ISSN 0956-9979

MAY 1999

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Smashing results!** Eighteen products jockey for position in this month's *Windows 98* Comparative Review, which starts on p.12.

• **Rhyme and reason?** Sarah Gordon has spent years researching the whys and wherefores of virus writing. The first instalment of her two-part feature attempts to explain the inexplicable on p.8.

• **Round one:** Get stuck in to the new Comment page which this month was sent in by a young Tech Support professional. See what you think on p.2.

• **Who's that girl?** By now, everyone's heard of Melissa. A full analysis cuts through the hype and reveals a rather ordinary Class-style infector, starting on p.5.

CONTENTS

COMMENT

Quis Custodiet Ipsos Custodes?

[*What better way to kick off the new column than this recent distress call from a member of a well-known, international anti-virus company's 'tech support' staff. Though only twenty-four, he's been on the end of a customer advice line for two years. Feel free to respond. Ed.*]

The recent media furore about Melissa should have reinforced the view that anti-virus software is not just a tick box but a necessity. It is not just an application but an integral part of your system's security. The last three viruses to hit the media were the results of poor security.

> *"The last three viruses to hit the media were the results of poor security."*

On Friday 26 March at 2pm (GMT minus 5 hours), an infected document was posted to ALT.SEX. If we believe the rhetoric, by close of business mainland USA was riddled with the virus. What the hell happened? A Usenet group of questionable nature was being accessed during working hours on corporate America's desktops! Am I the only one who thinks that strange? The majority of corporate management does not like staff taking personal telephone calls. Recognizing legitimate email is difficult, but justifying complete Internet access on the desktop for work? Please! For those of you who do have it, how much of your surfing is actually for work purposes? A company or organization with some inkling of security should not have been caught out. However, there is still the possibility that an employee is on an address book of someone whose security is more lax.

One thing that will probably come up in the trial of the person accused of writing/posting Melissa is 'my client was exposing a security hole'. This lame argument has been rolled out by the 'computing underground' since the year dot. It holds no water – there is a difference between exposing and exploiting. Yes, there are huge holes in *Microsoft's* security policies – until *NT* came along, they did not really exist. Even *NT* has faults in this area. Were I a paranoid SysAdmin I would be loath to run it. Why, when I install an application, does it update my OS? Why do *Office* components need a fully functional programming language? As SysAdmin, I should be able to update the OS and then lock it down to stop my users messing. There should be a more formal divide between applications and the OS. I would like to know that the App will do 'exactly what it says on the can'. If I want to do a 'Mail Merge', I would prefer a fully functional scripting language, separate from applications, that can be run by specified staff.

CIH highlighted other procedural flaws. A user can be expected to launch a document but why were they running executables? CIH got its kickstart into the wild by infiltrating the GAMEZ sites. In Britain, it was distributed on magazine cover CDs! Why were users running unauthorized software? Worse still, how did they spread the virus internally? I had many conversations like this:

Support: CIH only runs in Windows 9x.

Customer: No, it doesn't. It's infected my server!

Support: That's because while browsing the network from an infected 9x machine CIH saw the executable files and infected them because the user had write access to those executables.

If you are storing *Word* on the server on administration or security grounds, should users be given write access? Local administrators believe that they have implemented a security policy by giving users login passwords. Naivety and poor security caused the CIH headaches – if developers did internal checksumming of executables it would make virus writing much more difficult.

Remote Explorer is a more worrying case. It runs as a service and therefore someone with rights to install services must have run the virus in order to infect *NT*. Whether it was malice or stupidity, the fact is that, in the majority of situations, you and I are not logged in with the appropriate rights. There are few cases in which we need Admin rights to a system. A chain is only as strong as its weakest link, how many of us are the weakest link? Hence my title from Juvenal's Satires 'Who shall guard the guardians?'. Is your conscience up to the job? A well thought-out security policy with an anti-virus policy at its heart should be the prime goal of the IT profession. If we stand up now to say what we want for the next generation of desktop machines, then perhaps we will get the machines that we need as opposed to equipment which is cool and neat.

NEWS

Who's Afraid of the Big Black Hat?

Unsolicited gifts continue to wing their way to the *Virus Bulletin* offices via email. Consider one such recent offering, preceded in mid-April by an 'official' request. *VB's* webmaster received an email headed 'Virus Supply Request' which, judging by the professional-looking sig, had apparently been sent by an old friend of ours – the Research Manager of a leading anti-virus company.

Alarm bells rang – why would a well-respected professional, who develops one of the most competitive anti-virus engines around, be asking *Virus Bulletin* for over 60 samples (plus source code, naturally) of viruses including old favourites like Cap, Paix, Laroux, assorted worms and construction kits? Not to mention 30 or so 'source only' requests for Win32 and Win95 viruses? Why address it to the webmaster? How 'URGENT' could it be?

Hot on the heels of this rather ham-fisted enquiry came a zip file, amateurishly named the 'Destruction Project' with the less than chatty message – 'Here is a completely new virus. Do some research on it.' Well, that decided it for us at *Virus Bulletin* – no banter? No friendly greeting? Not even some sensible description or analysis? A fake, surely.

Of course, it was. Joking aside, and bearing in mind this month's Comment and the *Content Technologies* survey featured on the back page, make sure that all your staff are on constant alert for the potential dangers of email traffic. On closer inspection, the sig was slightly different from the one we had come to recognize, but only slightly. It transpires that the person responsible had registered a new vanity domain. The police are investigating this particular incident, and we will, of course, keep you posted ▮

Get Yours Here!

Your *VB* conference brochure, that is. Regular subscribers will have received the new VB'99 brochure with this issue. The full-colour six-page folder contains all the details of the upcoming *Virus Bulletin* conference in Vancouver from 30 September – 1 October 1999.

A complete programme of speakers and papers is included, along with details of social events, travel and accommodation information. To receive your VB'99 brochure, contact Jo Peck; Tel +44 1235 555139 or visit the *Virus Bulletin* web site at http://www.virusbtn.com/ ▮

RSVP, If You Please

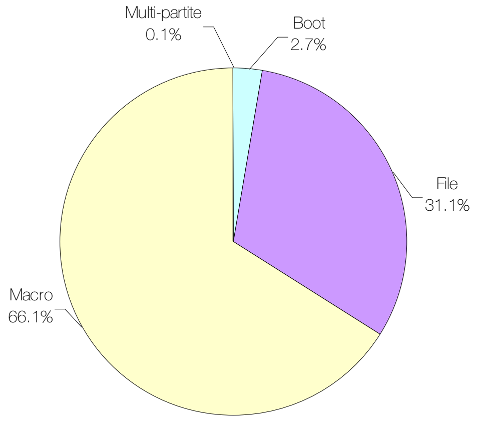
VB intends to reinstate the letters page of the magazine, because of popular demand. Respond to the monthly Comment page or simply air your views on what's happening in the anti-virus world. Email editorial@virusbtn.com ▮

Prevalence Table – March 1999

Virus	Type	Incidents	Reports
Win95/CIH	File	1249	22.9%
ColdApe	Macro	1136	20.8%
Cap	Macro	662	12.1%
Win32/Ska	File	423	7.7%
Class	Macro	369	6.8%
Ethan	Macro	336	6.1%
Npad	Macro	193	3.5%
Appder	Macro	115	2.1%
Concept	Macro	106	1.9%
Munch	Macro	100	1.8%
Laroux	Macro	85	1.6%
Marker	Macro	84	1.5%
Temple	Macro	84	1.5%
CopyCap	Macro	55	1.0%
Form	Boot	32	0.6%
Melissa	Macro	32	0.6%
DZT	Macro	26	0.5%
Parity_Boot	Boot	25	0.5%
AntiEXE	Boot	24	0.4%
Proteced	Macro	24	0.4%
Angelina	Boot	23	0.4%
Suck	Macro	20	0.4%
Wazzu	Macro	20	0.4%
Others [1]		241	4.4%
Total		**5464**	**100%**

[1] The Prevalence Table includes a total of 241 reports across 60 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

Distribution of virus types in reports



VIRUS ANALYSIS 1

In Frome the Cold

Andy Nikishin
Kaspersky Lab

A lengthy procession of macro viruses continues to penetrate computers and dominate users' reports. From the ancient Concept virus, overgrown with hundreds of modifications, through old-timers like Laroux and Cap to the thoroughly modern ColdApe and Class, this type of virus still tops the WildList. In this identity parade a new suspect has recently appeared – W97M/Ethan.

Ethan infects *Word 97* documents and the normal template. It contains one Macro – Document_Close() – in the ThisDocument module and infects the global macro area on closing an infected document.

It must be said, this simple virus is nothing to write home about. There is nothing in its code to grab the attention of experienced virus experts. Basically, this is a pure virus with a pure payload and, fortunately, no destruction routines. Unfortunately, however, this virus has made a name for itself in the wild.

Infection Routine

While infecting, Ethan turns off *Word's* virus protection (the VirusProtection option) and sets an option which allows *Word* to save changes to the Normal template automatically before it quits. It also disables the ability to cancel its macros while running. Then it obtains the 'Saved' property of the active document. This is 'true' if the specified document or template has not changed since it was last saved, but 'false' if *Word* displays a prompt to save changes when the document is closed.

At the start of infection, the virus checks for a file named ETHAN.___ in the root folder on the C: drive. If it is not present, the virus creates it and copies all the code lines from the macro module to that file. If the module contains any other macros Ethan will copy them, too. Then it sets its file attributes to System and Hidden and closes the file. After that, the virus checks for C:\CLASS.SYS (this file contains the source code of W97M/Class viruses) and if it finds it, Ethan deletes this file.

Subsequent to this check, Ethan chooses a victim for infection. It checks the first line in the normal template and if it does not contain the Private Sub Document_Close() string, the virus selects the normal template (usually NORMAL.DOT) as its victim. If NORMAL.DOT is already infected (or contains the above string), the virus goes on to check the active document for a previous infection. Ethan's infection mechanism is the same for templates and documents.

The virus opens the C:\ETHAN.___ file and reads it string by string, inserting them into the victim's macro module. This strange method of reproduction is intended to fool anti-virus scanners' heuristic analysers. Also, Ethan checks for the size of this file and if it is zero does not continue with the infection routine. This feature may be used as a vaccine to protect against W97M/Ethan.

As the virus does not delete any macros from the victim file it is capable of infecting documents together with other viruses (for example, one sample of Ethan infects with W97M/Class.Seed.II). Furthermore, if the procedure names do not contain both viruses, the two are able to continue their spread together (see *VB*, March 1999, p.6).

Finally, Ethan checks the file name of the active document. If it is not equal to Document, it saves the file with its full name to avoid the standard 'Do you want to save the changes you made to…' dialog box, and sets the previously saved document's Saved properties.

Payloads

Ethan has several payloads which trigger during the infection routine. There is also a small chance (dependent on a random counter) that it will change some of the properties of an infected document. For example, the title is changed to 'Ethan Frome', the author to 'EW/LN/CB' and keywords to 'Ethan'. The file ETHAN.___ can also be created in the root directory on the C: drive.

Known Modifications

This virus has recently shot ahead of the pack in the wild and several modifications are already known. One of them (W97M/Ethan.d) has a distinctive payload which warns the user about the year 2000. On 1 December 1999 it will say:

```
“Good Luck (30 days to go) Well, this will be
the final installment in the Y2K preparation
lessons. If you have followed my advice over
the past few months, you will be in excellent
shape to bring in the New Year. May the New
Year bring you health and happiness. Best
wishes.  Bye!”
```

W97M/Ethan

Aliases:	None known.
Type:	Native *Word 97* macro virus.
Payloads:	Creates a C:\ETHAN.___ file, deletes the C:\CLASS.SYS file and changes infected document's properties. Some variants display message boxes.
Detection:	Check for C:\ETHAN.___ file.

VIRUS ANALYSIS 2

Melissa – The Little Virus That Could…

Ian Whalley
Sophos Plc

[*After this analysis* VB *gauges* IVPC's *reaction to Melissa. Sarah Gordon's feature also mentions its author. Ed.*]

Saturday 27 March was going to be a quiet day – or at least, that was what I thought when I got up at around 8.30am. After a quick breakfast, I dialled my ISP to retrieve my email and read some news. Shortly afterwards, I was in the car on the way to the office.

Newsgroups, mailing lists, on-line news services – all were talking about one thing; a macro virus called Melissa that was (apparently) causing havoc in North America. Companies were reported as being effectively forced to stop all internal and external email in an effort to halt its spread. Consequently, after the initial creation of a patch for our product to detect and remove the virus, a more detailed analysis followed.

The Nitty-gritty

In and of itself, Melissa is almost entirely uninteresting – it is a perfectly standard *Word 97* Class-style infector. The first time an infected document is opened on a given machine, the virus receives control via the standard Document_Open() macro.

The first thing it attempts to do is deactivate macro security. It checks for the value Level in the registry key: HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security. If this value is found, Melissa assumes that it is running inside *Word 2000*. Subsequently, it disables the Security… option on the Macro menu (this causes that option to appear greyed out on the menu), and then resets the Level value mentioned above to 1.

If the Level value is not found, Melissa assumes that it is running under *Word 97*. It greys out the Macro option on the Tools menu, disables format conversion warnings, *Word's* own virus protection, and prompts to save the global template. Instead of setting these options to False or 0, it sets them to (1 – 1) in an attempt to fool macro heuristics. Following this initial work, Melissa moves on to trigger the payload – more on this later.

Infection

This is fairly standard – it copies itself from the source document to the destination one using the InsertLines method on a CodeModule object. It takes care to change the first line of the macro appropriately. This is dependent upon whether it is copying itself into the global template from a document, or into a document from the global template. This is necessary because the macro has two different names – in a document, it is called Document_Open() (as mentioned above), and in the global template, it is called Document_Close().

It is worth noting at this point that Melissa has a little-noticed side effect – it will overwrite the first item in the components collection of documents and global templates which it infects. For most documents, this will not be an issue, of course – however, for global templates, it might be more of a problem.

Payloads

Melissa has two payloads. Not surprisingly, the least significant of the two is also the simplest to explain. Whether or not the virus has had to copy its body from one place to another, at the end of its execution it checks the time. If the minutes of the hour are the same as the day of the month (for example, 11.15 on 15 December, or 10.04 on 4 July), it will insert the following text into the active document, wherever the cursor happens to be:

```
Twenty-two points, plus triple-word-score,
plus fifty points for using all my letters.
Game's over. I'm outta here.
```

At this point in the virus, the following text appears in comments:

```
WORD/Melissa written by Kwyjibo
Works in both Word 2000 and Word 97
Worm? Macro Virus? Word 97 Virus? Word 2000
Virus? You Decide!
Word -> Email | Word 97 <—> Word 2000 ...
it's a new age!
```

A quick session with *Altavista* reveals that Kwyjibo and the text that the virus inserts into the current document derive from an episode of *The Simpsons* called 'Bart the Genius'. The family are playing Scrabble, and Bart says: 'K-W-Y-J-I-B-O… Kwyjibo. 22 points… plus 50 points for using all my letters! Game's over, I'm outta here… '. When asked, he defines Kwyjibo as 'a big, dumb, balding, North American ape with no chin…'.

That Other Payload

The reason for Melissa's sudden infamy is contained within the other payload, referred to at the start of this analysis. Immediately after the virus attempts to disable *Word*'s security features, it uses the CreateObject() function to intialize an instance of *Microsoft Outlook*. This will, of course, fail if *Outlook* is not installed (in fact, it only works with *Outlook 98* or later).

This is not a problem. The virus has installed the now-traditional ‘On Error Resume Next’ handler, so that if and when all the following commands fail, it will blunder on regardless, without telling the user that anything is wrong.

Once Melissa has obtained a running instance of *Outlook*, it asks it for a MAPI (Messaging API) namespace. In this context, ‘namespace’ represents ‘an abstract root object for any data source’, which translates into English as ‘something you have to log on to and which you can retrieve information from and do stuff with’. Following this, it checks for the existence of a value ‘Melissa?’ in the registry key: HKEY_CURRENT_USER\Software\Microsoft\Office.

If this value is set to ‘... by Kwyjibo’, then it skips the next set of instructions – after the payload has been executed, the virus will set that value to that string, preventing the payload from being executed more than once. Administrators should note that a system with a write-protected registry would allow the payload to execute each and every time an infected document is opened. In this case, security works against the prepared.

Then Melissa logs on to *Outlook*. I have been unable to find documentation to describe the code it is using, but when the code is run, it logs on to *Outlook* as the default user on that machine. I suspect, in many environments, *Outlook* attempts to connect to the server using the current network username and password, which would obviously work well in *Exchange*-based environments.

Melissa now iterates across all the ‘members’ of the MAPI session’s AddressLists ‘collection’ – MAPI (and *Outlook*) allow the user to have multiple address books in which to store names and email addresses of both individuals and groups of individuals for easy access. Once again, in *Exchange*-based environments, one or more of these address books can be held on the server – these address books are shared between multiple users.

The impact of this type of set-up on Melissa’s spread should not be underestimated. This is because it seems that in such environments, a large number of addresses in server-based address books are for groups of people.

For each list in the collection, Melissa constructs a message to the first fifty entries, with the subject line ‘Important Message From <username>’, where <username> is set to the name used to register the currently-running copy of *Word*. The body text is set to ‘Here is that document you asked for ... don’t show anyone else ;-)’, and (here comes the problem), Melissa attaches the current document (which is, of course, infected) to the message, and sends it.

Melissa’s Initial Spread

Melissa was distributed on Friday 26 March via a posting to the Usenet group ALT.SEX, in an infected document containing what was claimed to be a list of passwords for porn sites (LIST.DOC, contained within LIST.ZIP).

Unsurprisingly, therefore, the first document to be widely emailed by the virus was LIST.DOC itself. This has led to several stories about the virus mentioning LIST.DOC explicitly (no pun intended). However, whilst initially the mail messages generated by the virus did indeed predominantly contain LIST.DOC, as the virus naturally infected other files, other documents (often confidential ones) were transmitted as well.

The initial impact of Melissa was considerable – news stories quoted *Microsoft* officials as saying that they had been forced to shut down their outbound and inbound email servers. During the weekend of 27/28 March, only two of *Microsoft*’s five inbound mail servers were in operation. One large organization reports that between four hundred thousand and half a million email messages were generated by the virus in under three hours – after which time they also shut down their servers.

So unusual was the spread that *CERT* (an organization not normally noted for its interest in viruses) issued an alert on Saturday 27 March concerning Melissa. This gave, amongst other things, a link to an irrelevant security warning about the ‘*Word 97* Template Vulnerability’ on *Microsoft*’s web site; information on how to update some anti-virus products to detect the virus, and an example of how to configure sendmail to reject all messages the subject lines of which start with ‘Important Information From’.

While this type of patch may have been acceptable in the short term, it clearly has significant problems as a long-term anti-virus measure. As it happens, however, the problem has been magnified somewhat by the discovery that, under certain fairly unusual circumstances, the virus can mail *uninfected* documents!

Conclusion

Melissa is undoubtedly the fastest spreading virus we have ever seen. As is now documented, its speed of spread attracted the attention of US law enforcement services, who have since made an arrest, giving David Smith worldwide notoriety. *VB* will, of course, follow the case.

Melissa

Aliases:	Maillissa.
Type:	*Word 97/2000* macro infector.
Trigger:	(1) Upon initial infection; (2) when the day and the minute are the same.
Payload:	(1) Mails the first fifty addresses in all *Outlook* address books; (2) inserts text into the current document.
Disinfection:	In a clean *Word* environment, delete the virus’ module with the *Visual Basic* editor.

CONFERENCE REPORT

IVPC You in Chicago!

[*This month we offer two different viewpoints on the recent IVPC conference in Chicago. The Chief Researcher at* SARC, *and the Product Manager of* McAfee Labs *make their respective reports. Ed.*]

Good Views and Good News – Carey Nachenberg

Mobile code threats, more Melissas on the horizon, managing anti-virus software, and content security – these and other topics were the buzz at this year's *International Virus Prevention Conference* (*IVPC*). The biggest names in anti-virus and industry were treated to picture-perfect weather and entertaining presentations in Chicago, USA. This year's conference was unique in that there were two keynote speeches; heavyweights from both *Symantec* and *Network Associates* delivered their vision of the future of content security and anti-virus in the enterprise.

IVPC had a total of thirteen different sessions this year. In one of the more interesting sessions, five corporate and government representatives from the front line provided insight into their daily routine battling viruses (I know all the anti-virus vendors were listening intently). Happily, I made it to my session 'Mobile Code Threats: Fact or Fiction' without so much as a headache after a long night of virus chat, raunchy jokes and a little alcohol at the bar. [*Subscribers may remember the incriminating photograph of Carey at the bar in Munich at VB'98.Ed.*]

After a fairly lively discussion by Virus Bulletin's ex-editor Nick FitzGerald and others, I think many conference attendees were surprised to find that not one of them had been hit by a wild malicious ActiveX or Java threat in their organization. At least there's some good news on the front!

Last month's *IVPC* immediately followed the *Gartner Group's* more general Information Security conference; this resulted in some new attendees and fresh perspectives. Given the interesting sessions, the great weather and the fine Chicago food, everyone enjoyed this year's *IVPC*.

Melissa, Melissa, Melissa! – Vincent Gullotto

Had enough? Perhaps not. The 1999 *IVPC* conference was not without her, but then again, how could it be? Melissa made her way into about every presentation and conversation over the two-day conference. She tended to hog the limelight as researchers, administrators and security wizards compared notes and swapped potential solutions.

This year's conference included some impressive papers. Outstanding presentations included Carey Nachenberg on 'Malicious Code and Threats', Péter Ször on '32-bit virus threats', and Jimmy Kuo's 'All About Melissa'. All credit to Jimmy, for creating a presentation, in two days, on the overall facts and affects of this particular virus.

This presentation generated a great deal of conversation among the attendees and researchers. From this stemmed a reminder that the infamous April 26 date was fast approaching and that Melissa may very well have helped some companies as they updated and scanned, and updated and scanned their environments.

The same old faces showed up again with new ideas and concerns. There were after-hours discussions lasting, as usual, late into the night, which in turn ended up being early mornings. Many of those that continued their programme of consecutive conferences travelled a great distance and showed great spirit and support for the researchers they work so closely with on a daily basis.

As I mentioned earlier, in addition to each of the numerous mentions of Melissa, there was a great deal of talk about trust and policies. The messages conveyed were delivered in a way that was simple and sounded almost surreal. They were spoken as reminders and recommendations – between them forming an efficient method of utilizing sensible measures for protecting an enterprise by establishing policies of 'do's and don'ts'.

The presenters also spoke of ways in which to demonstrate to users who and what they can trust. With these simple measures and consistent practices, companies can go a long way in developing safer environments.

This year's conference offered a twist with a customer/user panel as opposed to a researcher/security expert panel. This proved interesting as some of the largest corporations and agencies in America gave their accounts of the infamous Melissa weekend. All seemed to get through the episode somewhat the wiser. Each offered their antidotes to the crisis, presented ways in which they deal with viruses on a daily basis, and as always had some requests for the anti-virus community. For the most part they asked for more information, better response, and faster updates.

Despite the presence of the *Gartner Group*, attendance this year was much the same as last year. Perhaps virus prevention is just not quite interesting enough. It seems that in the IT and security sector, viruses do not seem to be quite as attractive as encryption or the ever popular firewall seminar. Funny – when was the last time a breach of an encrypted file generated as much news and concern as a virus that made it around the world in less than 24 hours? Let's face it, this is important stuff and perhaps companies might consider sending a representative or two each year, to a virus conference or two. They can almost be guaranteed to come away with much more than they expected.

FEATURE

Virus Writers – Part 1

Sarah Gordon
IBM Research

There are six questions I am often asked. The first is 'when will you update your research on virus writers?' The answer is 'all of the time'. Several years of research produced The Generic Virus Writer study, the results of which were presented at the *Virus Bulletin* Conference in 1994. This initial qualitative research provided many valuable insights into the cognitive development of some of the world's most prolific virus writers – at that time.

These insights allowed me to show that virus writers were *not***,** despite some claims, a homogenous group. Understanding their differences and discarding stereotypes, the research began to play a role in helping others to understand this pressing problem – and begin developing some strategies for combating it. It enabled us to realize that they, and perhaps others like them, could be expected to 'age out' of virus writing. Good to know; there were not that many virus writers at that time and any leaving that proclivity behind would significantly ease the problem.

The second question is really two-fold: 'what exactly is "ageing out", and how can "normal" kids do things which most adults view as anti-social?' The idea behind ageing out is relatively simple, and is well-accepted in other areas of research into anti-social behaviours [1, 2, 3].

Let us begin with one of the theories of moral development [4]. It is not the only one, but it is the one chosen as an instrument for the original study. As a child begins to mature, his moral/ethical development goes through a number of stages, with ages roughly correlated to levels in these stages:

Level 1: Pre-conventional morality.

Stage 1 – The 'rightness' of an act depends upon the immediate consequence of it. Rules are obeyed to avoid punishment.

Stage 2 – Naïve instrumental hedonism. Being good is the way to get a reward or satisfy a need.

Level 2: Conventional morality.

Stage 3 – Actions are judged on the merit of their intent. 'Right' is having a right motive and a concern for others. Conform to avoid disapproval or dislike of others.

Stage 4 – Acceptance of authority. 'Right' is keeping the rules of society. Conform to avoid censure by legitimate authorities, with resulting guilt.

Level 3: Post-conventional morality.

Stage 5 – Judgements become more flexible; rules must be impartial, and 'the welfare of the many' becomes paramount. Abide by laws for the welfare of the community.

Stage 6 – Normative ethics, based upon self-chosen principles. 'Right' is an obligation to the universal principles of equality, justice and respect for persons.

This is the short form of this particular theory. It is not without some weaknesses, primarily it disregards cultural differences that determine what is 'moral' in non-Western societies, resulting in a form of moral absolutism [5]. However, the strengths of this particular instrument are well-documented [6].

The existence of a normal, ethical, developmental stage/age relationship does not necessarily moderate individual behaviour consistently in any given situation until an individual is older, and capable of integrating thought and action in a more mature way. This brings us to the second part of the question 'How can otherwise "normal teenagers" do irresponsible "wrong" things like "writing viruses"?'

I am sure most readers can think back to a time when they, or their children, behaved in some reckless or anti-social way. Just as one could know it is 'wrong' to stay out after curfew when his parents have told him it is (a) illegal and (b) against the house rules, one can know it is 'wrong' to write viruses – yet, still *do* the 'wrong' thing.

Usually, in those people who are within ethical norms, the anti-social behaviours tend to go away as they grow up. (Whether or not those who commit the acts are labelled 'delinquent' often depends on whether they are caught; it can also depend on race or socio-economic status.) When these behaviours go away, it is sometimes referred to as 'ageing out'. Sometimes the behaviours may recur from time to time; usually they go away completely.

If it were really the case that the virus writers profiled were 'normal young people' in terms of general development, as the research suggested, we would expect them to 'age out' of virus writing. Would they? I pressed on, past the usual hurdles in longitudinal study, following up on the subjects over several years. (The only subject with whom I was unable to maintain contact was the adult employed virus writer and distributor.) To date, the original ex-virus writer has remained an ex-virus writer. The college student has aged out of virus writing. I would expect the last to follow suit, but this remains to be seen.

'Ageing out' will probably continue to be one factor in lessening the number of active virus writers. However, they do not all do it. That follow-up study also discussed developing trends, and predicted a future that was a bit darker. Okay, a lot darker.

The Darker Venture

Question three is 'how old are these guys?'. I have talked with virus writers who claim to have started in their preteen years, and given their level of skill and familiarity with viruses, I see no reason to disbelieve them; however, youth does seem to be diminishing as a primary attribute.

Whereas in the early days, virus writing groups were generally populated by young men in their mid-teens to early twenties, the mean age of the virus writers in one currently active and well-known virus writing group is 23; the oldest member is 33. I have talked with virus writers who are in their forties. This is indicative of one disturbing new trend featured in The Generic Virus Writer II – involvement of those who are older and possibly more ethically mature in virus writing. How can this be?

Sure enough, we saw more and more of this type of involvement of older people, and predicted this would continue and increase. This involvement seems to take various shapes, sometimes not malicious, just curious. For example, it is not uncommon for some adults involved in testing of anti-virus software to alter a virus in an ill-conceived but well-meaning attempt to see 'how good virus detection is'. No matter how well-intentioned, this can lead to problems, which are documented in [7].

Several macro virus variants appear to owe their creation to ordinary users' experimentation. This is sometimes carried out as part of a quest to 'understand' the virus; or it is done with what appears to be no good motive, as such viruses have been released into the wild seemingly intentionally.

It is unclear whether these trends are due to a change in people (unlikely), technology (possibly), or simply that experimenting with viruses is seen as 'less wrong' as we approach the year 2000. In general, when objectionable or questionable behaviours are tolerated, even tacitly, they can take on a 'legitimate' tinge of acceptability [8]. Research is currently in progress to shed some light on this. My guess is that it is a combination of the three.

Data taken from The Generic Virus Writer II seemed to indicate that there is indeed a 'New Age' virus writer beginning to take shape – older, more network-aware and more technologically advanced than some of his predecessors. Did I say older and network-aware? I did. The fourth question people ask me is 'what's next in viruses?'. Well, I hate to say I told you so, but…

Melissa Magic

With regard to the virus *writer* known as VicodinES, several self-proclaimed virus writers have expressed sentiments along these lines:

> If Vicodines did it, I'm sure he didn't realise how many problems this would cause. I know that Vicodines spread some of his viruses, but he always said that he doesn't want to destroy anything, he said 'he just loves to annoy people arround the world'. He hates destructive payloads, but he likes simple 'annoying' and rather humorous payloads like this 'I think that [username] is a big stupid jerk.' payload. I'm sure he wouldn't have released this virus if he had known how much problems it would cause. [9]

At the same time, some of the same virus writers express anger at the idea of a virus being distributed to unknowing and unwilling individuals: many virus writers have wiped their hard drives, vowing to lay low until things cool down. In the words of one virus writer:

> I hear how some vX people say that they'd kill the author of melissa as it is his fault for other vx people getting hunted now also, for vX webpages being closed and so on., even though my own webpage has been closed also it doesn't make me feel very good when i hear others talk about my friends like that. sure all of that has been caused by melissa, but i'm sure the author (of the virus) didn't want this to happen, he wanted to spread his virus (like many of these, now pissed off, vX people do also),and teach vX people some new things – not bring their sites down and get them arrested. [10]

Another had this to say:

> 31th March – Melissa fucked us. Melissa has been tracked down to its author thanx to Micro$oft GUID... They know have a proff that VicodinES is the author. Now the media hype has sarted again, and the word virus is everywhere.... And, TOTALLY unrelated to that, sok went down as well as codbreakers.... Weird, uh ?? My server is still running and kicking asses, you can use my board communicate if you want... (It's here for that, USE IT !!) Now I really wouldn't be VicodenES, because I think media will make him an example and he WILL be bashed… [11]

Yet another had this to say:

> to be honest guys,whoever wrote and spread melissa fucked all of us...to add more viruses to this thing would be lame as fuck and pointless....we would all just end up joining the now RIP authors.. for fucks sake get real people...we dont need any more grief . [12]

Profiles of individual virus writers are under re-evaluation, and are scheduled for presentation at The Blackhat Briefings in July 1999. Part 2 of this article (next month) will answer question five 'How have they changed?' and the most frequently asked question six: '*Why* do they do it?'.

1. Hollister, R. G. and Hill, J. *Problems in the Evaluation of Community Initiatives*. New York: Russell Sage Foundation. 1995.
2. Pfohl, S. *Images of Deviance and Social Control*: *A Sociological History*. 2nd ed., McGraw-Hill. 1994.
3. Keel, Robert. *The Evolution of Classical Theory: Rational Choice, Deterrence, Incapacitation and Just Dessert.* Rational Choice and Deterrence Theory. The Sociology of Deviant Behavior. 1999.
4. Craig, G. J. *Kohlberg's Stages of Moral Development.* Human Development. Seventh Edition. Prentice Hall. 1996.
5. Colby, A. & Kohlberg, et. al. *A longitudinal study of moral development.* Monographs of the Society for Research in Child Development, 48 (1-2 Serial 200). 1983.
6. Baumrind, *D. A Dialectical Materialist's Perspective on Knowing Social Reality*. New Directions for Child Development. 1978.
7. Gordon, S. *Real World Anti-virus Reviews and Evaluations - the Current State of Affairs.* Presentation. 19th National Information Systems Security Conference. National Institute of Standards and Technology, National Computer Security Center. Baltimore Maryland. 1996.
8. Craig, G. J. Development in Modern Life: The effects of television. *Human Development*. Seventh Edition. Prentice Hall. 1996.
9. Private communication. Used with permission. 1999.
10. Private communication. Used with permission. 1999.
11. Publicly available communication. 1999.
12. Publicly available communication. 1999.

INSIGHT

Engineering with Flair

Cindy Snow graduated from Brigham Young University (BYU) with a BS and MS in Computer Science, not to mention a minor in mathematics and a minor in business. Now Engineering Manager for *Intel*, she started her professional life as a programmer on the technical staff at *Hughes Aircraft* in California.

Her first project was typically colourful and dramatic – it involved work on the 688 nuclear submarine (the American sub in Tom Clancy's 'Hunt for Red October'). Her tasks included the design, code, test, and integration of the on-line monitor (the pre-cursor to an operating system) for the torpedo firing system.

Bitten by the Bug

She remembers it well, 'Debugging was wild considering that the computer, the assembler, the peripheral hardware, and our software were all in development. It took us three months to find one bug – a hardware error when doing certain double-word register divisions. I learned that the assembler dropped one bit in one instruction in my program.'

Six months after the final product had shipped, Cindy got a call from Newport, Rhode Island saying her application did not work. She was instantly suspicious, 'I asked if they had recently reassembled. They had, so I asked them to check the certain bit that always seemed to get dropped. They insisted, instead, that I fly out. I got on a plane from Fullerton to LAX, then to Boston, then rented a car and drove to Newport. I checked the bit. It had been dropped by the assembler. I fixed the bit and the on-line monitor was up and running. I drove to Boston, got on the plane… a long and expensive one-bit trip!'

After several years at Hughes Cindy and her husband Bruce started what was destined to be a large and close family. Through it all Cindy has managed to keep her sense of humour and developed a talent for multi-tasking – 'I had four small children who could climb on the roof, fill the toilet with soap bars, pour vegetable oil on the floor; paint the garage and both cars with flour; wash their hair with "make-up", fill their brother's mouth with sand; fall on the rocking chair and knock out a tooth; well, you get the picture.' Bruce and Cindy celebrated their 27th wedding anniversary at VB'98 in Munich.

It comes as no surprise that this particular family enjoys dramatic hobbies. 'We are white-water rafters' says Cindy, 'I'm the jinx. I've been at the bottom of every white water river in Idaho. We are hikers, bikers, and campers. We snowmobile in Yellow-stone Park in the winter. I love practical jokes, ran a book club (classics only), and led aerobics for several years. Every evening we gather in a circle, sing a song, say an evening prayer, and repeat our family motto – Don't marry a jerk!'

Into Anti-virus

Cindy worked at a consulting company for some years. Whilst there, *Intel* employees and her students from BYU asked repeatedly that she join *Intel*. She had no interest *until* she had the chance to manage the anti-virus team.

'Anti-virus development is more fun than anything – desktop GUI to server monitor UI to directory walking to kernel level zero (to intercept OS file actions). Development covers the gamut. Nothing is so dynamic as AV. There is always the 'unknown' aspect – we can plan and design, but get thrown for a loop with a new virus type. Every computer and every corporation needs AV protection. AV is always a top seller. What other software product offers such a range?'

Intel's identification as a developer of microprocessors is so strong that it is difficult to associate it with non-microprocessor products. Cindy remembers what she calls the 'strategic inflection point' that moved the company from memory chips to microprocessors in the early 1980s. Since that time, there continue to be numerous stepchildren coming out of *Intel's* Research and Development Department. The *LANDesk* software products, based in Utah, represent one such stepchild.

She is enthusiastic about her product, and can catalogue its history: ‘Intel’s LANDesk Software Products are produced as part of the Systems Management Division (SMD) of Intel Corporation. The software groups of SMD found their roots in Utah nine years ago. Dana Doggett, an engineer hired by the fledgling Novell Corporation, became an expert at NetWare, branching out to write software that made NetWare more usable.

‘His LANSchool and Print Server products caught the attention of LANSystems, Inc. – a New York based systems integrator. They offered him a job to continue work on the Print Server. They had named the product LANSpool and its sales were going well. LANSystems allowed him to work from his Utah home and modem in all new software. LANSpool exploded and the rest is history.’

Within six months the growing group, now selling four products, had put Utah on the map as the true headquarters for the software division of *LANSystems*. Growth continued until *LANSystems* had two distinct divisions: the Utah-based software company, and the New York-based integration company. Cindy recalls ‘Soon Intel pulled LANSpool from the product mix, assigning it to the Print Server group in Oregon – we had lost the product that provided 90% of our revenue! We needed to re-invent ourselves and do it quickly. We re-focused on a new concept – Desktop Management software.’

Either by fate or by luck, the first global computer virus scare, Michelangelo, hit right when Cindy and her team were redefining themselves. A version of the Michelangelo virus even sneaked onto a production machine and then onto a release disk of *LANSpool v2.13*. The need for anti-virus as part of Desktop Management was clear. *Intel* duly shipped *LANProtect*. Suprisingly, sales of *LANSpool* actually went up after the problem. Cindy thinks it got free publicity. ‘Intel even made the front page of USA Today! Once again, sales exploded and we again had sufficient revenue to develop our vision of Desktop Management.’

Anti-virus software sales boomed after the Michelangelo scare. This funded *Intel’s* growth into the full Management Suite of products *LANDesk* currently ships. The suite included, until *Intel* sold *LDVP* to *Symantec*, *LANDesk Virus Protect* (an outgrowth of *LANProtect*), *LANDesk Management Suite*, *LANDesk Server Manager*, *LANDesk Client Manager*, and *LANDesk Configuration Manager*.

When questioned on the subject of viruses and their creators Cindy is suddenly dismissive, ‘viruses are to space shuttle software what graffiti is to El Greco (my personal favourite). The old myth that virus writers are geniuses is rapidly being debunked. Those who interpret virus code often find it laughable. Most is rudimentary and undisciplined. A truly talented software engineer can make big bucks in honest pursuits. Virus writers today are more commonly viewed, and treated, as criminals. It is unwise and unnecessary for anti-virus companies (or anyone) to hire ex-virus writers.’

All Change!

In the February 1999 issue of *Virus Bulletin*, former Editor Nick FitzGerald wrote ‘And speaking of Intel, it pretty much silently switched detection engines...’. Cindy’s recollection of that time captures the fast-changing topography of her industry. ‘We planned a marketing blitz – Intel LDVP licenses IBM anti-virus technology – but, before the words got out of our mouths, they hung open! Symantec had bought IBM’s AV technology. The anti-virus business ecosystem was maturing; the dominant players gaining strength to themselves like a whirlwind. We had to be sucked in or left behind.’

She dealt with her disappointment in typically strenuous fashion, ‘The sale of the product meant the dismemberment of our team. I immortalized my frustration at the sale of LANDesk Virus Protect by building a 100-yard rock wall, named ‘LDVP Lament.’ Intel requests a downsize when a product with a large staff is sold, so our close-knit team of 30 was almost immediately reassigned to different projects. It was a perverse and frustrating time. I took it out on the rock! After a month of vigour, Bruce joined the effort. We gathered the rock, dug and hauled hundreds of wheelbarrows of dirt, and built the 100-yard rock wall ourselves. We had to replace two sets of wheelbarrow wheels, and broke two shovels in the process!’

LANDesk management software will continue to include anti-virus capability, but it will license it. Cindy has got plans of her own; she and another team member and have proposed a ‘new business’ to Intel which was just approved for initial funding. She appreciates that security and anti-virus have growing viability as the Internet expands and the world converges.

Cindy Snow’s rationale neatly combines her experiences as a mother and a Manager of a constantly changing engineering team, ‘LANDesk Virus Protect customers were mainly corporate. Corporations, until recently, had their computers (servers and desktops) tucked tidily in their corporate buildings and connected via IT-managed intranets. Like parents of young children, IT pushed information and configurations, and controlled their children. When desktops got sick, IT visited. When desktops weren’t awake, they sat quietly in their cribs.

‘Now, the desktop has hit its teen years. It goes out at night. It travels in cars, planes, and trains. In connects with the corporate LAN in the daytime and with the Internet (outside the firewall) at night. It may bring home unwelcome friends, picked up via a night-time rendezvous. It may not get (IT’s) urgent messages – or may get mixed messages from multiple sources. Now the desktop is mobile, and the Internet the network. As the mobile desktop walks out the door, IT loses control. When it walks in the door it needs to be trained to tell the parent (IT) that it’s home and pick up pertinent messages. Instead of pushing and controlling, IT must recognize the maturation to the mobile client, teach it correct policies, then let it manage itself!’

COMPARATIVE REVIEW

Windows-shopping

Though it did not prove to be as problematic as first thought, various stability problems were encountered in the previous *Windows 98* Comparative Review some six months ago. It was with a degree of trepidation, therefore, that *VB* approached this review.

Eighteen products from across the globe were submitted for entry into the *Windows 98* arena, four of the offerings featured in the previous test being absent this time – *eSafe Protect*, *Intel LANDesk*, *Norman ThunderByte* and *Stiller Integrity Master*.

Test Procedures

Three identical machines were used for every aspect of the testing, and the hard disks of each were completely rewritten from the approprate image files prior to the installation of each of the products. Despite the three machines being nearly identical, all the timed tests (disk scanning rates and overhead tests) were performed on a single PC disconnected from the local network. The other two machines were simultaneously used to perform both the on-demand and on-access detection tests.

The test-sets were updated from those employed in the previous comparative, and, where appropriate, matched to the February 1999 WildList. Due to a delay in the publication of the WildList, the call for products deadline was extended from 26 February to 3 March 1999.

Following its spring clean the WildList is merely a shadow of its former self totalling just 145 viruses compared to the 266 that featured in the March NT comparative (based on the January 1999 WildList). New additions to the list include W97M/Class.B, W97M/Ethan.A, W97M/Brenda.A and W97M/Nono.A. Additionally, the polymorphic multipartite One_Half.3577 joins its 3544 byte comrade.

For products that provided a facility to scan network drives, all detection tests were performed with the test-set stored on a network drive as a read-only share. For products that either did not permit the scanning of network drives or were incapable of producing a workable log-file, the test-set was copied to a local hard drive, and the products were set to ‘Delete File if infected’.

In all cases the detection tests were initially performed with the default configuration settings – i.e. those selected after a fresh installation prior to any user intervention. Perhaps the use of a larger, bolder typeface for this previous statement may help some of the developers register this point, but then again perhaps not? Following the first test runs performed with such configurations, the tests were typically repeated with alternative, more thorough, options selected. Details, where appropriate, can be found within the report for each product.

The timed tests were performed in accordance with previous comparatives, such that the scanning rates can be directly compared to previous results. Hard disk scanning rates were determined by timing the scanning of 5,500 executables, a process which doubles up as a false positive test. Floppy disk scanning rates were measured for both clean and infected files, using two disks, identical except that the files on one were infected with Natas.4744.

A second Clean set consisting entirely of OLE2 files is currently being prepared for future comparatives. This will facilitate the measuring of scanning rates over OLE2 files.

To measure the overhead of the on-access scanners, 200 files were moved using XCOPY. In contrast to previous comparatives, these 200 files were composed of 100 executables and 100 OLE2 (.DOC and .XLS) files. The OLE2 files were included in order to make the overhead tests as realistic as possible. The overheads have been normalized with respect to an average baseline of 12 seconds and are presented in units of time.

Complete detection and timed test results are presented in the main tables. The overall In the Wild detection rates are corrected by weighting them to the number of samples of each virus. Thus, for cases where there are multiple virus samples in a particular test-set (especially relevant to the Polymorphic test-set), the results are not distorted. The results reported in the summaries are only for on-demand scanning unless otherwise indicated.

Alwil Avast32 v2.0-730

ItW Overall	99.8%	Macro	96.5%
ItW Overall (o/a)	n/a	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.8%

In the last *Windows 98* comparative *Avast32* went home with a VB 100% award for total In the Wild detection, but unfortunately this was not to be repeated this time. Failure to detect one of the EXE samples of Win95/Fono was all that stood in its path.

Performance elsewhere in the testing was maintained at the level expected from previous reviews of *Avast32*. The Czech product once again proved to be as stable as ever, and unlike several of its competitors detected floppy disk changes consistently during the on-access scanning tests. High detection rates were returned against all the test-sets, the area of most concern perhaps being *Avast32’s* detection of macro viruses.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	44	100.0%	525	99.9%	99.8%	2671	96.5%	14435	99.9%	1260	99.8%
CA InnoculateIT	44	100.0%	526	100.0%	100.0%	2747	99.1%	14433	99.9%	1258	99.7%
Command AntiVirus	44	100.0%	525	99.9%	99.8%	2737	99.0%	14444	100.0%	1251	99.3%
Cybec Vet AntiVirus	44	100.0%	523	99.7%	99.4%	2643	96.0%	14430	99.3%	1261	99.8%
Data-Fellows FSAV	44	100.0%	525	99.9%	99.8%	2747	99.3%	14444	100.0%	1252	99.6%
Dialogue Science DrWeb32	44	100.0%	526	100.0%	100.0%	2640	94.9%	14444	100.0%	1263	99.9%
Eset NOD32	44	100.0%	526	100.0%	100.0%	2750	99.3%	14444	100.0%	1264	99.9%
Frisk F-Prot	44	100.0%	526	100.0%	100.0%	2741	99.1%	14444	100.0%	1260	99.6%
GeCAD RAV	44	100.0%	509	99.0%	97.0%	2729	98.6%	13668	95.7%	1206	96.3%
Grisoft AVG	44	100.0%	525	99.9%	99.8%	2618	94.5%	14440	99.9%	1233	98.4%
H+BEDV AntiVir	42	95.4%	449	92.5%	86.1%	2419	88.5%	12930	85.8%	1239	99.0%
iRiS AntiVirus	44	100.0%	526	100.0%	100.0%	2750	99.2%	14433	99.9%	1258	99.7%
Kaspersky Lab AVP	44	100.0%	526	100.0%	100.0%	2754	99.4%	14444	100.0%	1261	99.8%
NAI VirusScan	44	100.0%	514	99.3%	97.8%	2742	99.2%	14190	98.8%	1264	99.9%
Norman Virus Control	44	100.0%	526	100.0%	100.0%	2712	98.3%	14444	100.0%	1249	99.5%
Proland Protector Plus	36	81.8%	318	65.9%	62.1%	1284	46.9%	2275	14.5%	658	60.5%
Sophos Anti-Virus	44	100.0%	526	100.0%	100.0%	2703	98.4%	14444	100.0%	1249	99.3%
Symantec Norton AntiVirus	43	97.7%	525	99.9%	99.6%	2725	98.4%	14443	99.9%	1247	99.5%

CA InnoculateIT v4.53

ItW Overall	100.0%	Macro	99.1%
ItW Overall (o/a)	97.8%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.7%

The user-friendly and intuitive (if slightly outdated) layout of the user interface initially lulled the innocent reviewer into believing that the testing of *InnoculateIT* from *Computer Associates* would be a relatively painless process. How true it is that first impressions can be deceptive…

On-demand ItW file and boot virus detection was perfect, resulting in *InnoculateIT* retaining its VB 100% award. This impressive detection rate is not the end of the story however. After finishing each scan of the test-set, the program hung immediately upon choosing another scan. Exiting and restarting the program avoided this problem, but on reloading, *InnoculateIT* gave false warning messages about viruses being in memory. Annoyances such as these have been encountered and reported in previous reviews, but hopefully, will be fixed in the near future so as not to plague *VB* in the future.

Matters became worse when testing the on-access scanner, which exhibited extremely poor stability. When attempting to open and close the infected test-set files stored on a network drive, a dialog box saying that REALMON had performed an illegal operation appeared persistently.

In order to test the on-access scanner therefore, the test-set had to be copied to a local drive, and the scanner set to delete infected files. Even then, only clusters of 100 or so files could be opened and closed without the system hanging. Trawling through the Polymorphic test-set in such a manner was considered too depressing, not to say onerous, a task and as a result the on-access capabilities of *InnoculateIT* have not been tested against this particular *Virus Bulletin* test-set.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	44	100.0%		n/t	n/a		n/t		n/t		n/t
CA InnoculateIT	44	100.0%	514	99.3%	97.8%	2734	98.8%		n/t	1255	99.6%
Command AntiVirus	44	100.0%	525	99.9%	99.8%	2737	99.0%	14444	100.0%	1250	99.3%
Cybec Vet AntiVirus	44	100.0%	523	99.7%	99.4%	2640	95.9%	14430	99.3%	1261	99.8%
Data-Fellows FSAV	44	100.0%	525	99.9%	99.8%	2750	99.3%	14444	100.0%	1252	99.5%
Dialogue Science DrWeb32	44	100.0%	526	100.0%	100.0%	2626	94.7%	14444	100.0%	1263	99.9%
Eset NOD32	44	100.0%	526	100.0%	100.0%	2750	99.3%	14444	100.0%	1265	100.0%
Frisk F-Prot	44	100.0%	526	100.0%	100.0%	2700	98.5%	14444	100.0%	1260	99.5%
Grisoft AVG	33	75.0%	264	58.6%	52.1%	1500	55.5%	1651	13.5%	719	67.3%
H+BEDV AntiVir	42	95.4%	457	92.3%	87.5%	2381	87.6%	13176	86.9%	1238	98.9%
iRiS AntiVirus	44	100.0%	526	100.0%	100.0%	2747	99.1%	14432	99.9%	1258	99.7%
Kaspersky Lab AVP	44	100.0%	526	100.0%	100.0%	2754	99.4%	14428	99.8%	1258	99.5%
NAI VirusScan	44	100.0%	513	99.2%	97.7%	2742	99.2%	14190	98.8%	1250	99.3%
Norman Virus Control	44	100.0%	526	100.0%	100.0%	2715	98.3%	14442	99.9%	1249	99.4%
Sophos Anti-Virus	44	100.0%	525	99.9%	99.8%	2704	98.4%	14444	100.0%	1249	99.3%
Symantec Norton AntiVirus	43	97.7%	525	99.9%	99.6%	2725	98.4%	14443	99.9%	1247	99.5%

Command AntiVirus v4.54 (SP1)

ItW Overall	99.8%	Macro	99.0%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.3%

This was a fairly middle-of-the-road performance by *Command Antivirus* (*CSAV*), with detection rates too low for any accolades, yet too high for significant rebuke. The VxD sample of Win95/Fono proved to be a thorn in its side, remaining undetected in both on-demand and on-access tests, denying *CSAV* the VB 100% award. Simply changing the configuration settings to 'All Files' mode did not remedy the situation, the VxD sample proving too elusive a prey. Though disappointed with incomplete ItW detection, *CSAV's* developers can at least take heart from the high level of detection across the remaining test-sets.

In terms of speed *CSAV* is once again the fence-sitter, its performance somewhere in the middle of the pack, the scanning rate slightly improved over that reported previously. The overhead of the on-access scanner remains high, however, at a little over 400%.

Cybec Vet AntiVirus Premium v9.9.4.0

ItW Overall	99.4%	Macro	96.0%
ItW Overall (o/a)	99.4%	Polymorphic	99.3%
ItW Boot	100.0%	Standard	99.8%

Despite *Cybec's* acquisition by *Computer Associates*, *Vet AntiVirus* is still attributed to the Australian development team. Three XLA samples of XM/Compat.A remained undetected during on-demand scanning pulling the VB 100% award away from *Cybec Vet's* grasp. Complete detection of the In the Wild test-set was achieved with the configuration settings set to scan 'All Files', once again raising the issue of which file types to scan and which not. Detection rates elsewhere were respectable, although the Macro test-set proved troublesome.

Speed tests revealed *Vet* to be as fast as ever, although it was pipped to the winning post by a Slovakian competitor. The slight blemish on its high scanning speed was the reporting of a suspected infection during scanning of the hard disk Clean set. A commendably low overhead was observed upon activation of its resident protection.

Data Fellows F-Secure Anti-Virus v4.03.1090

ItW Overall	99.8%	Macro	99.3%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.6%

Data Fellows FSAV is another product this month to miss out on the VB 100% award thanks to Win95/Fono. Using the default settings, the VxD sample was missed in both on-demand and on-access scanning. This is attributable to the omission of the VxD file extension from the extensions list, since the sample was detected when the configuration settings were changed so that ‘All Files’ were scanned.

Respectably high detection rates were achieved against the other test-sets. The performance of *FSAV* against the macro test-set is much improved following the last comparative, the product showing a detection rate second only to *Kaspersky Lab’s AVP* for both on-demand and on-access scanning. Infected *PowerPoint* presentation and template files and the extension-less samples of the O97M/Tristate variants accounted for all the misses in the Macro test-set.

Results were not quite so favourable in the speed tests, however. *FSAV*, though not the slowest, was at the slower end of the scale for both floppy disk and hard disk scanning, with throughputs of approximately 20 and 600 KB/s respectively. The overhead of the on-access scanner was significantly higher than that of the other products, a feature which has not previously been associated with *FSAV*. This is presumably attributable to the inclusion of OLE2 files in the file-set copied during the tests.

Dialogue Science DrWeb32 v4.04b

ItW Overall	100.0%	Macro	94.9%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.9%

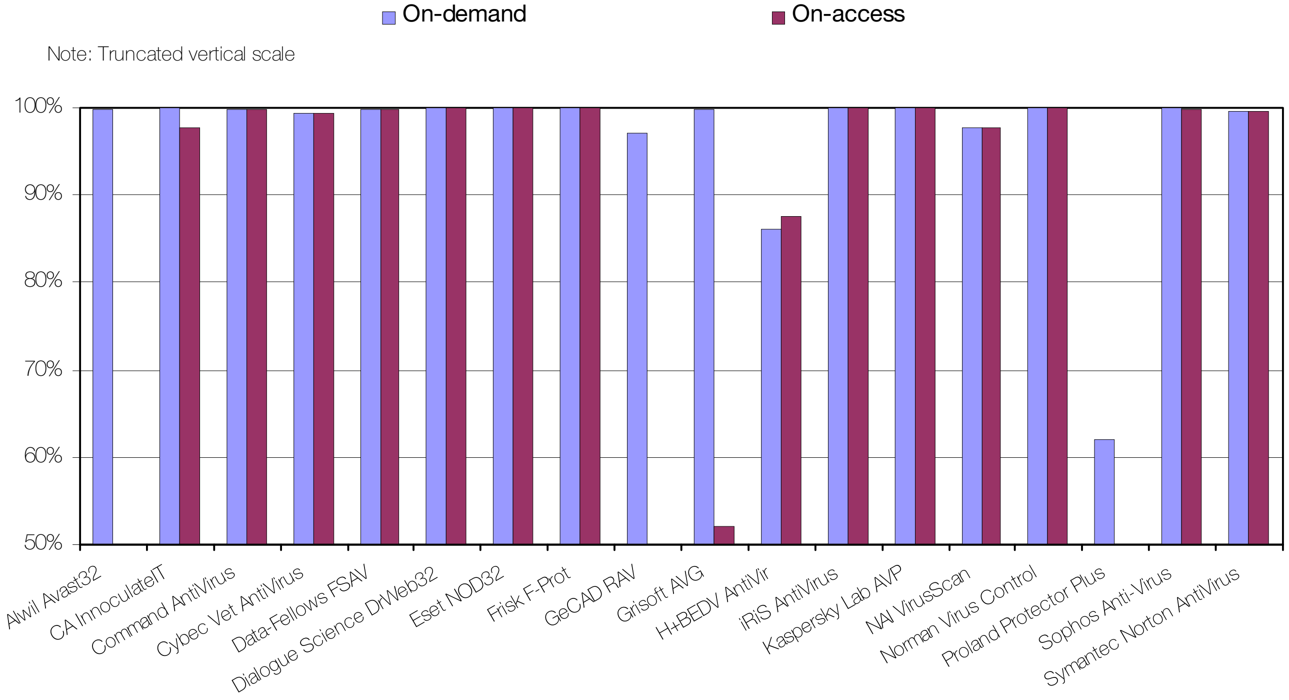
A beta product version was entered for this comparative by the Russian developers of *Dialogue Science’s DrWeb32*. The interface is certainly outdated, but extremely straightforward and usable. Contrary to previously tested *DrWeb32* products, this version features an on-access component called *SpIDer Guard* for *Windows 98*.

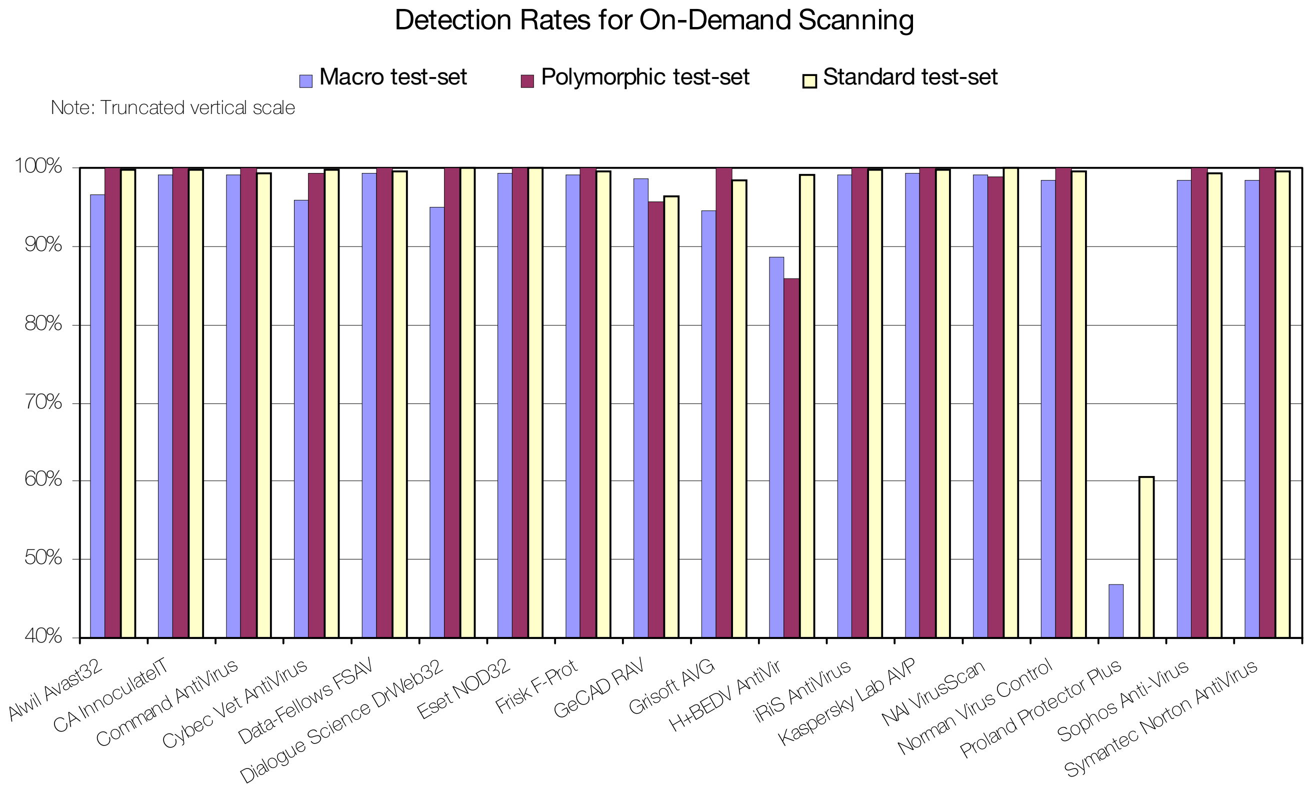
On-demand detection rates were admirable across all the test-sets, sufficient to earn *DrWeb32* the VB 100% award for detection of all the ItW viruses. The weakest area was detection of Macro viruses, where only a 94.9% detection rate was observed.

Extremely promising results were seen during testing of the new face of *DrWeb32*, the *SpIDer Guard* resident protection component. Detection rates mirrored those observed during on-demand scanning, the Macro test-set again proving more troublesome. Slight stability problems were encountered during testing of *SpIDer Guard*, mainly during on-access boot sector scanning.

Interestingly, the overhead of the on-access scanner when set to scan on File Open only, was much higher than that when scanning on File Close or File Open and Close. The hard disk scanning rate was at the slower end of the range

In the Wild Overall Detection Rates





for the products tested in this comparative but not significantly so. Perhaps more important were the false positives registered during scanning of the Clean test-set – one infection and 17 suspected infections were reported.

ESET NOD32 v1.15

ItW Overall	100.0%	Macro	99.3%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.9%

High detection rates on all platforms have been the norm for this Slovakian product in previous *Virus Bulletin* Comparative Reviews, and this month proved to be no exception. Aside from detecting all the In the Wild file and boot sector viruses, *NOD32* had the highest overall detection rates across all the other test-sets.

If this accolade was not enough, *NOD32* was also the leader of the pack in terms of both hard disk and floppy disk scanning rates. Only a slight overhead was observed when the on-access scanner was activated – impressive given the high detection rate.

Frisk F-Prot v3.04 (trial version)

ItW Overall	100.0%	Macro	99.1%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.6%

Better known as one of the engines behind the *DataFellows FSAV* product, this is the first showing of *F-Prot* as a standalone antivirus product in a *Virus Bulletin* review.

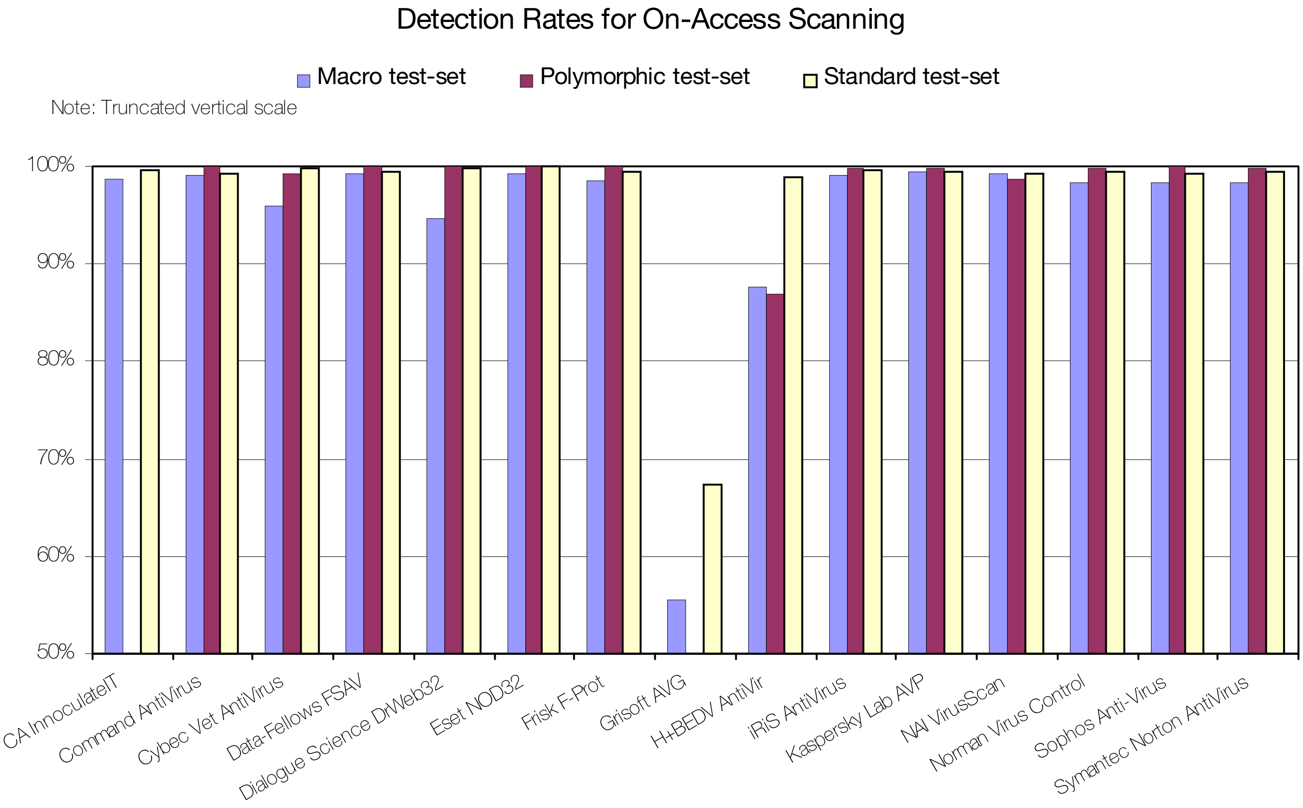
The Icelandic developers obviously believe that first impressions count, and *Frisk F-Prot* is up there with the best of them, delivering high detection rates across all the test-sets. Most importantly, complete ItW detection earns the newcomer a VB 100% award. At present this product is only commercially available in Iceland, Germany, Switzerland and Austria, although it was recently distributed on the cover CD of a major PC magazine. As to its availability elsewhere, it's a case of watch this space.

GeCAD RAV v6.54

ItW Overall	97.0%	Macro	98.6%
ItW Overall (o/a)	n/a	Polymorphic	95.7%
ItW Boot	100.0%	Standard	96.3%

Back in January 1998 Romania-based *GeCAD* submitted their anti-virus product *RAV v5.0* to *Virus Bulletin* for testing. Detection rates were far from perfect, but given that prior to testing the product was directed at a purely regional market, there were promising signs.

More than a year on from its first review, *RAV v6.0* has lived up to some of those early signs. All the ItW boot viruses were detected, but failure to detect 13 Marburg samples, 3 TPVO.3783.A samples as well as the VxD



Win95/Fono sample still keep the VB 100% award well out of reach. Elsewhere across the test-sets, the Polymorphic and Standard test-sets were *RAV's* weakest points in terms of detection rates.

Grisoft AVG v5.0.1241

ItW Overall	99.8%	Macro	94.5%
ItW Overall (o/a)	52.1%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	98.4%

Only one sample stood between *AVG* and its first VB 100% award, and there are no prizes for guessing which one. The VxD sample of Win95/Fono, having tripped up several other products in this review, was also missed by *AVG*. Unfortunately for the *Grisoft* developers, on-demand scanning of the other test-sets revealed slightly lower detection rates, especially in the Standard test-set.

The real weakness of *AVG* showed its face during on-access testing, however. Truly pathetic detection rates were observed against all the test-sets, with over 15,000 out of 19,000 virus samples missed. Little wonder then that the overhead of running the on-access scanner was negligible.

H+BEDV AntiVir v5.17.1.2

ItW Overall	86.1%	Macro	88.5%
ItW Overall (o/a)	87.5%	Polymorphic	85.8%
ItW Boot	95.4%	Standard	99.0%

Missing Win95/Fono and Moloch infected boot sectors coupled with a littering of misses against the ItW File-set led to *AntiVir* having the second worst ItW overall detection rate out of all the products submitted for testing – not pleasing news for the German *H+BEDV* development team. Against the other test-sets, detection rates were equally poor for on-demand and on-access scanning.

Aside from poor detection, the stability problems associated with the *VirusGuard* on-access scanner that were reported in a previous Comparative Review still remain. Numerous lock-ups and fatal exceptions were encountered during the overhead tests, making the process very laborious indeed. As if this were not enough, the 61 false positives reported during scanning of the Clean test-set ensure that the previously awarded timidity prize remains on its German mantelpiece.

iRiS AntiVirus v22.18

ItW Overall	100.0%	Macro	99.2%
ItW Overall (o/a)	100.0%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.7%

As has come to be expected of *iRiS Antivirus* (*iRiS AV*) in recent times, detection rates across the board were admirably high. With perfect detection of all the ItW file and boot viruses *iRiS AV* picks up its fourth VB 100% award. Detection in the other test-sets was consistently 99% plus, the Macro test-set being the weakest point of *iRiS AV*.

	Scanning Speed						False Positives + [suspected]
	Diskette - Clean		Diskette - Infected		Hard Drive - Clean		
	Time (seconds)	Throughput (KB/s)	Time (seconds)	Throughput (KB/s)	Time (min:sec)	Throughput (KB/s)	
Alwil Avast32	37	26.9	48	25.0	49:54	182.7	0
CA InnoculateIT	49	20.3	41	29.3	07:40	1189.0	0
Command AntiVirus	47	21.2	48	25.0	06:32	1395.2	[1]
Cybec Vet AntiVirus	25	39.9	30	40.0	02:35	3528.6	[1]
Data-Fellows FSAV	47	21.2	60	20.0	15:02	606.4	3 + [4]
Dialogue Science DrWeb32	43	23.2	40	30.0	15:52	574.5	1+ [17]
Eset NOD32	23	43.3	49	24.5	02:30	3646.2	0
Frisk F-Prot	33	30.2	51	23.5	06:32	1395.2	[1]
GeCAD RAV	38	26.2	65	18.5	11:47	773.6	8
Grisoft AVG	28	35.6	53	22.7	09:37	947.9	8
H+BEDV AntiVir	33	30.2	46	26.1	10:08	899.6	61
iRiS AntiVirus	49	20.3	40	30.0	07:44	1178.7	0
Kaspersky Lab AVP	59	16.9	48	25.0	07:59	1141.8	0
NAI VirusScan	36	27.7	62	19.4	05:10	1764.3	0
Norman Virus Control	31	32.2	56	21.4	04:56	1847.7	0
Proland Protector Plus	59	16.9	60	20.0	06:34	788.1	89
Sophos Anti-Virus	40	24.9	34	35.3	04:06	2223.3	0
Symantec Norton AntiVirus	64	15.6	62	19.4	06:21	1435.5	0

The interface is not pretty and wins no prizes for glamour, but in terms of functionality and performance it leads by example. The scanning rates observed for *iRiS AV* are reasonable, and a modest overhead of approximately 150% was observed when the on-access protection was activated.

Kaspersky Lab AVP v3.0.129

ItW Overall	100.0%	Macro	99.4%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.8%

Another safe bet in the high detection stakes, *AVP* from *Kaspersky Lab* did nothing to disappoint its loyal followers. High detection rates were registered across the board, and the stability problems that have previously been reported during on-access scanning seem to have been fixed, thankfully. The only problem encountered during testing was a build error creating problems for the installation program to overwrite an old system library file. This was solved by simply overwriting the existing library file with a more recent version sent by *Kaspersky Lab*.

Besides achieving 100% detection rates for both on-demand and on-access scanning of the ItW test-set, excellent detection rates were also observed against all the other test-sets. Having said that, on-access scanning of the Polymorphic test-set perhaps exposed a slight weakness in *AVP's* near-infallible armour, the product failing to detect 16 samples distributed across five viruses.

On-demand scanning of diskette boot sectors was a breeze thanks to the multiple disk option which requires only a single keypress in between diskette changes. Speed has not been one of *AVP*'s strong points in the past, and little has changed in this respect. Only modest throughputs of approximately 1140 and 20 KB/s were observed for hard disk and floppy diskette scanning respectively. The overhead of running the on-access scanner was in keeping with the bulk of the other products, at approximately 150%.

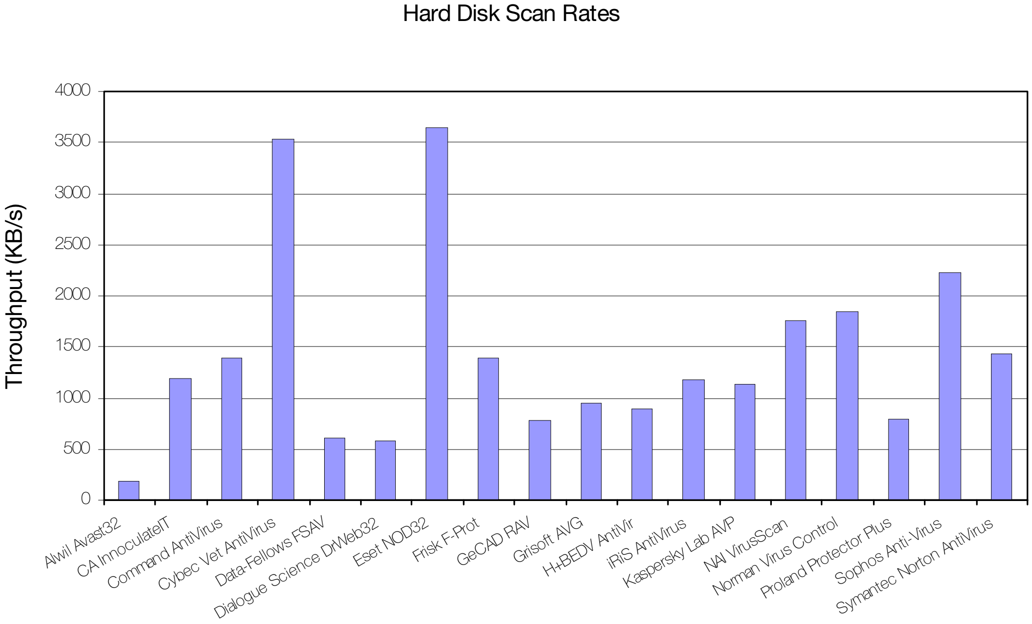
NAI VirusScan v4.0.2.4015

ItW Overall	97.8%	Macro	99.2%
ItW Overall (o/a)	97.7%	Polymorphic	98.8%
ItW Boot	100.0%	Standard	99.9%

Unfortunately for *Network Associates*, overall performance of the *McAfee*/*Dr Solomon's* hybrid seems to have dropped since the last *Windows 98* comparative review back in November 1998. The previously attained VB 100% award was missed this time around, due to the product failing to detect the screen saver (SCR) samples of Marburg and TPVO.3783.A. Just penance for failing either to bring the file extensions list up to date, or to introduce some sort of intelligent file type detection.

On the positive side, *NAI's VirusScan* was one of only two products to detect all the samples against the Standard test-set, and high detection rates were observed against the Macro and Polymorphic test-sets.

The overhead of running the *VShield* on-access scanner was noticeable (approximately 200%), but the stability problems reported in the previous comparative were not in evidence whatsoever.



Norman Virus Control v4.64

ItW Overall	100.0%	Macro	98.3%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.5%

The sole submission from *Norman* this comparative, *Virus Control* maintained the high standards it has set previously, attaining its seventh VB 100% award. A high level of protection is provided across the board by both the on-demand and on-access components, the latter being provided by the *Cat's Claw* component.

The '*Smart Behaviour Blocker*' that forms part of the *NVC* armoury is not testable by the standard procedures used throughout our tests, since as with *Alwil Avast32's* on-access scanner, it requires load-and-execute calls.

Proland Protector Plus v6.5

ItW Overall	62.1%	Macro	46.9%
ItW Overall (o/a)	n/a	Polymorphic	14.5%
ItW Boot	81.8%	Standard	60.5%

This is the third appearance of a *Proland Software* product in a *VB* comparative, the previous two being the *Windows NT*-based product versions. Once again the product name is irony itself, with extremely poor detection rates across the board. The pessimistic (or is it realistic?) will simply scoff at the presented statisitcs, dismissing *Protector Plus* as a contestant barely suitable for a first round warm-up.

The optimistic will see signs of improvement in the detection rates, especially in the detection of boot sector infections. Such signs are there, although many may argue that it would take a fool rather than an optimist to choose to protect their system with this Indian anti-virus offering.

Sophos Anti-Virus v3.19

ItW Overall	100.0%	Macro	98.4%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.3%

In the fortunate position of being the alphabetical successor to *Proland Software's* meagre offering, *Sophos AntiVirus* (*SAV*) is the opera singer following the karaoke flop.

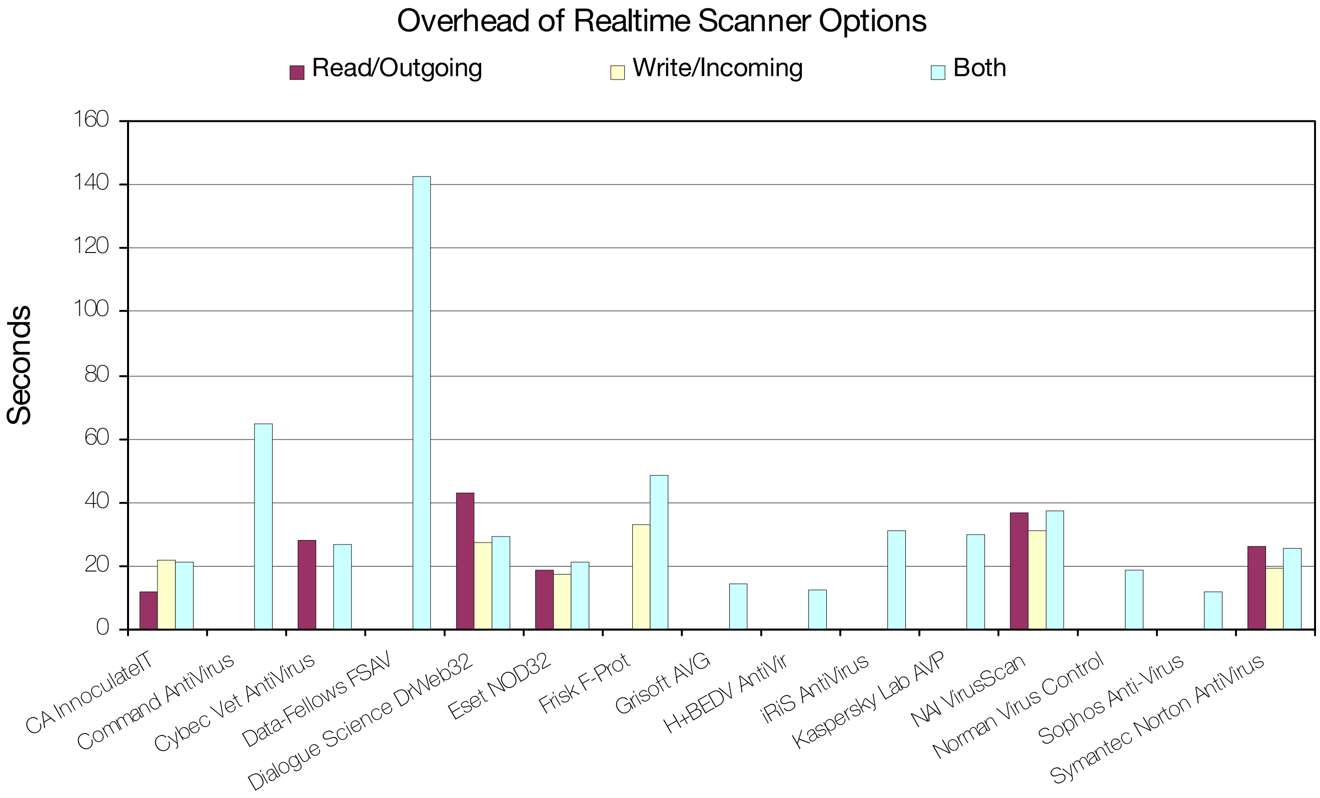
Maintaining the high standard that has been evident through previous comparatives, *SAV* is the last candidate in this line-up to receive the VB 100% award. Interestingly the on-access component *InterCheck* does not quite match up to the on-demand scanner, missing the troublesome VxD sample of Win95/Fono from the ItW test-set.

Along with several other products, detection in the Polymorphic test-set was perfect for both on-demand and on-access scanning. However, detection rates in the Standard and Macro sets though high, are not quite up to the mark set by many of *SAV's* competitors.

Symantec Norton AntiVirus v5.01.03

ItW Overall	99.6%	Macro	98.4%
ItW Overall (o/a)	99.6%	Polymorphic	99.9%
ItW Boot	97.7%	Standard	99.5%

Another 'big name' product failing to deliver the goods that might be expected from previous reviews is *Norton AntiVirus* from *Symantec*. Samples were missed in both the ItW File and Boot test-sets, Win95/Fono being the proverbial eel on both occasions. *Virus Bulletin* has been informed that the detection problems encountered with Win95/Fono have now been sorted out, but only after submission of *NAV* for this review.



Detection in the ItW File test-set was 100% when the on-demand scan was run in 'All Files' mode. However, even the simple remedy of adding VxDs to the default file extension list would not have brought the 100% award home to *NAV*, since the Win95/Fono infected boot sample was also missed.

Conclusions

In answer to the question of stability worries mentioned at the start of this review, thankfully no major problems were encountered. The on-access components caused most of the error messages, blue screens of death and system hangs that were observed.

Detection levels were generally very high, with eight, fourteen and sixteen products detecting 99% plus of the samples in the Macro, Polymorphic and Standard test-sets respectively (on-demand scanning). Similarly high detection rates were observed for on-access scanning of these test-sets for the products offering what has come to be a semi-essential feature of any anti-virus product.

Congratulations are due to the eight finger-on-the-pulse products who managed complete detection (on-demand) of the viruses in the February 1999 WildList. So hats off to *CA InnoculateIT*, *Dialogue Science DrWeb32*, *Eset NOD32*, *Frisk F-Prot*, *iRiS AV*, *Kaspersky Lab AVP*, *Norman Virus Control* and *Sophos AntiVirus*. Win95/Fono has been on the WildList since December 1998, and so the problems it has caused products seem inexcusable. For whatever reasons, various products missed infected files and/or boot sectors.

The age-old issue of what and what not to scan, seems to creep into each and every Comparative Review. This is not surprising – were we to run all the tests with each product set to scan 'All Files' the detection rates would certainly be higher and the marketing teams happier, but unfortunately the VB 100% award would also become cheaper.

With continual developments in the field of Macro viruses, choosing what to scan according to file extension alone is far too simplistic. Samples are not introduced into the *Virus Bulletin* test-sets purely with the aim of catching products out. Instead they simply reflect real world viruses as best possible. Users are not concerned with file extensions or file types. They merely demand what is offered on the box – protection from in the wild viruses. Unless developers are on the ball, forthcoming changes to the WildList could see some of the VB 100% awards slipping from the fingers of some established products.

Technical Details

Test Environment: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, all running *Windows 98*. The workstations could be rebuilt from image backups and the test-sets were in a read-only directory on the server. All timed tests were performed on one machine that was not connected to the network during the timed tests, but otherwise configured identically to the detection test condition.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199905/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW

NAI NetShield v4.0.2 for Windows NT

Martyn Perry

After six months or so of wedded bliss, how are the progeny created from the marriage of *Network Associates* and *Dr Solomon's* behaving themselves? This month we take a look at one such product.

NetShield's server licence is based on a *McAfee* Licence Agreement and runs for two years. A year 2000 compliance statement is included in Y2K.TXT.

Presentation and Installation

The supplied CD loads without autoinstall and allows the user to browse the various directories and subdirectories for the required product and operating system version. Installation follows the normal sequence of events by presenting a set of options. The first choice to be made is a decision to perform a local or a remote installation. A local install was chosen here, which led to a choice of Typical, Compact or Custom install, the main difference being whether Alert Manager is included in the installation. The final selection concerns which target directory to use. A nice touch is the confirmation of the settings before loading.

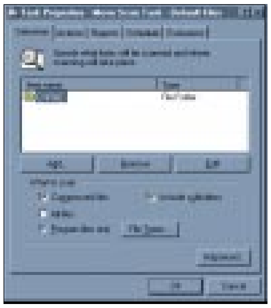
At the end of installation, a SETUP.ISS file is created which records the various installation options. This file can be used to install the product onto other machines. For the purpose of these tests, the components installed on the *NT* server are NetShield Console, NetShield Task Manager, McShield on-access scanner and Alert Manager.

What I like about this product is the continued tradition of detailing the function of each file installed. It also highlights the fact that some files are located in program directories away from the main body of files. This means that an administrator can identify files from a particular product. This is especially relevant for users needing to check files from various vendors for Y2K compliance. It would be useful if more anti-virus vendors documented this kind of detail.

The EICAR test script file is included. This allows the effect of a virus being detected so that the alert functions can be checked without resorting to an actual infection.

NetShield

The scans for *NetShield* are defined as tasks. Each task consists of configuration options. There is a task wizard which is, essentially, a step-through sequence of the options available under the standard task editor.



The detection option defines what is to be scanned (drive, directory or individual file). The choice of scanning all files or just a default selection can be made. In the event of a virus being found, actions to be taken include: Continue scanning, Move infected file to a folder, Clean infected file, and Delete infected file. These come with an additional option to notify the Alert Manager.

Reporting on the scan activity can be included with the choice of setting the log file and the items to be logged including virus detection, cleaning, deletion, and moving. These depend on the action option taken earlier, along with session settings and summary with a date and time stamp.

Scanning Options

The default set of files to include in a scan are COM, EXE, DO?, XL?, MD?, VXD, DLL, RTF, BIN, SYS, and OBD. In a separate table there is the option to create an exclusion list. The default entries are PAGEFILE.SYS, …\NetShield NT\ and its subdirectories.

With regard to on-access scanning, the task can be set up in a similar way to the Manual scan but this time there are different options available. The types of file to be scanned can be all files or specific extensions. The default list is the same as those for Manual and Scheduled scans. There are also choices about when to scan – inbound files, outbound files, floppy during shutdown and network drives.

There is a separate option to activate File Scan Caching. This is used for performance improvement by only checking a file the first time it is accessed after either the system or the Task Manager is started. If it appears that the file has been amended, then it will be rescanned. For timing test purposes the cache was switched off, so that the files were checked each time.

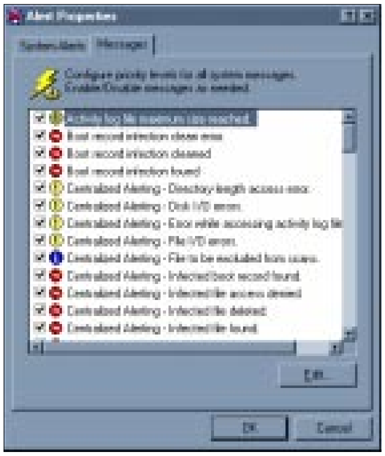
It is possible to control whether on-access scanning is enabled at system startup or not. In the event of a virus being found, then one of the following actions can be chosen to deal with the situation. The options are to Clean infected files automatically (if it cannot be cleaned, then it is renamed with a VIR extension), Move infected files to a folder, Deny access to infected file and continue, and Delete infected files automatically.

With the move option, the files are relocated to the quarantine directory (INFECTED). A log file is left in the original directory (INFECTED.LOG). This lists the files that have been moved and their destination directory. There is an additional option of sending a message to the user. Reports and Exclusion options are the same as for Manual and Scheduled scanning.

Scheduler can be defined with options to run once, at start up, hourly, daily with a choice of days in the week, weekly with the day, monthly with day in the month. The start time can be defined separately. The default file selections are the same as for Manual scanning. The final option provides an exclusion list, again the same as for a Manual scan.

Administration

There is a tools option which handles the configuration of alerts and the Alert Manager. The Alerts configuration provides for the centralizing of the various alerts into a specific folder and activates the Alert Manager.



Configure priority levels for all system messages.
Enable/Disable messages as needed.

☑ Activity log file maximum size reached.
☑ Boot record infection clean error
☑ Boot record infection cleaned
☑ Boot record infection found
☑ Centralized Alerting - Directory length access error.
☑ Centralized Alerting - Disk I/O errors.
☑ Centralized Alerting - Error while accessing activity log file
☑ Centralized Alerting - File I/O errors.
☑ Centralized Alerting - File to be excluded from scans.
☑ Centralized Alerting - Infected boot record found.
☑ Centralized Alerting - Infected file access denied.
☑ Centralized Alerting - Infected file deleted.
☑ Centralized Alerting - Infected file found.

The various system alert messages can have their priority level set at High, Medium or Low with the additional option of being able to edit the message associated with the alert.

The Alert Manager can be used to issue warnings to a number of destinations – Printer lists the printers which will receive the alert, SNMP activates SNMP alert messages, DMI enables DMI alerts if supported on the systems, Program allows the definition of a program that is to be run either the first time that the alert occurs or every time. Logging lists the systems which will receive information about alerts into their event logs. Sound sets the warning either as a WAV file (default WARNING.WAV) with the ability to select the response depending on the level of alert. Mercifully this option can also be turned off. The Forward option lists systems to which messages will be forwarded. Network Message lists computers receiving the alert, E-Mail and Pager are self-explanatory.

Updates

The scanner shipped for testing was v4.0.2 with engine v4.0.0.2. This was upgraded for use with v4.016 DAT files after a certain amount of difficulty. The product ships with an automated update and upgrade facility. The updated data files are available from a zip file. The automated facility unzips the files, creates backups of the originals and copies the new data files over the originals.

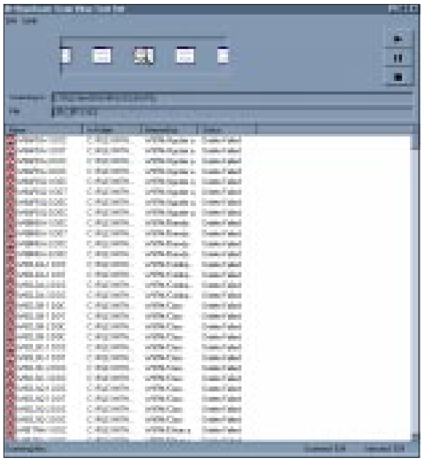
That is the theory. In practice, all appears to work without any error message. However, on inspection, the DAT files have not been updated. OK, try a manual approach. Files unzip fine, but attempting the copy gets errors with the DAT files, due to an access clash. This is because they are still in use by the scanner! It was necessary to close down the scanner as well as its services. This now allowed the files to be updated successfully. The automated update could be a very useful facility when it is made to work!

Scanning Overhead

To measure the extra work performed in detecting a virus, a diskette comprising 26 EXE and 17 COM files was scanned. The scan was repeated with the files infected with Natas.4744 virus. It took 24 minutes and 10 seconds to scan 5,500 clean files. No false positives were returned.

Detection Rates

The scanner was checked using the standard VB test-sets – ItW, Standard, Polymorphic, Macro and Boot Sector. The tests were conducted using the default scanner file extensions supplied. The scan action option was selected to delete the infected files. The residual file count was then used to determine the detection rate.



The initial results were way out of line with what would normally be expected, with many macro viruses appearing to have been missed because they still appeared in the original directory. The test was rerun with all files and the log file switched on. It appeared that many of the files were being detected as infected but removal was failing because the files were set as read-only.

The remaining files were reset to be read/write and the default test rerun. This still failed. On page 118 of the manual there is a note which says ‘If NetShield is unable to delete an infected file, confirm the file is not write-protected.’ If the action is changed to Move, then the files with detected viruses are moved to the quarantine directory. It appears that the *Network Associates* designers are trying to protect data files from accidental deletion during a clean-up, but I feel that this could be conveyed to the user in a much better way.

As far as the actual results are concerned, it is the typical set of results that you would expect from such parentage. The Boot sector test produced a 100% result. Eagle-eyed readers may have noticed that the Boot sector test-set has been substantially reduced. This is due to the revised WildList reporting a reduced set of Boot sector viruses.

Against the ItW test-set *NetShield* missed the screen saver (SCR) samples of Marburg and TPVO.3783.A, due to a failure of the program to scan such files with the default configuration settings. Performance against the Standard test-set was much more competent, with only the DLL sample of Win32/Ska being missed.

From the Polymorphic set, the Marburg screen saver samples were missed in addition to a number of EXE versions. W97M/Christy.A was missed in the Macro set, along with the *PowerPoint* virus samples (PPT and POT files) which are not included in the file extensions list with the default configuration settings. When tests were run with 'All Files' selected, the only change was to remove the Marburg screen saver files.

Real-time Scanning Overhead

To determine the impact of the scanner on the workstation when it is running, the following test was executed. 200 EXE and COM files of 21 MB were copied from one folder to another using XCOPY. The folders used for the source and target were excluded from the scan, avoiding the risk of a file being scanned while waiting to be copied.

The default setting of Maximum Boost for Foreground Application was used for consistency in all cases. Due to the different processes which occur within the server, the time tests were run ten times for each setting and an average taken. The tests were as follows:

- Program not loaded: establishes the baseline time for copying files on the server.
- Program installed, scanning inbound files only: tests the impact of the application scanning files being transferred in to the server.
- Program installed, scanning outbound files only: tests the impact of the application scanning files being transferred out from the server.
- Program installed, scanning inbound and outbound files: tests the impact of the application scanning files being transferred in and out of the server.
- Program installed, scanning inbound and outbound files *and* running Manual scan: tests the impact of the application scanning files being transferred in and out of the server with the additional load of an application accessing files.
- Program unloaded: run after the server tests to check how well the server is returned to its former state.

The normal overhead impact can be seen. Although the main tests were performed with cache off, one sample run was made to check the effect of cache on an inbound scan. The result was only about half a percentage point improvement. Again, the test was made without Alert Manager operating. One test run was made for inbound and outbound files with Alert Manager active. In this instance, the scan time increased by 95%, similar to running Manual scan.

Summary

How is the new scion performing? Frankly, there are a few teething problems which mar the overall effect of the product. Firstly, there were initial problems in updating the DAT files in the review software. For a single test server, this may not be a big issue, but trying to deploy it over a network of servers could be a different story. Furthermore, the issue of the way infected data files are handled needs to be tidied up and better documented.

Although the detection rate remains at the high level that we used to see from *Dr. Solomon's*, the scan rate was fairly average, especially when scanning floppy diskettes.

Finally, some of the Boot sector viruses were having early problems being read by the floppy handler. This was particularly true for those based on 720 KB floppies, although once the warning message was cleared, the detection was fine. While highlighting the problems, it is important to remember that the detection rate is still up with the best of them.

NAI NetShield v4.0.2 for Windows NT

Detection Results

Test-set[1]	Viruses Detected	Score
In the Wild Boot	44/44	100.0%
In the Wild File	514/526	97.7%
Standard	1264/1265	99.9%
Polymorphic	14190/14444	98.2%
Macro	2744/2773	99.0%

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 200 COM and EXE files (21 MB). Each test was repeated ten times, and an average taken.

	Time	Overhead
Not loaded	13.8	–
Loaded, incoming	20.8	50.7%
Loaded, outgoing	20.4	48.3%
Loaded, inc + out	20.5	49.0%
—– + manual scan	43.6	216.4%
Program unloaded	13.9	1.0%

Technical Details

Product: *NAI Netshield for Windows NT.*

Developer: *Network Associates Inc*, 3965 Freedom Circle, Santa Clara, CA 95054, USA.
Tel +1 408 9883832, WWW http://www.nai.com/.

Price: $5600 for 100 users, with full updates and upgrades for two years.

Hardware Used: Workstation: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NT Server v4.0 (SP3).*

[1] **Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199905/test_sets.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:

Virus Bulletin, 18 Commerce Way, Woburn, MA 01801, USA

Tel (781) 9377768, Fax (781) 9320251

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

END NOTES AND NEWS

***Sophos* has introduced a new calendar of workshops and courses.** May 1999 dates include: Advanced Internet Security on 12 May, Implementing *Windows NT* Security on 13–14 May and Practical Anti-Virus on 15–16 June. Courses investigating computer crime and misuse are planned for June and November. All the sessions will take place at the organization's training suite in Abingdon, UK. For more details on future dates or to register for a place, contact Karen Richardson; Tel +44 1235 544015, fax +44 1235 559935, or find more information at http://www.sophos.com/.

CompSec'99, the 16th World Conference on Computer Security, Audit and Control will take place from 3–5 November 1999 at the QE2 Centre, Westminster, London, UK. A Directors' Briefing will be held on 4 November. Conference topics include malicious software, firewalls, network security and Year 2000 contingency planning. For more details contact Tracy Stokes at *Elsevier*; Tel +44 1865 843297, fax +44 1865 843958, or email t.stokes@elsevier.co.uk.

***NetSec'99*, the 9th *Computer Security Institute* (*CSI*) Annual Network Security Conference,** is to be held from 14–16 June 1999 in St Louis, Missouri at the Hyatt Regency Hotel. Over 1500 computer and information security professionals are expected to attend the conference and its concurrent exhibition. For an events calendar or further details on this year's conference, contact the *Computer Security Institute*; Tel +1 415 9052626, fax +1 415 9052218, email csi@mfi.com or visit http://www.gocsi.com/.

***Data Fellows* announce the recent release of *F-Secure Workstation Suite v4.0* for use on *Windows 95*/*98* and *NT*.** It is supported by three key components: *F-Secure Administrator* – a Java-based console, *F-Secure Management Server* – the repository for policies, software updates, status information and alerts, and *F-Secure Management Agents* which enforce the policies on network workstations, servers and gateway machines. Prices start from $99 for a 100-user licence. *F-Secure Workstation v3.0* users may upgrade free of charge. For information contact Tracey Thomas in the US; Tel +1 408 9386700, fax +1 408 9386701, or email Tracey.Thomas@DataFellows.com/.

Following the panic about Melissa and the increasingly predominant role of email commerce in the virus news, ***Content Technologies*, the developers of *MIMEsweeper***, has conducted a recent survey of 50 users in UK corporations. 61% said that they had sent email to the wrong recipient at some point in their careers and 73% said that if a director emailed for information they would automatically reply without checking the source. *Content Technologies* deduces from this survey that 'spoofing' remains a little-understood phenomenon in the corporate arena. For more information about the survey, see the web site http://www.mimesweeper.com/.

***Command Software Systems* announces the release of *Command AntiVirus for Microsoft Exchange*.** Based on the *F-PROT Professional* engine and using *Command's HoloCheck* scanning technology, this product offers email and groupware virus protection. For more details visit the web site http://www.commandcom.com/.

Sybari Software* announce the immediate availability of an upgrade to *Antigen v3.15 which offers full support for *Domino R5*. This is an extension of *Sybari's Lotus R5* protection service. *Antigen v3.15* costs $4995 for a two year licence for 250 users. For further details contact *Sybari*; Tel +1 516 6308500 or visit the company web site at http://www.sybari.com/.

***Network Associates Inc* has released the *Magic Total Service Desk* (*TSD*) enterprise software suite**, which claims to automate the entire support and change management process, enabling organizations to centralize around a common IT support management application. For further details about this fully functional browser-based service desk solution and its extensive new features, contact *Network Associates*; Tel +44 1753 827500 or visit http://www.nai.com/.

Following the success of last year's conference exhibition, *Virus Bulletin* is now inviting those corporations wishing to exhibit at VB'99 in Vancouver from 30 September–1 October to contact Jo Peck at Virus Bulletin; Tel +44 1235 555139, fax +44 1235 531889 or email joanne.peck@virusbtn.com. 10 ft by 10 ft exhibition booths cost £2,500. This price includes two delegate registrations, with full social events and entry to conference presentations. The exhibition itself will be held very close to the technical and corporate session rooms at the Hotel Vancouver. Maximum exposure to all delegates is guaranteed as all tea and coffee breaks will take place in the exhibition hall. Find further details about the **1999 *Virus Bulletin* conference** at the web site http://www.virusbtn.com/.