/99)

ITW Overall	98.0%	Macro	96.1%
ITW Overall (o/a)	98.0%	Standard	97.4%
ITW File	97.9%	Polymorphic	92.9%

Aladdin Knowledge Systems' eSafe Protect is a product packed with a whole host of features – anti-virus protection being just one. Inserting the CD produces the standard installation front screen, where aside from proceeding with the installation, options to view the user manual, a demo and a white paper are presented. Unfortunately, for those using a screen resolution less than 800x600 pixels, scrolling of this screen is not possible, preventing access to any of the options!

Though not achieving the highest detection rates, particularly in the Macro and Polymorphic sets, no problems were encountered during the testing of *eSafe Protect* – something that cannot be boasted by a few of the other products in this review. Pleasingly, the on-access scanner of *eSafe Protect* proved perfectly stable throughout both the detection and overhead tests. The only slight niggle is the lack of a 'keypress option' during scanning of floppy boot sectors.

The detection rates in the Macro and Polymorphic test-sets are perhaps the weakest areas of this product. *eSafe Protect's* detection of infected document templates has been noted as a weakness in previous reviews, and it still seems to be an area of concern now. Eight DOT files (infected with Carr.A, Class.F, Groov.D, Metamorph.A, Nottice.A and Walker.B), remained undetected, despite the corresponding DOC files being successfully detected.

Alwil Avast32 v3 (26/8/99)

ITW Overall	100.0%	Macro	95.2%
ITW Overall (o/a)	99.8%	Standard	96.9%
ITW File	100.0%	Polymorphic	99.9%

As with all previous *VB* Comparatives, the on-demand scanning rates in this review have been determined from the products' scanning logs. Unfortunately for *Avast32*,

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Missed	%	Missed	%	%	Missed	%	Missed	%	Missed	%
Aladdin eSafe Protect	0	100.0%	11	97.9%	98.0%	143	96.1%	425	92.9%	31	97.4%
Alwil Avast32	0	100.0%	0	100.0%	100.0%	162	95.2%	9	99.9%	34	96.9%
CA InoculateIT	0	100.0%	0	100.0%	100.0%	0	100.0%	5	99.9%	0	100.0%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	28	99.2%	264	93.9%	1	99.9%
Command AntiVirus	0	100.0%	0	100.0%	100.0%	14	99.6%	112	98.0%	3	99.7%
Data Fellows FSAV	0	100.0%	1	99.9%	99.9%	3	99.9%	0	100.0%	8	98.9%
Dialogue Science DrWeb32	0	100.0%	0	100.0%	100.0%	17	99.4%	0	100.0%	4	99.5%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	3	99.7%
FRISK F-Prot	0	100.0%	0	100.0%	100.0%	25	99.6%	18	99.6%	3	99.7%
GeCAD RAV	0	100.0%	0	100.0%	100.0%	0	100.0%	3	99.9%	4	99.5%
Grisoft AVG	0	100.0%	8	98.1%	98.2%	87	97.3%	96	96.8%	43	97.3%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	4	99.6%
NAI VirusScan	0	100.0%	1	99.9%	99.9%	7	99.8%	0	100.0%	12	98.4%
Norman Virus Control	0	100.0%	0	100.0%	100.0%	12	99.6%	174	96.9%	1	99.8%
Sophos Anti-Virus	0	100.0%	0	100.0%	100.0%	15	99.4%	174	96.9%	20	98.4%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	18	99.3%	264	93.9%	1	99.7%

when set to scan the entire test-set, the latter half of the scanning log was observed to have been corrupted. To circumvent this problem, the test-set had to be scanned in chunks, producing smaller, but uncorrupted log files.

At first sight the detection rates against the ItW set look impressive – the only hurdle between *Avast32* and the VB 100% award being samples of CIH.1003 and CIH.101x, that were missed by the on-access scanner. Similar discrepancies between the on-demand and on-access scanner detection rates were also seen elsewhere in the test-sets.

Scanning of the infected floppy boot sectors proved fairly laborious, thanks partly to the lack of a multiple diskette prompt. However, all the boot viruses were detected, for both on-demand and on-access scanning.

Testing of the on-access scanner proved problematic. Due to the lack of a 'deny access' option, the scanner was set to scan on file writes and delete infected files, whilst the test-set was copied to a local hard drive. The copied files were then copied to a new location on the local hard drive, and this process repeated until no further detections were noted. Unfortunately, the sheer number of files in the test-set caused problems for the scanner, and so it had to be copied across in more 'bite-size' chunks. Even so, the number of files in the Polymorphic set still caused problems for the scanner, and so no results are presented here for this set.

Speed-wise, *Avast32* is at the slower end of the pack, particularly when it comes to scanning OLE2 files, but the overhead of the on-access scanner is in keeping with the bulk of products. One false positive was reported in the Clean set – an EXE file infected with Tequila.2468.

CA InoculateIT v4.53 (28/6/99)

ITW Overall	100.0%	Macro	100.0%
ITW Overall (o/a)	98.8%	Standard	100.0%
ITW File	100.0%	Polymorphic	99.9%

Computer Associates' InoculateIT has picked up the VB 100% award in the last three rounds of comparative product testing. A quick glance at the the percentages obtained here for on-demand scanning reveal another impressive performance in terms of detection. Out of the file viruses, only five samples of ACG.A were missed across all the test-sets. The on-demand scanner defaults to scan all files, but curiously the on-access component scans by file extension only. The default list was sadly a few months behind schedule, and so a multitude of *PowerPoint*, *Access* and infected screen-saver (SCR) files slipped through the net during the on-access tests. Additionally, failure of the on-access scanner to detect a Michelangelo-infected floppy disk pushed the VB 100% award further from the grasp of *InoculateIT* this time around.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Missed	%	Missed	%	%	Missed	%	Missed	%	Missed	%
Aladdin eSafe Protect	0	100.0%	11	97.9%	98.0%	143	96.1%	425	92.9%	31	97.4%
Alwil Avast32	0	100.0%	2	99.7%	99.8%	154	95.5%	n/t	n/t	16	98.8%
CA InoculateIT	1	96.9%	16	99.0%	98.8%	33	99.0%	251	98.9%	8	98.9%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	28	99.2%	264	93.9%	1	99.9%
Command AntiVirus	0	100.0%	0	100.0%	100.0%	14	99.6%	112	98.0%	3	99.7%
Data Fellows FSAV	0	100.0%	1	99.9%	99.9%	3	99.9%	0	100.0%	8	98.9%
Dialogue Science DrWeb32	0	100.0%	0	100.0%	100.0%	17	99.4%	0	100.0%	4	99.5%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	3	99.7%
FRISK F-Prot	1	96.9%	1	99.9%	99.7%	78	98.7%	n/t	n/t	3	99.7%
GeCAD RAV	0	100.0%	0	100.0%	100.0%	45	98.5%	33	99.0%	25	98.1%
Grisoft AVG	1	96.9%	9	98.0%	98.0%	93	97.2%	268	93.9%	116	91.5%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	5	99.8%	0	100.0%	3	99.7%
NAI VirusScan	0	100.0%	1	99.9%	99.9%	7	99.8%	0	100.0%	14	98.2%
Norman Virus Control	0	100.0%	0	100.0%	100.0%	12	99.6%	174	96.9%	1	99.8%
Sophos Anti-Virus	0	100.0%	3	99.7%	99.7%	32	98.9%	174	96.9%	20	98.4%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	18	99.3%	264	93.9%	1	99.7%

A couple of minor problems which have been mentioned in previous reviews unfortunately still remain, including false warnings about viruses in memory following a reboot. Also, the product managed to detect a previous installation of itself despite the fact that is was being installed onto a freshly imaged machine.

CA Vet Anti-Virus v10.1.0 (31/8/99)

ITW Overall	100.0%	Macro	99.2%
ITW Overall (o/a)	100.0%	Standard	99.9%
ITW File	100.0%	Polymorphic	93.9%

Despite the ownership change, *Vet Anti-Virus* still remains a pleasant and easy product to test. Identical detection rates were observed for both on-demand and on-access scanning, and detection of the ItW file and boot sets was complete, earning *Vet* its second VB 100% award this year.

One sample of Win32/Parvo in the Standard set, and a handful of X97M/Laroux variants in the Macro set account for the bulk of the misses. Additionally, there seem to be problems in detecting samples infected with the polymorphic X97M/Soldier.A and XM/Soldier.A. Failure to detect samples infected with the A and B variants of ACG account for the misses in the Polymorphic set.

Historically one of the fastest scanners, recent results suggest that it no longer occupies the prime perch in this sense – scanning rates seem to be slightly slower than those previously observed.

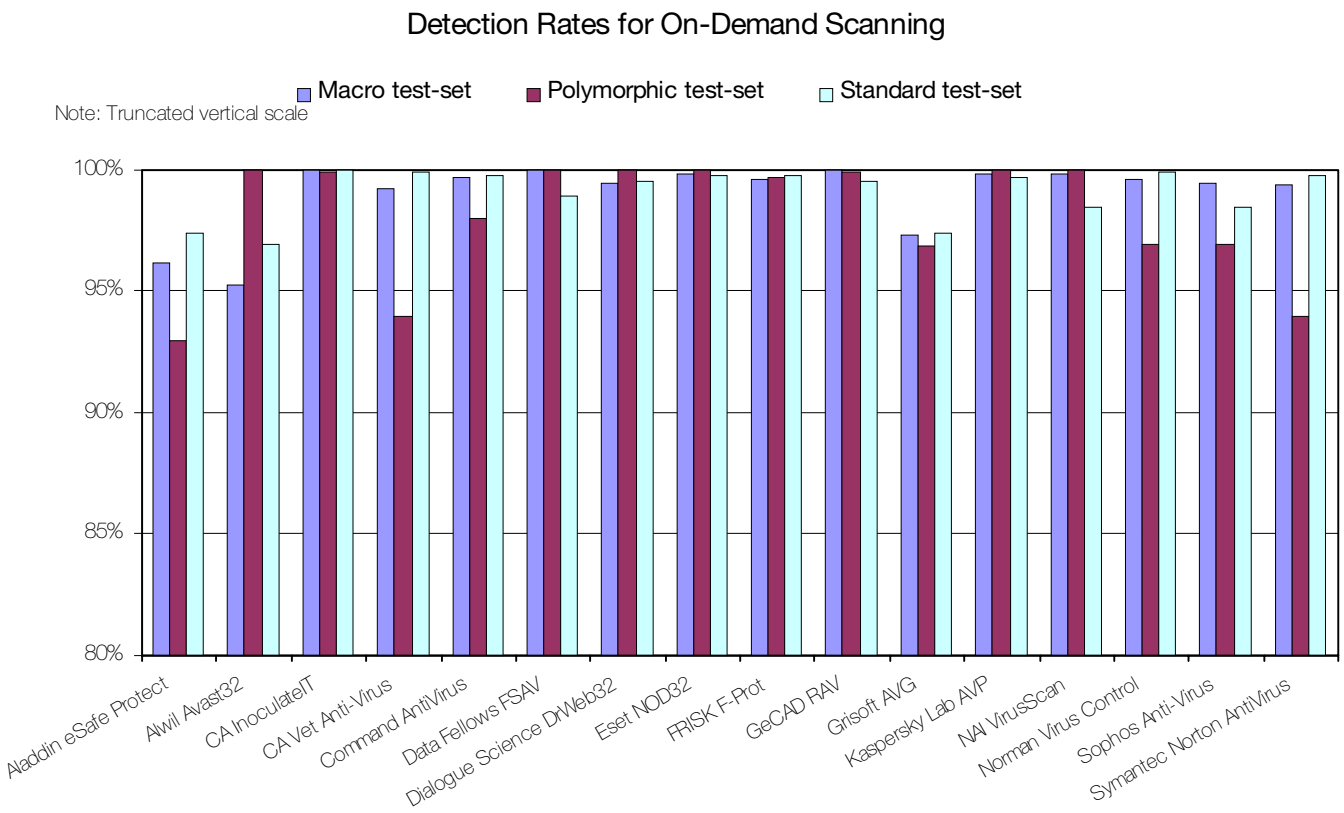
Command AntiVirus v4.57 (30/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	98.0%

The second recipient of the VB 100% award this month is *Command Software AntiVirus* (*CSAV*). Impressive detection rates were observed across all the test-sets.

Both the on-demand and on-access scanners are configured by default to scan files of certain extensions only. However, unlike other similarly configured products, the extension lists have clearly been kept up to date. Interestingly, two of the three VBS/Freelinks samples were missed, as was the JavaScript (JS) file infected with VBS/First.C.

One gripe with *CSAV's* on-access scanner is that it did not appear possible to turn off the on-screen messaging, which caused the test machine to become unstable when scanning the entire test-set.



Data Fellows FSAV v4.05 (25/8/99)

ITW Overall	99.9%	Macro	99.9%
ITW Overall (o/a)	99.9%	Standard	98.9%
ITW File	99.9%	Polymorphic	100.0%

Thanks to its use of two virus engines (*F-Prot* and *AVP*), the double-barrelled anti-virus protection provided by *Data Fellows F-Secure Anti-Virus* (*FSAV*) gives the expected high detection rates across all the test sets. As ever, the downside of the increased armoury is the scanning speed, which was observed to be at the slower end of the range observed across all the products.

Since its last appearance in a *VB* Comparative, detection of infected *PowerPoint* files is now firmly in place in *FSAV*. In fact, only a handful of samples were missed across all the test-sets, for both on-demand and on-access scanning. Unfortunately, the failure to scan extensionless samples prevented *FSAV* achieving the VB 100% award, since the BOOK1 samples infected with the A, B, C and D variants of Tristate were missed.

VBS/Freelinks, VBS/Happy and VBS/First samples were missed during both on-demand and on-access scanning. The samples were detected when the necessary file extensions were included in the default 'to scan' list, or the product reconfigured to scan all files.

Three clean files were flagged as suspicious (by one or both of the engines) during scanning of the Clean set. The overhead of *GateKeeper*, the on-access scanner, was just below the average of that observed from all the products.

Dialogue Science DrWeb32 v4.12a (30/8/99)

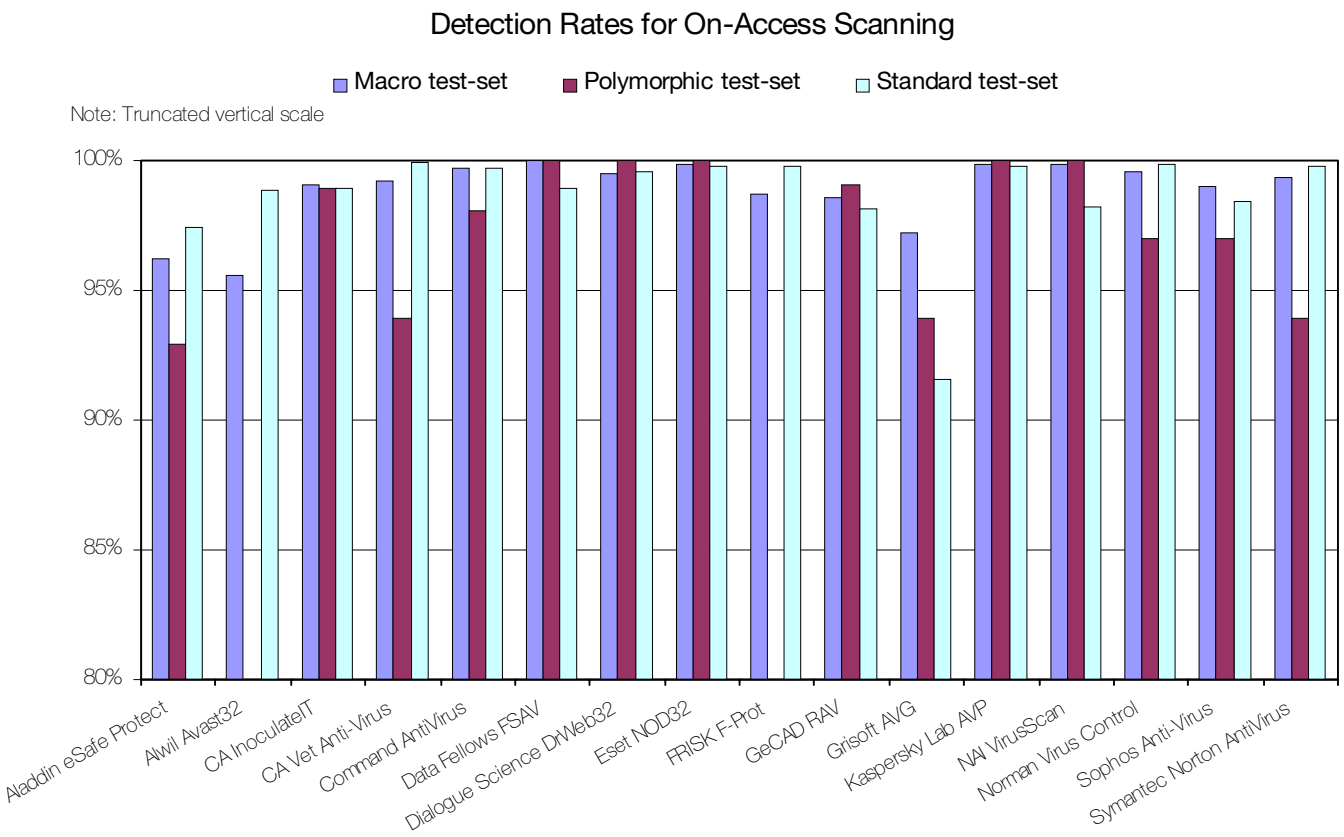
ITW Overall	100.0%	Macro	99.4%
ITW Overall (o/a)	100.0%	Standard	99.5%
ITW File	100.0%	Polymorphic	100.0%

Impressively high detection rates across the board ensure that *DrWeb32* maintains its VB 100% record on the *Win 98* platform, and picks up its second VB 100% award this year.

The high detection rates are due partly at least to the use of heuristics. Traditionally, this can have the downside of causing false positives to be registered, a fact that was in evidence during the speed tests, where one and 17 files were flagged as infected and suspicious, respectively.

SpIDer Guard, the on-access component, is a relatively new addition to the *DrWeb32* product, and made its first appearance in *VB* tests in May 1999. Detection-wise, its performance is excellent, the detection rates mirroring those of the on-demand scanner. Unfortunately however, it is let down by its stability. Problems were encountered during the on-access boot sector tests. Attempting to access diskettes infected with either Boot-437 or Cruel caused the machine to hang, irrespective of the configuration settings of *SpIDer Guard*. However, since both viruses were detected and identified successfully, the 100% scoreline remains.

SpIDer Guard is definitely the weakest component of the *Dialogue Science* anti-virus package. Aside from its slight stability problems, the overhead of *SpIDer Guard* was amongst the largest observed for all the products.



Eset NOD32 v1.24 (30/8/99)

ITW Overall	100.0%	Macro	99.8%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	100.0%

The fourth recipient of a VB 100% award this month, *Eset's NOD32* puts in the usual strong performance that has come to become expected from this Slovak offering.

The high detection rates in the non-ItW sets owes some thanks at least to the use of heuristics in as well as to virus signatures. Only seven samples were missed over all the test-sets. *NOD32* also exhibited extremely impressive scanning speed, blitzing some of the other products with its scan rates well in excess of 2500kB/sec.

FRISK F-Prot for Windows v5.05c (30/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	99.7%	Standard	99.7%
ITW File	100.0%	Polymorphic	99.6%

In its first appearance in *VB* tests back in May, *F-Prot* for *Windows* (*FP-WIN*) returned impressive detection rates, and earned itself the VB 100% award. Unfortunately, this time around the award is lost due to the failure of the on-access scanner to detect the extensionless BOOK1 samples infected with O97M/Tristate.C, and the boot sector infected with Michelangelo.

When enabled, the 'deny access' option of the on-access scanner appeared to hang the test machine whenever access to an infected file was requested. Thus, the on-access detection rates have been determined from the scanning log created whilst attempting to copy the test-set to the local HD. Even this method proved problematic since *FP-WIN* consistently hung the test machine during copying of the Polymorphic set. As such, on-access detection rates against this set are not reported here.

The lower detection rates of the on-access scanner (*F-Stop*) are due mainly to the fact that heurisitics are not enabled by default, as they are for the on-demand scanner. Thus, the detection rates (particularly against the Macro set) are noticeably lower.

Further problems with the on-access scanner were encountered during the overhead tests. When configured to scan purely outgoing files, fatal exceptions were consistently observed. The same problem was not evident in any other configurations, even when set to scan both incoming and outgoing files. Four false positives and 12 suspicious files were registered during scanning of the Clean set. The scanning rates and on-access scanner overhead were in line with the average seen across the product range.

GeCAD RAV v7.0 (30/8/99)

ITW Overall	100.0%	Macro	100.0%
ITW Overall (o/a)	100.0%	Standard	99.5%
ITW File	100.0%	Polymorphic	99.9%

A regular participant in *VB* tests, and featured in a standalone review last month (see *VB*, October 1999, p.20), *Romanian Anti-Virus* (*RAV*) from *GeCAD Software* doubles its collection of VB 100% awards this month.

Unfortunately, as described for previous products, the test experience was not a particularly pleasant one – once again the problems centred around the on-access scanner, in this case, *RAV Monitor*. During initial tests (using a utility that attempts to open all of the files it comes across), access to almost half of the test-set samples was 'allowed'. The test was repeated by copying the test-set to the local HD with *RAV Monitor* configured to 'block' infected files. Fewer files were missed this time, although still far more than expected from the results of the on-demand scanning tests. Furthermore, the test-machine repeatedly hung during copying of an *Excel* file infected with O97M/Teocatl.A. The missed files were copied between locations on the local HD until no further detections were made – the final on-access results mirror those of the on-demand scanner.

Both the scanning speed and on-access scanner overhead were observed to be in line with those for the bulk of the products tested. Unfortunately, one file in the Clean set was flagged as suspicious.

Grisoft AVG 6.0.77 (31/8/99)

ITW Overall	98.2%	Macro	97.3%
ITW Overall (o/a)	98.0%	Standard	97.3%
ITW File	98.1%	Polymorphic	96.8%

Upon insertion of the *Grisoft AVG* CD, an HTML page is displayed from which the various installation options are presented. The updates submitted to this review were only compatible with the US product version, and so that was the version tested.

The *AVG* user interface is somewhat different to the bulk of anti-virus products, but once accustomed to it, the product is extremely simple to use.

Over recent Comparatives, the on-demand detection rates have been climbing, and once again a respectable performance is displayed. Unfortunately, *Word* files infected with W97M/Marker.O were missed in the ItW set, which coupled with the failure to detect Michelangelo infected boot sectors during on-access scanning, pulled the VB 100% from *AVG's* grasp.

Slightly poorer detection rates were observed during on-access scanning, but on the positive side it was noticed that no stability problems were experienced throughout testing.

The integrity checking facility, which is enabled by default, was disabled for the duration of the speed tests, where, unfortunately, seven false positives were registered, and two files flagged as suspicious.

Kaspersky Lab AVP v3.0.131 (28/8/99)

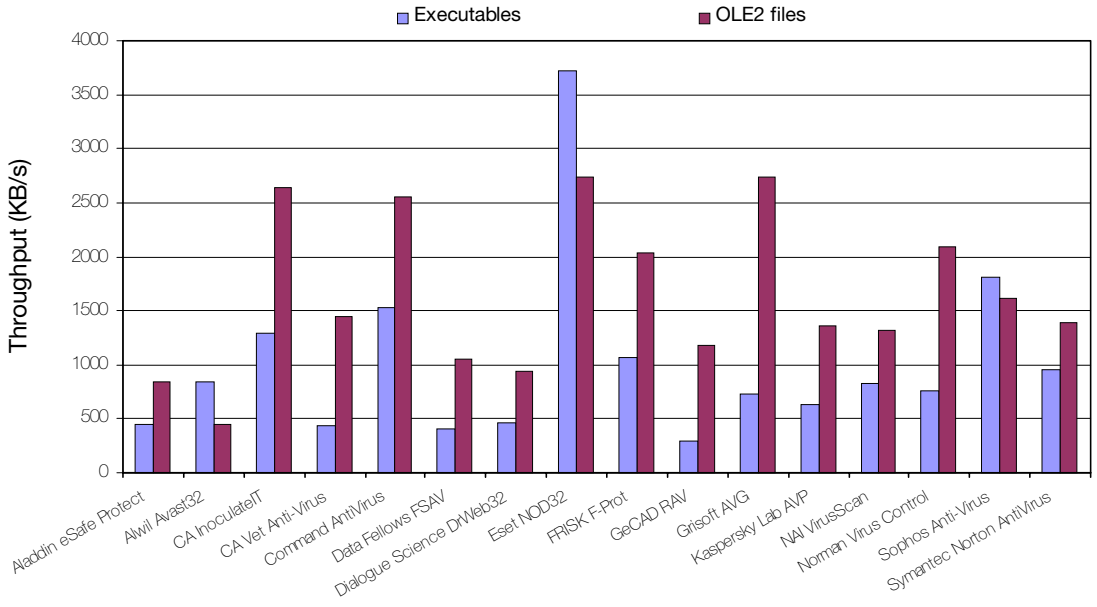
ITW Overall	100.0%	Macro	99.8%
ITW Overall (o/a)	100.0%	Standard	99.6%
ITW File	100.0%	Polymorphic	100.0%

Last time around it was a clean sweep for *Kaspersky Lab's AVP* – 100% detection of all the samples in the test-sets for on-demand scanning. The feat was not to be repeated this time, although results were sufficient for *AVP* to claim its tenth VB 100% award.

During both on-demand and on-access tests, all three of the VBS/Freelinks samples were missed, along with *Word* documents infected with W97M/Chack.AR. Also, the on-access scanner missed one of the XM/Laroux.F samples.

Problems were encountered during the speed and overhead tests, due to one of the executables in the Clean set – STAT.EXE. As soon as this file was copied between the HD locations during the overhead tests, with *AVP Monitor* enabled, the test machine slowed almost to a halt, some-

Hard Disk Scan Rates



	Hard Disk Scanning Speed					
	Executables			OLE2 files		
	Time (min:sec)	Throughput (kB/s)	FPs [susp]	Time (min:sec)	Throughput (kB/s)	FPs [susp]
Aladdin eSafe Protect	20:00	455.8	0	1:34	844.0	0
Alwil Avast32	10:52	838.9	1	2:59	443.2	0
CA InoculateIT	7:04	1289.9	0	0:30	2644.5	0
CA Vet Anti-Virus	21:05	432.4	0	0:55	1442.4	0
Command AntiVirus	5:59	1523.5	[12]	0:31	2559.2	0
Data Fellows FSAV	22:21	407.9	[3]	1:15	1057.8	0
Dialogue Science DrWeb32	19:35	465.5	1 + [17]	1:24	944.4	[1]
Eset NOD32	2:27	3720.6	0	0:29	2735.6	0
FRISK F-Prot	8:30	1072.4	4 + [12]	0:39	2034.2	0
GeCAD RAV	31:38	288.2	[1]	1:07	1184.1	0
Grisoft AVG	12:33	726.3	7 + [2]	0:29	2735.6	0
Kaspersky Lab AVP	14:29	629.4	0 +[2]	0:58	1367.8	0
NAI VirusScan	11:00	828.9	0	1:00	1322.2	0
Norman Virus Control	12:00	759.6	0	0:38	2087.7	0
Sophos Anti-Virus	5:00	1811.0	0	0:49	1619.1	0
Symantec Norton AntiVirus	9:36	949.5	0	0:57	1391.8	0

times hanging up completely. In order to measure meaningful overhead times, STAT.EXE was temporarily replaced by a similarly sized executable, and the tests repeated. The overhead of *AVP Monitor* was finally measured to be approximately 160% – in keeping with that for other products featured in this review.

NAI VirusScan v4.0.3.4040 (25/8/99)

ITW Overall	99.9%	Macro	99.8%
ITW Overall (o/a)	99.9%	Standard	98.4%
ITW File	99.9%	Polymorphic	100.0%

Returning very similar detection rates to those observed during testing of its *Windows NT* incarnation, *VirusScan* missed only a few samples across all the test-sets. Sadly, at least in terms of the VB 100% award, these included the extensionless BOOK1 samples infected with the four variants of O97M/Tristate.

On-access protection is provided with the *McAfee VShield*, which offers system scanning and email scanning (the latter was disabled throughout these tests). Other than two samples infected with Cruncher, the results of the on-demand and on-access scanners were identical.

VirusScan failed to detect samples infected with HLLP/Toadie variants – in this respect the product was certainly not alone. Samples of the relatively high profile (thanks to its potentially destructive payload) macro virus W97M/Thus were also missed.

Speed-wise, *VirusScan* is the same as ever, in the middle of the pack. The overhead of *VShield* is perhaps slightly larger than that of some of the other products, but not significantly so. Pleasingly, no false positives were registered against the Clean set. The only real gripe with the product concerned its sporadic (at best) detection of floppy disk changes. This problem has been noted before, but still persists.

Norman Virus Control v4.72 (31/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	100.0%	Standard	99.8%
ITW File	100.0%	Polymorphic	96.9%

Another impressive display from *Norman Virus Control* (*NVC*) earns the product its tenth VB 100% award. The majority of the misses can be accounted for by the samples of ACG.A from the Polymorphic set. Elsewhere, misses were few and far between – a handful of *Word* macro viruses (Ozwer.A,

Chack.AR and IIS.H) and a JavaScript file infected with VBS/First.C. It was pleasing to see similarly impressive results during the on-access tests, thanks to *NVC's* on-access scanner, *Cat's Claw*.

Sophos Anti-Virus v3.25 (31/8/99)

ITW Overall	100.0%	Macro	99.4%
ITW Overall (o/a)	99.7%	Standard	98.4%
ITW File	100.0%	Polymorphic	96.9%

A typically strong performance from *Sophos Anti-Virus* (*SAV*), although unfortunately not sufficient to claim the VB 100% award. *PowerPoint* files infected with O97M/Tristate.C were missed from the ItW set due to the failure of *InterCheck* (*SAV's* on-access component) to include *PowerPoint* files by default. To include such files (and any others deemed necessary), *InterCheck's* configuration file has to be edited manually.

As ever, *SAV* was one of the easy products to test, with perfect stability exhibited by both its on-demand and on-access components. The latter gives an overhead of approximately 100% when enabled, which is slightly less than that induced by some of the other products.

Symantec NAV v5.02.04 (27/8/99)

ITW Overall	100.0%	Macro	99.3%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	93.9%

As can be seen from the results, impressive detection rates were observed with *Symantec's Norton Anti-Virus* (*NAV*), and the product picks up its seventh VB 100% award.

The final product in this Comparative, *NAV*, behaved impeccably, just like *SAV* before it. It was perfectly stable throughout testing. In keeping with some of the other products featured in this review, *NAV* uses heuristics by default. Thankfully, the *Bloodhound* heuristics employed by *NAV* did not register any false positives during the speed and overhead tests.

The misses were due to ACG.A and ACG.B samples in the Polymorphic set, VBS/Happy in the Standard, and a handful of *Word 8* macro viruses together with PP97M/Vic.A in the Macro set.

Summary

In this, the first Comparative where on-access scanning is incorporated into the VB 100% award, eight products managed to make the grade. A number of others came close, but missed due to the simple product configuration issue of failure to scan sufficient file types.

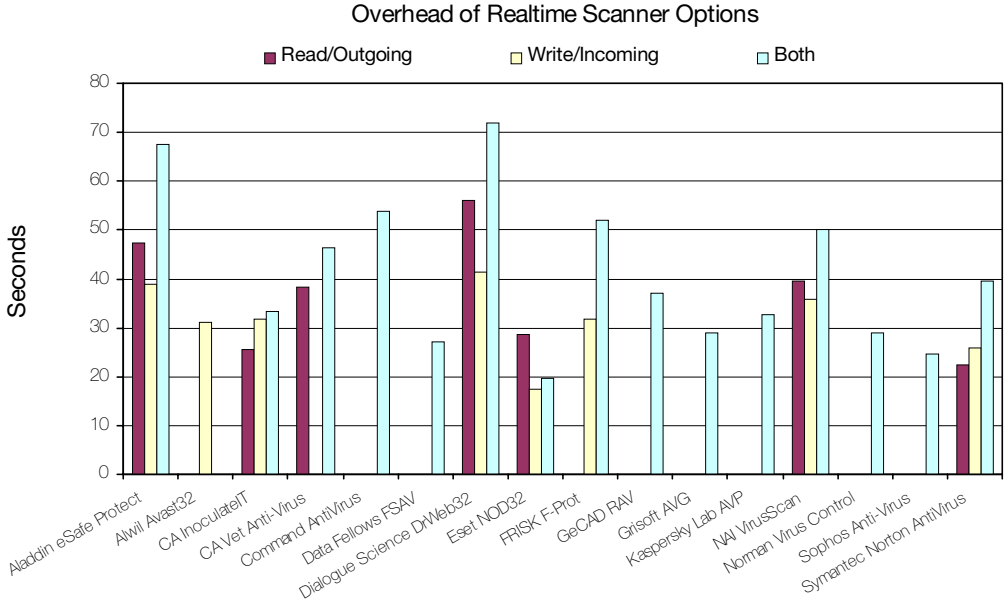
Another Comparative first is the fact that all the submitted products sported an on-access scanner of some description – perhaps reflective of how dependent users are on them nowadays. The stability of the on-access scanners is perhaps an area of concern, however. Certainly, exposing the scanners to almost 20,000 infected files might not be a realistic situation, but even so, the lack of stability exhibited by a few of the products does not inspire confidence.

The final first in this Comparative is the inclusion of VBS viruses in the test-set. This was partly driven by the recent reports of VBS/Freelinks in the wild. Despite the fact that this virus made its first appearance at the start of July, only five of the 16 products tested managed to detect all three of the variants included in the tests. Perhaps the fact that the first of these variants is now officially on the October 1999 WildList will see VBS/Freelinks' detection finally being added to the remaining products – a few of which already have the necessary updates available from their Web sites.

Technical Details

Test Environment: Server: *Compaq Prolinea 590*, 90 MHz Pentium with 80 MB of RAM, 2 GB hard disk, running *NetWare* 4.10. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, CD-ROM and 3.5-inch floppy, all running *Windows 98*. The workstations were rebuilt from image back-ups, and the test-sets were stored in a read-only directory on the server.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199911/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.



SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery:

UK £195, Europe £225, International £245 (US$395)

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

VB, 50 Sth Audubon Road, Wakefield, MA 01880, USA

Tel (781) 2139066, Fax (781) 2139067

END NOTES AND NEWS

The *Computer Security Institute's* (*CSI*) 26th annual conference and exhibition is to be held from 15–17 November 1999 at the Marriott Wardman Park Hotel in Washington DC. For information on the 85 featured presentations or pre- and post-conference seminars, contact *CSI*: Tel +1 415 9052626 or visit http://www.gocsi.com/.

A two-day course concerning Practical Anti-Virus will be run by *Sophos* on 17 and 18 November 1999 at the organization's training suite in Abingdon, Oxfordshire, UK. For further information, or to reserve your place, please contact Daniel Trotman at *Sophos*; Tel +44 1235 559933, fax +44 1235 559935, visit the company Web site http://www.sophos.com, or email courses@sophos.com.

***Commercial Seminars* (*CS*) is running a course on Computer Crime and Misuse in London on 18 November.** This intensive seminar examines computer-related threats in the business environment and the technical and procedural methods needed to investigate computer misuse. Contact *CS*; Tel +44 1572 757751.

The *Information Society Technologies* conference (IST'99) is to take place in Helsinki, Finland from 22–24 November 1999. There are parallel sessions and workshops, a concurrent exhibition and an Investment Forum aimed primarily at businesses and corporations. On 23 November the 1999 European *IST* Prize Awards will be held. For more details on the conference programme email ist99@cec.be or you can register on-line at http://www.ist99.fi/.

***Computer Fraud and Security's* fifth annual conference takes place from 29 November–1 December 1999 at the Copthorne Tara Hotel, Kensington, London.** Day 1 is devoted to the subject of the Internet with Day 2 dealing with 'Who and Where and Recovery'. Day 3 is an all-day *NT* Security and Audit Workshop. Delegates may register for one, two or all three days of the conference. For further details contact *Audit Conferences Europe Ltd*; Tel +44 1892 526099.

Content Technologies Ltd* announces the release of *MAILsweeper for SMTP v4.1, the first of its products to offer dynamic updates of users lists from LDAP (Lightweight Directory Access Protocol) directory servers. There is also an in-built automatic reporting facility. Prices start at £1095 for 50 users. For more details contact Catherine Jamieson at *Content Technologies Ltd*; Tel +44 118 9301300.

Ensure maximum exposure for your company at the start of the new Millennium. ***Virus Bulletin* is offering a limited number of conference sponsorship packages for VB 2000.** Your company's official corporate logo will appear on all the associated materials and merchandise including the pre-conference brochure which will be mailed to over 50,000 specifically targeted IT professionals. For more details about this opportunity to sponsor the tenth international *Virus Bulletin* conference contact Jo Peck; Tel +44 1235 555139 or email jo@virusbtn.com.

The fifteenth annual *Computer Security Applications* (*ACSAC*) conference will take place at the Radisson Resort, Scottsdale, Phoenix, AZ from 6–10 December 1999. A two and a half day technical conference exploring general computer security technology will be preceded by two days of tutorials, both introductory and advanced. For details, contact *ACSAC*, 2906 Covington Road, Silver Sprint, MD 20910-1206, USA or email General_chair@acsac.org.

***IIR Training* is hosting a practical two-day foundation course called 'How Do Networks Work?' on 13 and 14 December in central London.** An optional workshop will be running on 15 December. For more information about location and prices contact; Tel +44 171 9155055, or email information@iirtraining.co.uk.

Symantec* announces the release of *Norton AntiVirus 2000 which offers protection across all entry points including email attachments and Internet downloads. Its redesigned interface offers users clearer action instructions as well as task-based and fully customised scanning. The product is for use across all *Windows* platforms including *Windows 2000* and is priced at £36 including VAT. Another recent addition to *Symantec's* product range is *Striker32*, virus detection and repair technology engineered to combat the growing threat of 32-bit *Windows*-based viruses. *Striker32* is included in all current *Norton AntiVirus* products. For more details about either product, contact Lucy Bunker; Tel +44 1628 592222.

The ninth annual *EICAR* conference, also known as the first European Anti-Malware Conference, takes place in Brussels, Belgium, from 4–7 March 2000. For more information, to place your booking or to order a timetable of events visit the *EICAR* Web site at http://www.eicar.dk/.