ISSN 0956-9979 FEBRUARY 2003

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Another fine mess:** Although no dazzling new techniques were used in the construction of W32/Winevar.A, it still made the rounds on the Internet during its 15 minutes of fame, leaving those responsible for cleaning up the mess with a very long day ahead of them. See p.5.

• **XMHell:** While a good deal of time and effort has been invested in developing streamlined OLE2 engines that read only the macro-related sections of an *Office* document, when it comes to the new XML format included in *Office 11* a scanner will have to parse the entire XML storage. Users are unlikely to be happy about the resulting drop in performance. Gabor Szappanos believes there may be a solution. See p.8.

• **Epic proportions:** The line-up of products taking part in *VB*'s comparative reviews has seen a flurry of new submissions recently, and this month is no exception. Three newcomers bulk up the numbers this month and a total of 25 products for *Windows NT* are put on trial. See p.16.

CONTENTS

COMMENT

A Short Saga of Security Bulletins …

They say: 'It took the power of two C64s to put man on the moon … yet it takes a *Pentium III* to run *Windows XP* – what went wrong?'.

I don't know exactly how many C64s are needed to put a man on the moon, but I do know that *Windows XP* will not be used on any critical system on a space shuttle in the near future. It's not that *Windows XP* or *Windows 2000* are bad or insecure systems – in fact, since *Windows NT 4.0*, *Microsoft* has created a complex yet flexible, strong and sound security model. For all those *Linux* fans I have one question: how many years did it take to finally move further in access rights beyond the standard -rwxrwxrwx? Sure, now I can install grsecurity or even use *SELinux* if I am looking for a trusted operating system, but I already have many of those security features in *NT*, *W2K* and *XP*.

" Windows XP *will not be used on any critical system on a space shuttle in the near future. "*

And don't forget the *.NET* platform. When I first saw the platform I was amazed and terrified. *.NET* is huge – and it introduces the potential for a lot of new vulnerabilities – yet it seems to be working quite well and, personally, I would understand why many developers may want to move from Java to *Microsoft* technology. If only I could use it without *IIS* (actually I can!) or, better still, why can't *Microsoft* rewrite *IIS* to be more secure? They have all the necessary resources. For now, though, we have a new *Microsoft Security Bulletin* policy to cope with.

First (and I am sure many other people have noticed this), it seems that someone at *Microsoft* has decided that security comes in numbers. At the end of the day, why would anyone want to waste money on an *IIS* or *IE* rewrite? The easier – and more economical – thing to do is to incorporate several security problems into one security bulletin. If all goes well, the number of security bulletins issued will decrease. Unfortunately, debugging and disassembling tools like *SoftICE*, *IDA Pro* and *Spike*, not to mention some internal audit tools that will never see the light of day, are available to many researchers across the world. In the hands of an experienced auditor these tools can produce a lot of vulnerability reports.

But security is not just a technical problem. In fact it is a social problem, and most *Windows* users either don't care or don't understand the need for security. So *Microsoft* decided to take action and the result is that, today, we have two versions of every new security bulletin: one for security pros and another for casual users.

The flaw in this approach is highlighted by our observation that many users do not care about security, so it does not matter to them what information is included in a bulletin as they will never read it. Meanwhile, if you are still using the http://www.microsoft.com/security/ link you are doomed, as finding the list of all security bulletins is very tricky now. Perhaps I should stick to those new, short and easy-to-read bulletins after all!

However, the details of, for example, the WM_TIMER hack are not clear without reading the technical bulletin – and that's a variant of a vulnerability discussed some time ago on a number of mailing lists.

Since *Microsoft* is using the CVE (Common Vulnerabilities and Exposures) standard – and God bless them for this – it is still easy to count how many holes *IIS* has had during a one-year period without counting the number of bulletins. Unfortunately, you need to know about the standard and a lot of users don't know it or don't understand.

There are some network administrators who still believe that a smaller number of vendor advisories is proof of security level. In fact it is, but in the opposite way to that in which they think. So, here we have an example of a sound security model that has been weakened by poorly written user applications and a marketing decision to create easy to read bulletins.

Aleksander Czarnowski, AVET Information and Network Security, Poland

NEWS

Calling All Speakers

Virus Bulletin has extended the deadline for submissions from those wishing to present at VB2003, the Thirteenth Virus Bulletin International Conference, which will take place 25–26 September 2003 at the Fairmont Royal York hotel in Toronto, Canada. All AV-related subjects will be considered. Abstracts of approximately 200 words must reach the Editor of *Virus Bulletin* no later than **Monday 31 March 2003** and should be sent as RTF or plain text files to editor@virusbtn.com. More details, including a list of suggested topics for papers, can be found at http://www.virusbtn.com/conference/ ▮

Standing Up for Free Speech

Network Associates Inc. (*NAI*) has landed itself a hefty fine to start the new year after a New York court ruled against the company last month in a legal battle that has been ongoing since early last year. New York State attorney general Eliot Spitzer sued *NAI* in spring 2002 over an 'unenforceable clause' on its software products and website, which curtails the user's right to publish product reviews. The clause reads 'The customer will not publish reviews of this product without prior consent from *Network Associates Inc.*'. The NY attorney general asserts that this is a violation of customers' rights to free speech.

Meanwhile, *NAI* claims that the sole purpose of the clause is to prevent the publication of reviews of outdated versions of the software – and there have been plans since February 2002 to update the wording to reflect this more accurately. However, a year later, the company is still in the process of changing the clause; *NAI*'s legal representative Ken Roberts said, 'We're trying to get it done as quickly as possible.' Justice Shafer of the State Supreme Court in Manhattan ruled that the clause was deceptive, and ordered *NAI* to pay 50 cents for every copy of its products sold bearing the licence – which, *VB* imagines, mounts up to a fair number and may somewhat increase the speed with which the 16 words are updated ▮

Two Years for Three Viruses

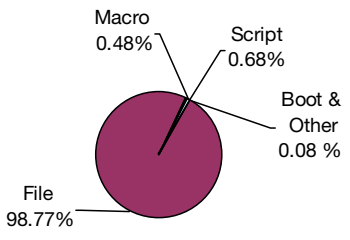
Simon Vallor, a 22-year-old web designer from Wales, who pleaded guilty to creating and distributing a trio of mass-mailing viruses – Gokar, Redesi and Admirer – has been given a two-year custodial sentence. The three viruses were proven to have infected 27,000 PCs across 42 countries. Vallor commented that he 'didn't have a clue it would do that' and it was 'quite a shock that it spread as it did'. Perhaps it isn't the *users* the anti-virus community should be trying to educate after all ▮

Prevalence Table – December 2002

Virus	Type	Incidents	Reports
Win32/Opaserv	File	7612	52.47%
Win32/Klez	File	3534	24.36%
Win32/Dupator	File	782	5.39%
Win32/Bugbear	File	545	3.76%
Win32/Funlove	File	439	3.03%
Win95/Spaces	File	330	2.27%
Win32/Yaha	File	240	1.65%
Win32/Magistr	File	216	1.49%
Win32/Nimda	File	93	0.64%
Redlof	Script	72	0.50%
Win95/Lorez	File	68	0.47%
Win32/Braid	File	64	0.44%
Win32/SirCam	File	61	0.42%
Win32/Kriz	File	58	0.40%
Win32/BadTrans	File	53	0.37%
Win32/Hybris	File	36	0.25%
Win95/CIH	File	31	0.21%
Win32/Lioten	File	28	0.19%
Laroux	Macro	26	0.18%
Win32/Elkern	File	15	0.10%
VCX	Macro	13	0.09%
Win32/Kovar	File	12	0.08%
Win95/Whog	File	11	0.08%
Win32/Winevar	File	10	0.07%
LoveLetter	Script	9	0.06%
Win32/Frethem	File	8	0.06%
Haptime	Script	7	0.05%
Others [1]		135	0.93%
Total		14508	100%

[1] The Prevalence Table includes a total of 135 reports across 65 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

Distribution of virus types in reports



LETTERS

Best Vendor Practice?

I write in response to comments (with which I sympathise entirely) in Roger Riordan's letter, 'What the User Wants?' (see *VB*, December 2002, p.4). I feel it is worth pointing out that not all software vendors treat their customers in the same way …

I work for a company that specialises in 'Virus Control'. Once purchased by the user, our product will include *all* updates for the period of the licence. If we release a new major version upgrade, users will be entitled to download and install the latest version completely free of charge. When users update their definition files they also download bugfixes (should any be required) and any advances in functionality that may have subsequently been built into the product. On the whole, software vendors seem to have followed examples set by the larger vendors in the market, but this does not mean we should all be tarred with the same brush.

I feel that the comments from an employee of one of our competitor (see *VB*, October 2002, p.2) demonstrate the problem in a nutshell – that some anti-virus companies are out of touch with the requirements of the marketplace. Users *do* require additional functionality, but at the cost of security and sloppy code? I don't think so. If an AV vendor advertised their software as 'full of functionality and bugs' they would not get many people queuing to buy. These marketing people are a cunning bunch! Never fear, Roger, some software companies still have scruples.

Matthew West,
Norman Data Defense Systems, UK

The Author Responds

In his response (see *VB*, December 2002, p.4) to my comment 'Best Practice or Wishful Thinking?' (see *VB*, October 2002, p.2), Roger Riordan questions whether I talk to customers. I spend a great deal of my time doing just that, and what I have learned is that Roger may be right: perhaps users aren't interested in features. More importantly, I have learned that users don't seem to be overtly interested in security either.

To illustrate my point, let me ask, why is VBS/Kakworm one of the most widespread viruses of all time, despite the fact that the patch for the scriptlet.typelib/eyedog vulnerability had been available for four months prior to the virus being released? The answer is clear. Users and administrators simply aren't keeping their systems up to date with security patches. Operating system vulnerabilities are a source of infection that users are not addressing. Blaming *Microsoft* isn't really justified – once aware of the vulnerability, they patched it; exactly what all OS vendors do. In fact, this is exactly how open source development works. Rather than try to point the finger, isn't it a better idea for the anti-virus industry to accept the kind of environment we are providing a service to, and design software accordingly?

I find it interesting that the responses to my article involved taking the opportunity to indulge in clichéd Gates-bashing and badly disguised sales pitches. No one has commented on the message of the piece: anti-virus software in general could be designed in a way that users and administrators find more useful.

Phil Wood, Sophos, UK

Information Wanted …

It was interesting to read Nick FitzGerald's article on CARO's virus-naming conventions (see *VB*, January 2003, p.7). The taxonomy of viruses has been discussed at meetings of the SIG Security (Swedish Information Processing Society's Special Interest Group Security) Malicious Code Committee.

We fully understand that a common, industry-wide agreement cannot be reached. However, we found it remarkable that few vendors have strict definitions in their own taxonomies, and do not explain the implication of their own naming conventions in their glossaries.

In the user community, we are preoccupied with one parameter – the speed at which malware spreads. As we all know, a fair description of the payload of any malware cannot be obtained during the first 48 hours of the attack (and sometimes never). The concept of 'worm/not worm' is therefore the major information. Viruses spreading only within a PC, Trojans, backdoors etc. are not considered to be a problem in a properly managed AV framework.

The problem users face is how to thwart a major attack, and the reaction time in an organisation is of vital importance. The most important information about a piece of malware is its spreading capability and this should be easily comprehensible within the name. We can imagine the need for this naming standard from the AV researchers' point of view. Realizing the difficulties of implementing a global standard, one has to conclude that allowing vendor-specific extensions (in the standard named 'modifiers') is a very wise solution. This compromise may make it possible for the vendors to agree on the convention.

We ask that all vendors use the naming convention to provide information about the spreading speed of the malware in its name, rather than having to find the information in the full technical documentation – which, while essential, can prove hard to read at the best of times. We would also ask at the start of a new year that vendors start explaining documentation keywords in their glossaries.

Jaak Akker, SIG Security, Sweden

Caring for VGrep

In his article 'A Virus by Any Other Name – Virus Naming Updated' (see *VB*, January 2003, p.7) Nick FitzGerald used his widely known sarcasm and dramatic statements to throw a bright and sparkling lure. I could not resist and took the bait.

Nick writes: 'VGrep's very existence is evidence of an odd contradiction in this industry. The fact that it is needed is proof of how little the industry as a whole cares about naming consistency …'. As someone in the industry who uses VGrep from time to time, I see this differently. It is true that the creation of VGrep was due to the need for cross-referencing many different virus names. However, these days I use VGrep for the same reason I use MiniMavis, Virtue and other tools – because I *do* care about naming consistency. And I don't think I'm very different from other members of the industry actively involved in virus research and facing naming issues on a daily basis.

Nick says: '…if the industry really cared about naming, VGrep would not be needed (neither would this article).' I dare to disagree. If we do care about the naming consistency, then any initiatives and tools that help limit the problems and help solve them (including VGrep) are useful and needed.

We need all the help we can get, while making our efforts and pushing for a better and more unified naming system. Having said that, one should openly and honestly admit that total (100%) naming consistency across all anti-virus (and security) products is an unachievable ideal (for many reasons) – just like 'world peace' (unfortunately). Does this let us off the hook and allow us to give up on better and unified naming (or peace for the war-torn countries)? Absolutely not. And because the task is so hard, tools like VGrep can be of help rather than an excuse for complacency. I do believe that some companies don't care about naming consistency, but I believe they don't care about VGrep either.

Jakub Kaminski, Computer Associates, Australia

VIRUS ANALYSIS

A Taste of Wine

Vincent Tiu and Rodelio Fiñones
TrendLabs, Philippines

In November 2002, a worm believed to have originated in Korea was discovered In the Wild. Interestingly, W32/Winevar.A was discovered at around the time that the AVAR 2002 conference was concluding in Seoul, Korea – and it seems that this was not merely coincidental, since the worm contains messages and links pertaining to AVAR or the Association of Anti-Virus Asia Researchers.

Dissecting Winevar

Unlike most worms compiled using high-level language, Winevar.A does not reveal its evil intentions immediately through easily distinguishable embedded text messages. This is because the author made sure that all text strings were encoded properly, to prevent them from giving away hints as to the true nature of the executable. When they are needed, these text strings are decoded on-the-fly using a simple decoding algorithm.

When executed, the worm drops a copy of itself as WINxxxx.PIF in the *Windows* system directory using the GetTempFileName API to generate a unique filename. Entries are created on each of the following Registry keys to enable the worm to execute every time the system reboots:

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices` (*for Win9x and ME only*)

`HKLM\Software\Microsoft\Windows\CurrentVersion\Run`

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

The Registry entries are as follows:

```
{default} = original worm path and filename
WINxxxx = %systemdir%\WINxxxx.PIF
```

where 'xxxx' is a random hexadecimal number generated by the GetTempFileName API.

After this, the worm creates a mutex named '~~Drone Of StarCraft~~' and checks whether an Internet connection is present. It does this by accessing the default web page of http://www.symantec.com/ and saving it to a temporary file named WINxxxx.TMP.

When an Internet connection is discovered, the worm employs the old 'hide-from-the-task-list' routine for *Win9x* machines using the RegisterServiceProcess API. It then creates a thread which is responsible for its propagation through email. After constructing the infected email template, the worm drops a copy of itself on the *Windows* desktop folder as EXPLORER.PIF.

Winevar on Email

Before constructing the infected emails, the worm deletes the entry on the following Registry key:

`HKCR\Software\Microsoft\DataFactory`

This Registry entry will contain the email addresses of all recipients and serves to prevent the sending of duplicate emails to the same address.

The worm obtains email addresses from the all too familiar parsing of *.HTM and *.DBX files found by searching through all fixed drives.

In order to prevent infected emails being sent to *Microsoft* email addresses, the worm ignores addresses that contain the string '@microsoft'. The email addresses are then added to the HKCR\Software\Microsoft\DataFactory Registry key to prioritize unique email boxes.

The worm then constructs the infected email, containing the ever-popular so-called I-Frame exploit or 'Incorrect MIME Header Can Cause IE to Execute E-mail Attachment' vulnerability, using information extracted from the system including the RegisteredOwner, RegisteredOrganization, DNS Server, local language name and the current date and time. The RegisteredOwner and RegisteredOrganization information are obtained in the following Registry keys:

`HKLM\Software\Microsoft\Windows NT\CurrentVersion` (*NT*-based operating systems)

`HKLM\Software\Microsoft\Windows\CurrentVersion` (*Win9x* operating systems)

If no registered owner is found, the worm sets the default owner as 'AntiVirus'. Similarly, the registered organization defaults to 'Trand Microsoft Inc.'.

An email infected with Winevar.A has the following construction:

```
From: %RegisteredOwner%<Victim's Email Address>
To: <Victim's Email Address>
```

The subject line may be

```
Subject: Re: AVAR(Association of Anti-Virus
Asia Reseachers)
```

with a one in three probability, or

```
Subject: N'4 %RegisteredOrganization%
```

with a two in three probability. Similarly, with a one in three probablility, the body may be

```
Body: AVAR(Association of Anti-Virus Asia
Reseachers) - Report.
Invariably, Anti-Virus Program is very foolish.
```

or, with a two in three probability,

```
Body: %RegisteredOwner% - %RegisteredOrganization%
```

Finally, the email attachments are as follows:

```
Attachments: WINxxxx.TXT (12.6 KB) MUSIC_1.HTM
WINxxxx.GIF (120 bytes) MUSIC_2.CEO
WINxxxx.PIF
```

It is important to note that the worm manipulates the From: field, which enables it to spoof the email sender, thereby making it harder to trace an infected email back to its source.

Like other worms employing this scheme, Winevar.A does not reveal the source of the infection to the email recipients, and it is the recipients' ability to carry out detective work that determines whether the infected sources can be identified and informed that their systems are running amok.

The worm sends a query to the DNS server (obtained via the GetNetworkParams API) to get the default mail server (MX record) of the target domain name extracted from the email address. If the query fails, it uses the DNS server's IP address as the SMTP server IP address. It then connects to port 25 of the SMTP server and uses SMTP commands to send infected mails to the target recipients.

WIN + AVAR = WINEVAR

The attached files named 'WINxxxx.PIF' and 'WINxxxx.GIF (120 bytes) MUSIC_2.CEO' are slightly modified copies of Winevar.A.

For tracking purposes, the author included the following information appended to the worm:

- Language (i.e. [ENU] for US English)
- Date and time (day-month-year, 24-hour format)
- Registered owner
- Registered organization

As a result of this embedded information, the size of the worm increases after each propagation.

Relating the worm to the AVAR organization further still, the attachment named 'WINxxxx.TXT (12.6 KB) MUSIC_1.HTM' contains a hyperlink named 'Association of Ti-Virus Asia Researchers', which is directed to the AVAR website, http://www.aavar.org/. The AVAR website contains information about the organization and its members, including a list of the members' email addresses, which can easily be collected by Winevar.A when parsing through HTM files in the browser's cache.

The attached HTML file also contains an old *Internet Explorer* exploit known as 'Microsoft VM ActiveX Component Vulnerability' which, when triggered, associates .CEO file extensions to normal EXE files by manipulating the HKCR\.CEO Registry key.

Fun Loving Winevar

Like Klez and Braid, Winevar.A joins the list of worms that contain a virus within them (Elkern for Klez, Funlove for Braid).

However, Winevar.A takes virus-embedding to a different level. Instead of the normal process wherein the virus is appended or inserted into the worm code, Winevar.A assembles a slightly modified version of Funlove.4099 on-the-fly. It accomplishes this feat by placing the code to reconstruct Funlove.4099, byte by byte, into the file WINxxxx.TMP in the Windows system directory and subsequently executing it.

Two instances of the string '~Fun Loving Criminal~' have been replaced by the strings '~AAVER 2002 in Seoul~' and '~AAVAR 2002 in Seoul~'. Similarly, the filename FLCSS.EXE within Funlove.4099's code has been replaced with 'AAVAR.PIF'. Aside from these text changes, however, the dropped virus is identical to Funlove.4099.

Bad Taste

Winevar.A carries several payloads, which range from dipslaying a message box, to wreaking havoc on the infected system.

Almost always, depending on the current system's elapsed milliseconds (GetTickCount API) and commandline parameters, the worm displays the following message box:

The worm sets up two timers, the first triggers every 2.048 seconds, and the other every 1.024 seconds. Both timers continuously poll the currently loaded processes and services, and terminate selected processes/services based on certain rules.

When the following strings exist in the window name or class name of a process or in the name of a service, they are terminated immediately:

view	fir
debu	prot
scan	secu
mon	dbg
vir	avk
iom	pcc
ice	spy
anti	

On the other hand, if they contain any of the following strings, they are ignored:

microsoft	smtpsvc
ms	moniker
_np	office
r n	program
cicer	explorewclass
irmon	

The worm also sets up a timer which downloads the default web page of http://www.symantec.com/ every millisecond if the infected computer has an Internet connection. If the worm infects enough hosts on the Internet, this could cause a DDoS (Distributed Denial of Service) attack on the website.

As its destructive payload, the worm tries to delete folders and their contents on all fixed drives, if they contain the following strings:

antivirus

cillin

nlab

vacc

Unfortunately, due to a programming flaw, the worm proceeds to delete *all* files on all fixed drives, leaving behind read-only files, as well as locked files. This makes the cleaning of Winevar.A-infected systems difficult, if not impossible, if no backups have been made prior to infection.

The Exploits … Again

Like countless other worms jumping on the bandwagon, Winevar.A includes two *Internet Explorer* vulnerabilities:

MS00-075 – 'Microsoft VM ActiveX Component' vulnerability.

MS01-020 – 'Incorrect MIME Header Can Cause IE to Execute E-mail Attachment' vulnerability, also known as the Internet Explorer I-Frame exploit.

Unpatched *Internet Explorer 4.x* and *5.x* browsers are vulnerable to the MS VM ActiveX exploit, while unpatched *Internet Explorer 5.01* and *5.5* browsers are vulnerable to the I-Frame exploit. Both exploits will be executed automatically with the use of *IE*-rendered email clients such as *Outlook Express*.

Is it a Braid …?

A sense of déjà vu was encountered while analysing Winevar.A, simply because Braid.A seems to be this worm's older brother. Although the worms differ in terms of their code (Winevar.A was written in VC++6, while Braid.A was written in VB6), the packaging and contents remain similar.

One of the major similarities between Braid.A and Winevar.A is the fact that both worms drop a slightly modified version of Funlove.4099 – making up for Funlove's inability to propagate through email.

Other similarities include the use of system information such as the RegisteredOwner and RegisteredOrganization in the email fields, and the fact that the *Internet Explorer* I-Frame exploit was used by both worms, providing automatic infection for vulnerable systems.

Another interesting point of trivia can be seen by inspecting the file properties of the executables of these two worms. Braid.A shows the company name 'Trend Microsoft Inc.', which is the name Winevar.A uses as the default RegisteredOrganization information, although in Winevar's case it is slightly misspelled as 'Trand Microsoft Inc.'. Winevar.A's file properties show a digital signature, apparently belonging to a company named 'Symantec Microsoft Corp'.

The similarities seem to suggest that these worms came from the same author, but it is quite possible that we are reading too much into the similarities between the two worms.

Conclusion

It seems that old exploits, specifically *Internet Explorer* exploits, are still proving tempting for worm writers because they are so highly effective.

No dazzling new techniques were used for the construction of this worm, but still it did the rounds on the Internet during its 15 minutes of fame – proving either that email recipients still open unknown attachments or that they are still unpatched to common system vulnerabilities (or both).

This time, those tasked with cleaning up the mess could have a very long day ahead of them.

W32/Winevar.A

Aliases:	I-Worm.Winevar, W32/Korvar, W32/Winevar@mm, W32.HLLW.Winevar.
Payload:	Deletes files.
Removal:	Restore deleted files from backup. Delete dropped files and remove registry entries.
Patches:	http://www.microsoft.com/technet/security/bulletin/MS00-075.asp and http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.

FEATURE

XML Heaven

Gabor Szappanos
VirusBuster, Hungary

Office 11 (the official name of the new product is unknown at the time of writing this article) is at the gates and, as usual, anti-virus experts are eager to see the new features and enhancements built into it. They will be expecting *Microsoft* to have introduced new file formats into the *Office* product line, and they will not be disappointed. *Office 11* will include a new format – XML. (The *Office 97*/*2000* HTML page format was a true HTML file, which contained an XML tag, but the resulting page did not conform with the XML specification; *Office XP* uses standard-compliant XML format.)

Something Old, Something New

The first surprise in this product comes at installation, as the new *Office* version requires either *Windows 2000* with Service Pack 3 or *Windows XP*, giving up on the older OS lines entirely. As far as macro virus protection is concerned, all the good old tricks used in *Office XP* are present, and there are no obvious additions (except that the AV API will be supported in *Project*, *Publisher* and *Access*). There are some new features though, the most significant of which is the introduction of the XML document format. Although it is not yet the default file format, *Microsoft* emphasizes its importance.

Will it do us any good? Will the new file format, as intended, ease the workload of anti-virus scan engines? In the past virtually all anti-virus companies had to reverse-engineer the dreaded OLE2 file formats and invent their own OLE2 engines in order to handle document macro viruses properly. It should be much easier with a basically textual representation, like XML – shouldn't it?

Without going into unnecessary detail, the binary macro block is stored within a binData tag within a docSuppData tag. The binary block is BASE64 encoded data, which is a zlib compressed OLE2 macro storage, generated by the VBA engine. So, instead of the old OLE2 storage, we have four layers of coding (XML – BASE64 – zlib – OLE2), which is not speed-optimized, to say the least.

The default name of the binary data block is editdata.mso, and *Office* will always generate this. But this filename should not be relied upon alone. Although it will not create such a file by itself, *Word* will happily open and run macros if the name of the binary block is changed. The default is still the old OLE2 document format, but once an XML document becomes infected, the virus is stored seamlessly in the textual representation. One important question is where can the binary data be placed within an XML document? Normally *Word* places the macro storage after the styles collection and before the document body. However, this does not mean that it will handle macros only if they are stored there.

A quick investigation reveals that the macro storage can be anywhere inside the WordDocument root XML storage. While *Word* itself will not save the macros in any place other than its specific macro storage location, a virus could easily do so. We cannot expect viruses to be polite enough to follow *Microsoft*'s storage location conventions. So it is best to assume that the macro storage can be anywhere within an *Office* document.

At least this mess is uniform across the *Office* suite. Well, almost. *Word* can store macros in XML files, while *Excel* can't. The only option *Excel* provides is to save the document in web page format, which will be familiar from *Office 2000*. In this case the macros storage is placed in a separate file in a separate directory – at least we don't have to scan the entire HTML file to find it. *PowerPoint* is another story; it provides the web page file format, which is the same as in *Excel*, but in addition it introduces the single file web page format, which is a multi-part MIME file, with one of the parts being the BASE64-encoded zlib compressed OLE2 storage. *Access* maintains its own Jet database format, with no XML support. Did I say uniform storage across the *Office* product line? The usual mess, I should say.

Possible New Threats

To date it has been very difficult to implant a macro virus into an *Office* application without the active participation of *Office* itself. Even VBScripts that infected *Word* documents relied on the ActiveX server capabilities of *Word*, and were not viable if at least *Word 97* was not installed. It was almost impossible for binary malware to handle the OLE2-WordDocument storage format sandwich properly, and only a couple of viruses attempted this (Anarchy, HZDS). Use of a textual representation makes it a lot easier to insert macrocode into an ordinary document. A binary dropper can carry a copy of an infected macro storage, and insert it into an appropriate location within a *Word* document. As mentioned, *Office* is very generous about what constitutes an appropriate location; therefore the XML parser of the virus does not have to be sophisticated at all. This could happen on pretty much any platform, including Unix, *Linux* and others, on which active macro infection has not been possible until now.

This threat is not just theoretical; similar proof-of-concept viruses have appeared that infected another textual document representation – RTF files. VBS/RTFnfo (aka Infort) existed as an embedded shell scrap object within an RTF

file. Whenever a user double-clicked on the embedded object, the VBScript executed, found the RTF file it was running from (as an indicator it used the {\object\objemb} and {*\objclass Package} strings), then extracted the embedded object from the source, and injected it into all .RTF files. A very similar infection method would be quite easy for viruses attacking XML documents.

Conclusions

So, if we can't get rid of our home-brew OLE2 engines, what can we get rid of? Performance. Many companies in the anti-virus industry have invested a lot of time and effort in the development of streamlined OLE2 engines that read only the macro-related blocks in an *Office* document. This means that only minor parts of a large document have to be processed by the scanning engine, making the process significantly faster than if the whole document were processed. With XML documents, however, the scanning engine has to parse the entire XML storage, read macro-unrelated segments, and parse it for the binary macro block.

Our users will not be happy with the resulting drop in performance. The usual 'blame it on Redmond' excuse is no longer acceptable, and there is no good solution – other than waiting and hoping that all macro viruses die out before *Office 11* ships. I wouldn't bet a penny on it.

Solution

Is there a good solution? I think so. At this point, *Microsoft* could stick to the second commandment of virus-safe office applications: 'Thou shall not save macros and documents in the same file' (the first commandment, 'Thou shall not provide access to the VBA object model' has already been addressed in *Office XP* – well, sort of).

The web page save format introduced in *Office 2000* stored the macros in separate editdata.mso files. While the storage of embedded pictures and objects in the same XML file makes sense from the point of view of portability, nothing supports the storage of macros in the same file (why store a platform-dependent macro storage in a platform-independent file format?). Additionally, the ThisDocument object, representing the active document, should refer only to the XML file and not the additional macro storage, which may cause application developers minor problems.

Standalone *Office* utility developers are unlikely to release their products as XML files (it makes no sense to store the solution in a less effective format), and even if they did so, it is easy for them to package the macro file with the XML document file. Otherwise, it is only viruses that insert macros into documents. If the macros – and only the macros – were stored outside the XML files, the majority of users would not notice any problems, while viruses would be unable to spread easily. There would also be a performance increase in virus scanners, since it would be necessary to scan only the tiny macro storage. Does it make sense to you? [*Send* your *opinions to comments@virusbtn.com.*]

PRODUCT REVIEW

ViraLock 3.2.2.4

Nick FitzGerald
Computer Virus Consulting Ltd, New Zealand

ViraLock is not a traditional anti-virus product. It does not scan for known viruses, nor does it employ cunning emulation, sandboxing, behavioural or heuristic analysis of programs run on the 'protected' computer. The product's developers, or at least their marketeers, make many enticing claims for *ViraLock* such as 'zero escape for email viruses', 'complete the circle of protection', 'the first software that prevents the spread of email-borne viruses, allowing them no escape from an infected computer', and so on.

So, What's the 'Big Idea'?

ViraLock is touted as a 'breakthrough in anti-virus technology'. Revolutionary products are, of course, based on some big, new idea. What is *ViraLock*'s? In short, it encrypts email addresses in the *Windows* and *Outlook* address books (Contacts folders, etc.) and in email messages stored in *Outlook* and *Outlook Express* (*OE*) message folders. Thus, users of *Outlook* and *OE* are protected from having those email addresses found and used as target addresses by a virus that may break through their other defences.

During installation, *ViraLock* encrypts the addresses in existing messages and address book entries. However, entries added to address books and messages arriving after *ViraLock's* installation would be sources of potential target addresses. To thwart this, *ViraLock* runs POP3 and SMTP proxies, altering the mail entering or leaving via them. For this to work, the relevant *Outlook* and *OE* accounts are modified so they pass their email to, and source it from, these proxies. Finally, as the content of the user's *Outlook* and *OE* email folders and address books have been encrypted, there are tools for managing these, including tools for decrypting them should it be necessary.

As preventing viruses from arriving at the desktop mailbox is commonly seen as a high priority, *ViraLock* is not a product to use instead of a more traditional approach. To their credit, and despite some rather grand claims such as those above, the developers often describe *ViraLock* as an additional layer of protection, which is not to be seen as a replacement for other layers and technological approaches but as '[c]omplementary to current anti-virus software products'.

However, claims such as '*ViraLock* prevents all viruses, known or unknown, from using email addresses to spread by exiting to other computers' seem far-fetched if all the product does is encrypt email addresses held in the WAB and in messages stored in *Outlook* and *OE* mail folders and munge email traffic proxied from those applications to the

actual POP3 and SMTP servers they would normally talk to. Is *ViraLock* US$19.95-worth of extra protection?

To answer this question, *VB's* usual scanner-testing methodology was clearly not appropriate. As *ViraLock* does not use a scanning-based method, testing it would require a less straightforward approach than pushing a bunch of virus samples past it to see what was detected.

As *ViraLock* is claimed to prevent all emailing viruses from getting out, one obvious test would be to see whether some known viruses have self-mailing functionality that sidesteps the product. If any known viruses did seem to possess such features, and in testing beat the product, then some limits on its usefulness would be established.

But First, Installation and Use …

ViraLock is aimed primarily at the small business and home user market. Thus it was not surprising to find that the main form of distribution is via online purchase, followed by downloading a full product installer whose registration is activated by a key provided during the purchase process. The download is currently approximately 2.3 MB, which is not terribly onerous, even on a 33 kbs modem link. Evaluation keys may be obtained should one prefer to download and trial the product for 30 days.

ViraLock is claimed to work on *Windows 98, Me, NT 4.0 SP6, 2000* and *XP*, and with client software *Outlook 97, OE 5.0* and all later versions of both. When the installer – a typical *InstallShield* affair – is started, it displays a splash screen followed by a 'readme' about the product's main features and basic installation requirements. After accepting the licence agreement, the file copying begins and a registration key is required. Next a password is requested to 'protect' access to the *ViraLock* GUI – which, among other things, can undo all the encryption that is about to ensue.

Finally, various *Outlook* and/or *OE* email folders and address books are located, their contents parsed for email addresses, which are encrypted, and the *ViraLock* GUI minimizes to an icon in the system tray. Under a standard installation of *Windows XP* and early in the process just described, an Internet connection will be sought if the machine is not already online and the Microsoft Virtual Machine (aka 'MS Java') installer will be downloaded and installed before the main part of the *ViraLock* installation proceeds (users are well-informed of this in advance – at least, they are if they have read all the installation requirements material provided).

Installing the product was straightforward, although some difficulties were encountered under *Windows 98*. Initially it was suspected that this may have been due to issues with using the 'basic' (initial) release of *Windows 98* on the test machine, as some problems with that OS are alluded to in the support section of the product's website. Also, some confusion was noted between different pages on the website and the information provided in the product as to whether *IE 5.0* or *5.5* was the minimum required version. The test machine had been prepared with *IE 5.0*, as per the minimum specifications provided under the obvious link on the web page.

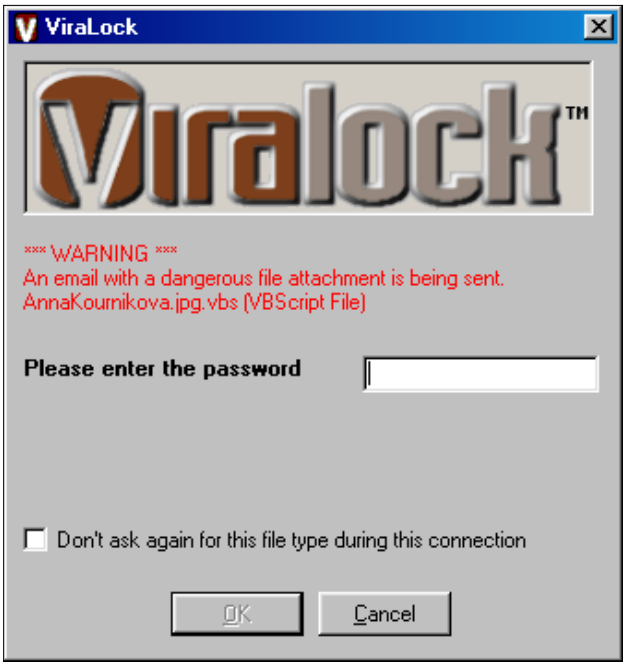
To check the *Windows 98* version, the test machine was scrapped and restored from a different image backup. However, with *Windows 98 Second Edition* and *IE 5.5* the same problems appeared. *ViraLock* itself seemed to have been installed properly, but it was not modifying the email account information correctly for either *Outlook* or *OE* on the test machine. Reconfiguring these settings manually, as per the changes seen when the product was installed on other OSs, resolved that problem. However, this measure seems likely to be beyond the 'obvious' for the product's main target market.

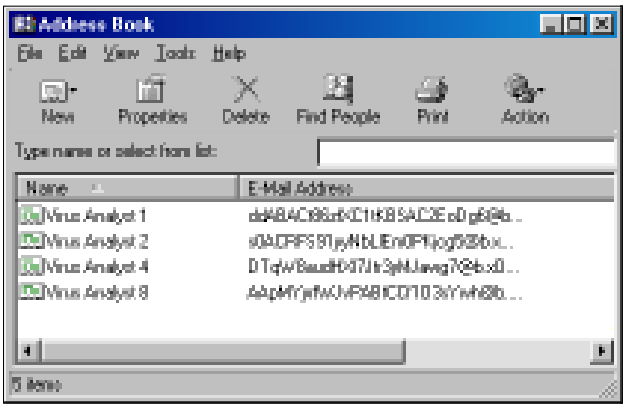
An Ounce of Prevention

ViraLock does encrypt the email address part of standard *Outlook* and *OE* address book entries. Simple mass-mailers that depend just on *Outlook* or the Windows Address Book (WAB) as sources of their addresses will be foiled by this feature of the product.

However, it struck the reviewer that such viruses depend mainly on *Outlook* or MAPI for sending their messages as well. *ViraLock* aids in the protection of these interfaces by monitoring the messages sent through them (recall *ViraLock* acts as a proxy for incoming and outgoing POP3 and SMTP to *Outlook* and/or *OE*). Thus messages sent by LoveLetter.A or VBSWG.J cause *ViraLock* to display dialog boxes (one for each outgoing email message) warning that a message with a 'dangerous attachment' is being sent.

In fact, *ViraLock's* POP3 and SMTP proxies can easily be used by other email clients. The proxies basically parse the





datastreams they are proxying, checking for what seem to be email addresses. They decrypt outgoing encrypted addresses and encrypt incoming addresses. (There are some exceptions – for example, addresses inside attachments are not encrypted.) This is demonstrated easily with any POP3 and SMTP mail client that *ViraLock* does not support (in this instance *Pegasus Mail* and some simple command line utilities were used).

So, what happens if a virus trawls the WAB for addresses, then emails itself to all of them via the default SMTP server found in the Registry? The latter are, of course, altered by *ViraLock* (or perhaps not on *Windows 98* machines!) to point to the proxies *ViraLock* establishes on the localhost (or 'loopback') address. Thus, wouldn't such a virus still be sent out via the *ViraLock* SMTP proxy?

No. First, there is the question of which addresses it found. Depending on how addresses are harvested, it may find none or just the encrypted forms. As *ViraLock* retains an '@' symbol in its encrypted addresses (as can be seen from the screen shot of the WAB above) a process that simply extracts strings that contain an '@' character may well extract the encrypted addresses. However, if the virus then sends copies of itself via the SMTP proxy, *ViraLock* will alert the user of the attempt to send messages with attachments. Thus, the fact that *ViraLock* would otherwise then have decrypted the addresses should not be an issue here. However, if a new exploit is discovered that tricks an email client into 'seeing' an attachment where the *ViraLock* parser sees none, there would be a problem.

But what about the increasingly popular techniques of trawling much more widely for email addresses and, using the virus's own SMTP engine, sending directly through open SMTP relays, directly to the target domains' SMTP servers as located from MX records in the DNS, or via other possible SMTP servers? Obviously, *ViraLock* cannot help there. For example, Klez.H will 'guess' the SMTP server to use by prepending 'smtp.' to the domain of the address it uses in the 'From:' header (see *VB*, July 2002, p.9). This completely side-steps *ViraLock*. Klez.H – the most common of viruses for the last half-year or more – happily ran on, and spewed huge numbers of Klez-carrying emails from, the test machines that were supposedly 'protected' by *ViraLock*.

One Swallow Does Not a Summer Make

As this review proceeded, the product's home page claimed the following: '*ViraLock* prevents the spread of email viruses and worms like Klez, Sircam, Magistr, Nimda and others. Unlike traditional anti-virus software like *Norton AntiVirus* and *McAfee VirusScan*, which blocks known viruses from coming in, *ViraLock* makes certain that all viruses, known or unknown, are unable to get out.'

Oddly, one of the viruses named in that blurb – Klez – was the first one found to circumvent *ViraLock's* 'protection'. Expert opinion is that the approach used by Klez is likely to become more common, and we have certainly seen other virus families adopting some or all of the Klez email tricks. A new move, to MX-resolving self-mailers that send directly to the target's primary mail handler, may also be starting. Some of the Yaha variants, and a few other recent viruses are doing this, and it is another approach that will also completely bypass *ViraLock*.

The product's address encryption and detection of the sending of undesirable attachments work. However, several usability issues, such as having to remember to decrypt email and address books before synchronising your PDA or handheld, and the spectacular failure against such a common virus as Klez, have to raise questions as to the value of the product.

The likely adoption by future viruses of Klez-like SMTP techniques, and others that entirely bypass *ViraLock's* 'protections', will likely render the product moot. A letter received from *SentryBay* during the course of this review acknowledged that the company is aware of these issues and further emphasized the complementary and partial nature of the protection *ViraLock* offers. Given this, one questions the number and prominence of the claims made both on the website and in the product's promotional materials, for *ViraLock's* total prevention of email replication of all viruses.

Technical Details:

Product tested: *ViraLock version 3.2.2.4* (Full version).

Test environment: All tests were performed on a 400 MHz Celeron with 512 MB RAM, 4 GB hard drive, 80 GB removable hard drive from which image backups of the OSs were installed, CD-ROM, 3.5-inch floppy and a TCP/IP Ethernet LAN connection. Windows 98, 98SE, ME & XP Professional were successively installed and tested with several of the supported client products.

Client software used: *Outlook 98, 2000 & XP, OE 5.0, 5.5, 6.0* configured to use a POP3 and SMTP server on the local (Internet-isolated) LAN.

Price: US$19.95 for a single user licence, dropping to US$14.95 per seat for 501 or larger licences. Academic and larger licence pricing is available from the distributor. Each licence includes one year's product updates and online support. Annual licence renewals are US$9.95.

Developer: *SentryBay Corporation*, 117-125 St. Georges Bay Road, Auckland, New Zealand, tel +64 9 3092491; email sales@viralock.com; website http://www.viralock.com/.

RESEARCH PROJECT

Malformed Email Project – Part 2

Andreas Marx, Mark Ackermans

Early in 2002 we embarked on a 'malformed email research project'. The details of how and why the project was started, along with our goals, were discussed in the first part of this series of articles (see *VB* November 2002, p.12). Here, we reveal the companies that were notified and the ways in which they responded. In many cases we have included details as to which versions of a product should be safe against 'malformed emails' according to *the manufacturers'* own tests. The results of our tests (carried out at *AV-Test.org*) will be published later this year.

In early April 2002, companies were informed of the project by email; a test set of malformed emails (version 1.02) was sent to all those who requested it, and the deadline we gave the companies for sending fixed products to us for testing was 6 June 2002 – however, following a large number of requests, this was extended to 22 July 2002. Since its original incarnation, the test set has been updated to reflect techniques seen in new viruses and other forms of malicious code, including W32/Junkmail (see *VB*, November 2002, p.10), W32/Yaha.K and W32/Sobig.A. Updated versions of the test set were sent to participants in May, September and November 2002, and the latest test set (version 1.07) was released in January 2003.

Aladdin, eSafe: *Aladdin* replied to our email within hours. In July 2002 *Aladdin* told us that *eSafe* detects malformed mails as 'unopenable', but the option to block them is disabled by default. We were told that they intended to rewrite their SMTP handling module to improve the handling of malformed mails. We have received no update.

Alwil Software, Avast!: *Alwil Software* responded to our initial email more than two months after it was sent. After sending *Alwil* the test set, we received no further communication from the company.

AMaViS – A Mail Virus Scanner: The *AMaViS* programmers responded to our email almost immediately. They informed us that their software relies on Perl's MIME-tools and that this library needed to be fixed. We shared our test set with the core *AMaViS* development team and, at their suggestion, informed the author of the MIME-tools library and the developer of the Convert-UUlib. The MIME-tools author responded quickly, saying that he knew about the bug and was working on the problem. We received only an auto-generated email from the author of Convert-UUlib.

At the request of the *AMaViS* developers we also notified the author of rip-MIME and Xamime. Updates were available about two months later. In addition we notified the author of qmail-scanner – changes are scheduled to be included in qmail-scanner version 2.0 – and contacted the author of MIMEDefang, who said that he would check the software using a third-party virus scanner engine. However, we received no further information. In August 2002 the authors of *AMaViS* warned in a security bulletin that *AMaViS 0.2.1* would not detect W32/Klez if rip-MIME is used. Their advice was 'upgrade to amavis-perl/amavisd, or fix the rip-MIME call'.

Astaro, Astaro Security: We received a response from *Astaro* within 24 hours. In June 2002 we received a new version of *Astaro Security* software for testing. *Firewall Astaro Security Linux version 3.214* is considered by its developers to provide sufficient protection against malformed emails.

Beginfinite, GWAVA for GroupWise: The *Beginfinite* developers replied to our email within 24 hours, stating: 'Our product actually gets the native attachments from the *GW* API (as opposed to relying on MIME decoding). Therefore we are hopefully "relatively" immune.' In July 2002 we were informed that the test messages caused a few abends, and that these had been reported to *Novell*. The product offers the raw message, the decoded body text and the decoded attachments to a virus scanner to be checked. According to the developer, adding an extra layer of decoding would 'slow down' the mail server 'enormously'. We received no further information about *GWAVA*.

BorderWare, Mail Gateway/MXtreme Firewall: *BorderWare*'s response came within 24 hours. They said that only about 10 per cent of the malformed mail samples were not blocked, according to their own tests. At the beginning of June 2002 *BorderWare Technologies* claimed that *Mail Gateway version 1.3* had passed all of the tests in the malformed email test set. In October 2002 *BorderWare* sponsored a *SecurityFocus* newsletter which included a link to a *BorderWare* web page, on which the claim was made that *MXtreme* 'detects and blocks 100% of invalid messages per University of Magdeburg test suite.' Furthermore, detailed information about the content of the test set was available on the *MXtreme* website – constituting a violation of our non-disclosure agreement. *BorderWare* was removed from the test set distribution list immediately.

Cat Computer Systems, Quick Heal: No reply was received to our original email until some five months later when *Cat*'s lead programmer found out about the project. Five days later, the developers sent us the first fixes for their products, with a detection rate 'up to 80%' of all malformed mails. In September 2002 we received *Quick Heal 6.07 SR* with fixes that should be able to detect all kinds of malformed files.

Clearswift, MAILsweeper: We received a reply from *Clearswift* within a few minutes. In July 2002 we received *MAILsweeper version 4.3_1 RC1* for testing. It should be noted that version 4.2, including all updates, is vulnerable to some malformed email attacks – for example, W32/Yaha.K cannot be found by this version if the AV engine is not scanning the whole EML file. All customers should upgrade to version 4.3 as soon as possible.

Command Software, Command AV: *Command Software* replied to our email within minutes. They told us that most of the messages in the test set were not MIME RFC-compliant. In fact, most MIME messages in our test set contained the error that the 'MIME-Version' header was missing, which caused additional problems for a number of programs. The developers told us that it would be almost impossible for them to fix the issues and certainly not within two months. In late July *Command Software* told us that they were still having problems with a German *Exchange* version and they were unable to send us a fixed version.

Computer Associates, InoculateIT/eTrust AV: *Computer Associates* replied to our message within a few hours. In July 2002 a patch, 'qo21090', for *eTrust AV 6.0* (*Windows* version only) was made available at the *CA* ftp server, but the patch was not mentioned anywhere on the public website. We understand that, following more QA, similar patches should be available for the *Linux* and *Solaris* platforms and that the patches, together with a number of other changes and new features will be included in *eTrust AV 6.1*, due to be released in mid-February 2003.

Computerized Horizons, Declude Virus: *Computerized Horizons* replied to our email within a few hours. In November 2002 the developers informed us that *Declude Virus* (*v1.63*) covers the most recent test sets of malformed messages.

DataEnter, XWall: *DataEnter* replied within a few minutes and, in May 2002, we received a download link of the current fixed *XWall* version for testing.

Finjan, SurfinGate: We received a reply from *Finjan* within 24 hours. *Finjan* explained that they could not fix their product, because it uses the *NAI/McAfee* engine which needed to be updated. In July 2002 we received *SurfinGate version 6.01* (without an updated engine) for testing. Version 4.2.40 of the *NAI*/*McAfee* virus scan engine is due to be released in late February 2003, when the current *SurfinGate version 7.0* should be updated accordingly.

Fortinet, FortiGate: *Fortinet* responded to our email within a few minutes. In July 2002 *FortiGate 300 Network Protection Gateway* was shipped to us for testing (this release included a beta version of the malformed email protection). A month later we received the final release, which is now available to all customers.

F-Secure, F-Secure Anti-Virus: Developers at *F-Secure* responded to our email within a few minutes, telling us that they were aware of malformed mails and they had made several fixes and hotfixes available to their customers to block such attachments. According to the developers, the fixes were first introduced in *F-Secure AV for Firewalls 6.10* (beta) and *F-Secure AV for Exchange 6.00* (beta). In July 2002 we were informed that *F-Secure AV for Exchange 6.0* (final version), *F-Secure AV for Firewalls 6.10* (final version), *Internet Mail 6.00* (final version with Hotfix 5) and all the Content Scanner Server modules included in these versions were fixed (the *Lotus Notes* AV solution has been discontinued and will not be updated).

G DATA, AntiVirenKit for SMTP Gateways: *G DATA* replied to our email six days after receiving it, and a fixed beta product was submitted for testing in July 2002 – the final version was released in January 2003.

GeCAD Software, RAV AntiVirus: We received a response within 24 hours from *GeCAD*, and we were told in July 2002 that we should test any of the *RAV* products after updating to the latest engine update.

GFI, MailSecurity/MailEssentials: *GFI* replied to our email within a few minutes. The developers said: 'We noticed that the email files which managed to bypass our products are so malformed that they tend to be harmless' (no email program was able to find an attachment) and declared that the program releases available at the time (May 2002) should, therefore, be safe.

Gordano, Messaging Suite: *Gordano* replied five days after our email was sent, informing us that they were already working on some malformed mail issues caused by ItW viruses and that an update was planned for release the following week. In May we were told that the most recent public release of *Messaging Suite* (3037) should protect against malformed mails in our test set.

Grisoft, AVG: *Grisoft* took two weeks to respond to our original email. By July 2002 the developers claimed that all problems besides one (a problem with file extensions) should be fixed with beta version 6.0.379 pre-release of the personal email scanner and *AVG 6.0.377*.

Group Technologies, iQ Suite: *Group Technologies* replied within 48 hours. In July 2002 they informed us that the problems were fixed in version 5.2c of the *Lotus Notes* product (at this time, a release candidate); the first release of the *iQ Suite for Exchange 2000* (planned for Q1/2003) should include all the necessary fixes.

H+BEDV Datentechnik, AntiVir Mailgate: *H+BEDV* replied within 48 hours and within five days told us that a new version that could decode all of the malformed messages was ready. In May 2002 version 2.0.0.4 was released, which fixed most of the issues and in July a further update – version 2.0.0.9 – was released. According to *H+BEDV*, this and all later versions should be safe.

IBM, Lotus Notes/Domino: We received the following email from *Lotus*: 'We would like to work with you to

address any issues you have discovered with our products … To date, we have not found *Notes* to be vulnerable to these recently reported types of MIME issues.' We did not hear back from them.

Ikarus Software, Virus Utilities: *Ikarus* replied to our email within 48 hours. In July 2002 We received fixed versions of *Ikarus MailWall/ContentWall* and their *Checkpoint FW-1* appliance '*SecureGuard*', developed by OSST.

Indefense, MailDefense: We received a response to our email from *Indefense* within 24 hours. In July *MailDefense 1.02.10* was submitted for our testing.

Kaspersky Labs, Kaspersky AntiVirus: *Kaspersky Labs* replied to our email within a few minutes. The developers investigating the test set identified some additional problems with the malformed mails in our test set – and another in their email gateway scanner, which was scanning our password-protected test set archive for some 25 hours. Despite some very interesting discussions about all kinds of malformed mail problems, we did not receive fixed versions of *Kaspersky* products for testing.

Marshal Software, MailMarshal: We received a reply to our email within 24 hours. In July 2002 we received *MailMarshal Build 5.0.3.54* for testing, together with some documentation of tests *Marshall Software* has performed with our test set.

MessageLabs, SkyScan AV: *MessageLabs* responded to our email within a few minutes, stating that additional checks would be implemented in their systems with immediate effect, to improve their existing malformed mail checker.

Microsoft, Exchange Server/ISA Server: We contacted *Microsoft* because we thought it could be useful for their developers to investigate these malformed email issues. For example, they could improve their Mail Server APIs to improve detection of malformed mails or they could limit their MIME parser in future product releases so it would no longer be able to catch all of these badly malformed attachments and reassemble them (which would make their products significantly more RFC-compliant). In June 2002 we received the following comment from *Microsoft*: 'If our MIME parser is used it's very robust and essentially can handle wide ranges of commonly found malformed MIME. *Outlook* and *Outlook Express* have very similar MIME parsing capabilities.' (Which is exactly the problem!)

MicroWorld Technologies, eScan/MailScan: *MicroWorld Technologies* replied to our email after a week. In May 2002 the company informed us, 'We have completed all vulnerability tests with 100% detection rates. The updated binaries of *MailScan* will be released as part of Service Pack 4.'

Mirapoint, Secure Messaging: *Mirapoint* replied to our email within 48 hours. *Mirapoint* requested that some of the undetected messages be sent to *Sophos*, as they believed it was the *Sophos* scanning engine that needed to be changed. We did not receive an appliance for testing.

MKS, MKS_VIR: *MKS* responded to our email within 48 hours. According to *MKS*, all products released after 12 July 2002 are 'known' to be safe.

Network Associates, VirusScan/GroupShield/NetShield: We received a response from *NAI* within a few minutes. In July 2002 we received the following versions for our tests: *GroupShield for Domino 5.0a Hotfix 7, WebShield for Windows NT SMTP Version MR1a HotFix 6, WebShield for Solaris 4.1 HotFix 3.* In addition, the following patches for appliances were available: e50: HotFix 3, e250/e500 (versions 2.1/2.0): Hotfix 11a, e250/e500 (version 2.5): Hotfix 2a. The *Exchange 5.5/2000* requires at least engine version 4.1.70 (beta) to fix the malformed mail issues. A public beta version of the new engine (labelled 4.1.80) was released in December 2002. The final version 4.2.40 should be available at the end of February 2003.

Norman, Virus Control: *Norman*'s developers responded to our email within a few minutes. In July 2002 we received fixes for the *Exchange 2000*, *Lotus Notes*, *Mimesweeper* and *Checkpoint FW-1* versions.

Open Access, MailGate: *Open Access* replied within 24 hours. In July 2002 we received *MailGate 3.5.174* beta for testing.

Panda Software, Panda AV: We received a response from *Panda Software* within a few minutes. In June 2002 we received updated products for *Postfix* (version 0.3) and *QMail* (version 1.01). In July 2002 we received updates for the *Exchange* and *Lotus Notes* products (version 2.51.81 of *Panda Administrator*).

Postini, Postini: Like *MessageLabs*, *Postini* is an email security service provider that does not ship any product to end users. *Postini* replied to our email within 24 hours, telling us that they had made enhancements to their scanner to identify and scan malformed mails, because the AV protection they were relying on (*McAfee*) didn't do so properly. Following the changes, all mails are extracted by *Postini* mail decoder and the AV engine gets only the extracted files for scanning.

Softwin, BitDefender: *Softwin*'s developers replied to our email within a few hours, telling us that they were working on a malformed email protection, to be included in the 7.0 engine, and that a fixed version should be available in less than a month. However, we have received no update.

Sonicwall, SonicWALL: *Sonicwall*'s response to our email arrived within eight days. The company stated: 'Our current product is a standard firewall/VPN concentrator. We have added some capabilities of filtering email attachments, but they are only based on filenames. We are developing additional security products that will scan emails for viruses, worms and other intrusions, but those products are still in development. We will be using your test suite to

validate our development.' We have received no further communication. However, the website shows that they offer a virus-scanning product called *SonicWALL Complete Anti-Virus* with *SonicWALL Network Anti-Virus.*

Sophos, MailMonitor: The developers at *Sophos* replied to our email within a few minutes. In July 2002 *MailMonitor for Lotus Notes* (version 2.0.2 beta) and *Exchange 2000* (version 1.0.3) were released and, according to *Sophos*, these should address the malformed mail issues. Ten days later *MailMonitor for SMTP 1.2.0 Beta* for *Windows NT*-based platforms was released, and in October *MailMonitor 1.2.0* (final) was released. In August 2002 *MailMonitor for SMTP 1.2.0 Beta 2* on *Solaris* and *Linux* were available for download from the 'Beta products' section of the *Sophos* website. *MailMonitor for Linux 1.2.1* (final) was released in December 2002.

Stalker, CommuniGate Pro: *Stalker* replied within a few minutes, saying 'Our company manufactures hi-end mail servers … To scan messages, we use plug-in modules that are developed by anti-virus vendors. Currently, we officially support and resell the *McAfee* Plug-in for *CommuniGate Pro*, though there are other plug-ins.' They asked to receive the test set for future enhancements, for example, to block malformed mails completely. In July 2002 we received a version for testing with the comment that detection is dependent on the plug-in provided by *McAfee*.

SurfControl, SurfControl E-mail Filter: *SurfControl* replied to our email five days after it was sent. In July 2002 version 4.0.52e was submitted for our tests.

Sybari, Antigen: We received a reply from *Sybari* three weeks after our email was sent. In July 2002 we were informed that *Sybari* was unable to give us a new version of *Antigen* since the development team was working on a new release which would include new features as well as an improvement in the scanning of malformed emails. A public beta was scheduled to be ready in October 2002. There was no further communication.

Symantec, Norton AV/Symantec AV: *Symantec*'s developers replied to our email within a few hours. In July we received a CD, but this included only the most current SMTP scanner version. In August we received a second CD, this time with all the products we needed for our tests.

Symantec provided the following information about the status of its products: *NAV for Lotus Notes 2.5.1* (*Linux*, *Solaris*, *Windows NT*/*2000*, *AIX*, *AS400* and *iSeries*): no known problems with malformed MIME/dependent on *Notes* decomposer; *SAV/F Exchange v3.03* (*Windows NT*/*2000*): no known problems with malformed MIME with latest update available from September 2002; *SAVSE 3.0* and above (*Windows NT*/*2000*, *Solaris* and *Linux*): no known problems with malformed MIME with latest update available from mid-2002; *SAV SMTP v3* and above (*Solaris* and *Windows NT*/*2000*): no known problems with malformed MIME with latest update available from December 2002; *SWS v2.5* and above (*Solaris* and *Windows NT*/*2000*): no known problems with malformed MIME with latest update available from October 2002.

Trend Micro, InterScan/ScanMail etc.: *Trend* responded to our email within minutes. We received updated *Windows*-based versions of the engine (version 6.350-1101) in August 2002. In September we received two CDs containing all *Trend*'s updated email security products. Engine version 6.510 was released to the public in December 2002 (this is a pre-condition to detect malformed mails with *Trend Micro* products; the new engine is also able to identify and block a few variants with older product releases). In January this year we received new beta builds of a number of products.

According to *Trend*, *ScanMail 6.1 for Exchange 2000* and *ScanMail 3.81 for Exchange 5.5* will be released in mid-March 2003 (for the last version, a special Registry key needed to be set to enable detection) and will include protection against malformed mails; a patch will be available for *ScanMail for Lotus Notes 2.6* to fix the issues; the next release (2.7) should include all changes and will be published in Q2/2003. All products of the *InterScan Messaging Security Suite* are affected by the malformed mail issues and a patch will be released in Q1/2003.

We received the following comment from *Trend Micro*: 'The amount of infections caused by malformed emails is currently low … when actual threats emerge, we have alternative technologies such as Outbreak Prevention Service (OPS), pattern updates, to address the threat.'

Vircom, VOP modusGate/modusMail: *Vircom* replied to our email three weeks after it was sent. Unfortunately, an oversight on our part led to the company being omitted from our mailing list, meaning that they did not receive the updated test set versions or revised deadlines. In October 2002 *Vircom* told us that only six files were still not detected according to our latest available test set and that publicly available updates would be released after finishing the final QA tests.

VirusBuster, VirusBuster: We received a response from *VirusBuster* within 24 hours. The first fixed version of *VirusBuster MailShield 1.10 for Linux* was publicly available in July 2002 and 20 days later version 1.10.02 was released.

WatchGuard Technologies, WatchGuard: *WatchGuard* replied within 24 hours but later declined to offer a *Firebox* appliance for testing, stating, 'It is not our policy to participate in this sort of review except under controlled conditions where our engineers are present to review the configuration of the *Firebox* and test environment.'

Webwasher, WebWasher: *Webwasher* responded three days after our email was sent. *WebWasher 4.1 Build 185* (Beta) was publicly available for *Windows*, *Linux* and *Solaris* in July 2002 and, according to the developers, this release should fix the issues.

ZoneLabs, ZoneAlarm: *ZoneLabs* responded to our email within minutes. In July 2002 we received fixed versions of *ZoneAlarm Freeware 3.1*, *ZoneAlarm Plus 3.1* and *ZoneAlarm Pro 3.1* (the older 2.x releases are no longer supported and will not be fixed).

Others

The following organisations contacted us after reading the introduction to the project in the November 2002 issue of *VB* and have been sent the test set:

- *eAcceleration, eAnthology*
- University of Southampton, *MailScanner*
- *Ositis, WinProxy/AVStripper*
- *eSoft, SoftPak*
- *Blackspider, BlackSpider AV*

The following companies were notified multiple times, but we have received no response to our mails:

- *Bluetail*
- *BVRP Software*
- *Checkpoint*
- *Computer Mail Services*
- *Critical Path*
- *Cyberguard*
- *Cybersoft*
- *Easylink*
- *Electricmail*
- *Elron Software*
- *Escon*
- *Eset*
- *GreenComputer*
- *Invisimail*
- *IP-Engine*
- *IPSwitch*
- *Lyris*
- *Merak Mail Server Software*
- *MultiTech*
- *Nemx*
- *Novell*
- *PPP-India*
- *Proland*
- *Sald*
- *Sendmail*
- *SSI-Mail*
- *TFS Technology*
- *Tumbleweed*
- *Webshuttle*

We hope these companies will get in contact with us (via the editor of *VB* – editor@virusbtn.com) as soon as possible.

Acknowledgements

We would like to thank the following people for their help, ideas and useful input to improve our reference collection (in no particular order): Alex Shipp (*MessageLabs*), Costin Raiu (*Kaspersky Labs*), Menashe Eliezer (*Finjan*), Peter Ferrie (*Symantec*), Pierre Laliberte (*Vircom*), Sanjay Katkar (*Cat Computer Systems*) and Scott Perry (*Declude*). We would also like to thank *GFI*, *Securiteam* and *Webwasher* for additional test set resources. The first results of our own tests, revealing how the products perform and whether their claims to be safe against malformed emails can be verified, will be released in April 2003.

COMPARATIVE REVIEW

Windows NT

Matt Ham

After the festivities of the new year it was straight back to work at *Virus Bulletin* for the production of a comparative review of epic proportions. This month 25 products for *Windows NT* were submitted for review.

With the December 2002 WildList delayed by the holiday season (only just released at the time of writing), the review was performed on an In the Wild test set based on the November 2002 WildList. The combination of an older operating system and a slightly dated WildList should be good news for the manufacturers – the odds of their products doing well under such circumstances are in their favour.

Products that were new to *VB*'s comparative line-up on this occasion were *AhnLab*'s *V3Net*, *MicroWorld*'s *eScan* and *New Technology Wave*'s *Virus Chaser*. Of these, *V3Net* is developed in-house by *AhnLab* and *Virus Chaser* is a rebadged version of *DialogueScience*'s *DrWeb* scanner. *eScan* is a rebadge of *GDATA*'s *AntiVirusKit* – which, in turn, is a blend of the *GeCAD* and *Kaspersky* engines behind a *GDATA* front end.

AhnLab V3Net for Windows Server SE SP2

ItW Overall	99.84%	Macro	97.58%
ItW Overall (o/a)	99.84%	Standard	80.05%
ItW File	99.83%	Polymorphic	45.58%

Initially there was some confusion over the version of *V3Net* that was to be tested. The first product version submitted was incapable of running on the *NT Workstation* version of *Windows* supplied. This was not surprising in itself, but the replacement version of *V3Net* (which did work on the same machine), was clearly labelled as being for servers.

Confusion aside, when extracting the detection data from the log files it became apparent that *V3Net* is very selective in its detection abilities – older DOS infecting samples were detected with significantly less success than newer or more prevalent viruses.

A little more concerning were a number of misses amongst the more recent polymorphics. A few samples were missed In the Wild, due to a problem that will be familiar to those who have read more than one or two comparative reviews. The files in question were the extensionless, POT- and PPT-extensioned samples of O97M/Tristate.C, while the other samples of this virus were detected without difficulty.

Alwil Avast32 3.0.519.1

ItW Overall	99.76%	Macro	99.56%
ItW Overall (o/a)	100.00%	Standard	98.39%
ItW File	99.75%	Polymorphic	91.21%

Avast32 maintained a fairly good detection record in this test. However, detection faltered among the polymorphics and a handful of files with odd extensions. Although extensionless files were detected, INI files and files with archived contents such as EML, ZIP and some viruses that utilise compression were missed.

Unfortunately, those that were missed included the DLL file installed as part of the infection routine of VBS/Redlof.A. This is not, in fact, a DLL file and is simply VBS code that has been renamed as a DLL file. However, Redlof alters Registry settings so as to render the file executable through the VBScript handlers and thus this file is both executable and dangerous on an infected machine. The fact that this file was missed was sufficient to deny *Avast32* a VB 100%.

CA eTrust Antivirus 6.0.101 23.59.12

ItW Overall	100.00%	Macro	99.90%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

eTrust Antivirus performed much as expected in this test – on demand, only W97M/Box.F files were missed. On access a few more files were missed – the packaged W32/Heidi.A in the standard set was quite predictable and this went undetected by many products throughout the test.

W32/Heidi.A inserts itself into ZIP archives, thus two samples of the virus are in infected archives. Products that have archive scanning activated by default are unlikely to encounter problems with detection here – however, relatively few products have archive scanning enabled on access, resulting in a few misses of these samples. With no ItW misses, *eTrust Antivirus* earns *CA* a VB 100% award.

CA Vet Anti-Virus Protection 10.54.0.12

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.90%
ItW File	100.00%	Polymorphic	98.50%

Files missed by *Vet* consisted of a pair of the more troublesome samples of the standard test set and a selection of the polymorphics. Two missed samples of ACG.A and W32/Etap.A contrast with the remaining misses, all of which were samples of the W32/Marburg.A virus. Since this was missed only in EXE files (and detected in SCR files), it seems likely that something strange is afoot here. Again, with no misses in the ItW test set, *Vet* gains *Computer Associates* a further VB 100%.

Cat Computer Services QuickHeal XGen 6.08

ItW Overall	99.76%	Macro	97.83%
ItW Overall (o/a)	99.76%	Standard	72.10%
ItW File	99.75%	Polymorphic	82.94%

QuickHeal is another product that shows a certain age discrimination in its detection abilities. While In the Wild and macro detection rates were good, the detection rate on the older files in the standard and polymorphic test sets was comparatively poor. However, even where newer viruses were concerned detection was imperfect, in particular, the VBS/Redlof.A DLL file was missed, which prevents *QuickHeal* from achieving a VB 100% award.

Command AntiVirus for Windows 4.75.0

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.76%
ItW File	100.00%	Polymorphic	93.21%

The files missed by *Command*'s product were very specific in type, with one exception. W32/Tuareg.B, W32/Zmist.D, W32/Etap.A and W32/Fosforo.A can all be categorised as 'modern polymorphics'. The exception was the HTM portion of W32/Gokar.A. However, there were no misses of files in the ItW test set, and without false positives *Command*'s product qualifies for a VB 100%.

DialogueScience DrWeb for Windows 95-XP 4.29b

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

The detection rate of *DrWeb* was, once again, of a very high standard. With misses only on access, and only on files containing archived viral code, *DialogueScience* gains another VB 100% award. As has become traditional, *DrWeb* generated 15 warnings in the clean test set, though none of these were declared to be viruses, all being simply 'suspicious' files.

Eset NOD32 Anti-virus 1.341

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

Yet again, *NOD32* provided what is becoming a rather dull score of no misses in any of the test sets upon which it was applied, thus being eligible for another VB 100% award to add to its growing collection.

FRISK F-Prot Antivirus 3.12d

ItW Overall	99.76%	Macro	100.00%
ItW Overall (o/a)	99.76%	Standard	99.82%
ItW File	99.75%	Polymorphic	97.41%

In terms of number of samples alone, the vast majority of misses for *F-Prot* were of W32/Etap.A. There was a smaller number of other misses, all of which were undetected by more than two products in the test – amongst these was VBS/Redlof in the ItW set, denying *F-Prot* its VB 100% award on this occasion.

F-Secure Anti-Virus 5.41 8490

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.86%
ItW File	100.00%	Polymorphic	99.92%

The files missed by *F-Secure Anti-Virus* were sufficiently well distributed across the test sets that no real categorisation can be made. None of the files that went undetected were in the ItW sets, either on access or on demand, therefore *F-Secure* achieves a VB 100% award.

GDATA AntiVirusKit 12.0.2

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.92%

AVK is in a unique position in terms of product evolution in that it is derived from the engines of two other companies, *Kaspersky* and *GeCAD*, and is itself used as the basis for another product, *MicroWorld*'s *eScan*. The use of two engines is now a tried and trusted mechanism for adding security to a product and, sure enough, *AVK* missed only one sample of W32/Etap.A in the entire test. With no false positives to spoil this result, *AVK* gains a VB 100% award.

GeCAD RAV for Windows 8.6.104

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.88%
ItW File	100.00%	Polymorphic	99.86%

With a product derived from *RAV*'s engine having claimed a VB 100% award already it remained to be seen whether the developer's own implementation could match the performance. Rather more misses were encountered in the polymorphic test sets, but these were not sufficient to deny *RAV* a VB 100% award.

Ggreat ZMW32 Virus Scan 2002 N22

ItW Overall	53.65%	Macro	57.46%
ItW Overall (o/a)	N/A	Standard	45.36%
ItW File	56.33%	Polymorphic	11.73%

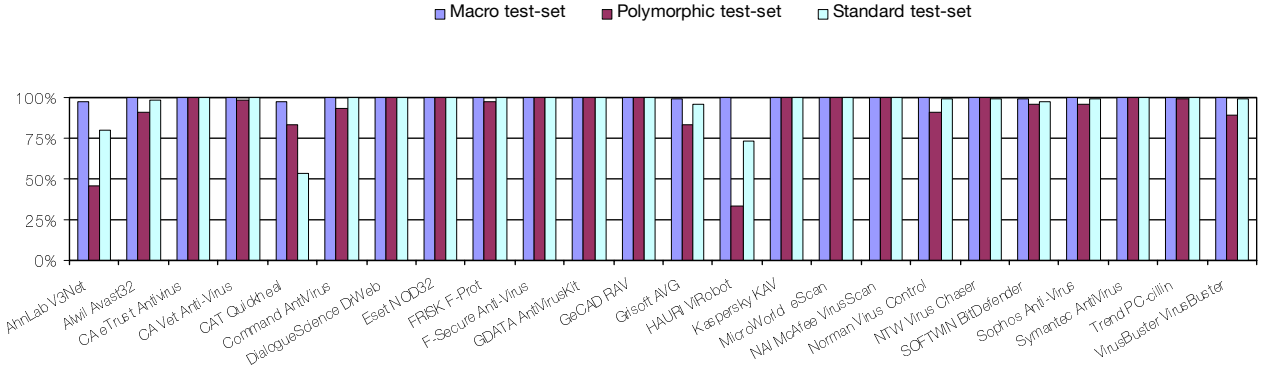
As noted in the last review, *Ggreat*'s product does not implement an on-access file scanner, rendering it ineligible for a VB 100% award. The product displayed a degree of instability, which seemed related to functions other than those tested but was an annoyance nevertheless. As for results, *ZMW32* was definitely the black sheep of this month's line-up, missing a considerable number of viruses in all test sets. The product also generated four full-blown false positives in the clean sets, the only such full declarations of viral infection seen in this review.

Grisoft AVG 6.0 Anti-Virus System 6.0.437

ItW Overall	100.00%	Macro	99.44%
ItW Overall (o/a)	99.76%	Standard	97.88%
ItW File	100.00%	Polymorphic	85.97%

The first set of results obtained for *AVG* were not good, but they were accompanied by a path error when installing the latest updates. The error mysteriously vanished after a reinstallation, leading to markedly improved results.

Detection Rates for On-Access Scanning



On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	4	99.83%	0	100.00%	99.84%	114	97.45%	8627	45.58%	413	80.08%
Alwil Avast32	0	100.00%	0	100.00%	100.00%	16	99.61%	153	91.21%	41	98.28%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	3	99.70%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	437	98.50%	4	99.78%
CAT Quickheal	1	99.75%	0	100.00%	99.76%	95	97.74%	2788	82.94%	835	53.67%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	123	93.61%	12	99.62%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.70%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	1	99.75%	0	100.00%	99.76%	0	100.00%	34	97.45%	3	99.82%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	3	99.86%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	7	99.86%	2	99.88%
Ggreat ZMW32	-	-	-	-	-	-	-	-	-	-	-
Grisoft AVG	1	99.75%	0	100.00%	99.76%	23	99.44%	425	83.72%	78	96.23%
HAURI ViRobot	1	99.83%	0	100.00%	99.84%	0	100.00%	10795	33.63%	534	73.58%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	3	99.79%	0	100.00%
MicroWorld eScan	3	98.96%	0	100.00%	99.01%	3	99.98%	3	99.79%	3	99.87%
NAI McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	5	99.68%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	9	99.78%	183	91.00%	14	99.50%
NTW Virus Chaser	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	5	99.52%
SOFTWIN BitDefender	1	99.96%	0	100.00%	99.96%	26	99.44%	109	96.10%	64	97.54%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	11	99.73%	60	95.79%	15	99.31%
Symantec AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	180	99.31%	8	99.82%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	159	89.13%	12	99.49%

Unfortunately for *Grisoft* these results were not perfect In the Wild, a single sample of W32/Zoek.D being the fatal slip.

Grisoft's scanner was not without some false positives in the clean sets, registering five warnings of potential infection. Like most of the false positives in this comparative, however, these were not absolute declarations of infection.

HAURI ViRobot Expert 4.0

ItW Overall	99.84%	Macro	98.87%
ItW Overall (o/a)	99.84%	Standard	73.58%
ItW File	99.83%	Polymorphic	33.63%

ViRobot was tested in the last comparative review (see *VB*, November 2002, p.16), and came tantalisingly close to

gaining a VB 100% award. On that occasion the VBS component of W32/Vote.A was responsible for dashing *HAURI*'s hopes, and the same was true this time. Misses were relatively frequent in other test sets, though confined, by and large, to older viruses where few encounters are likely in the real world, especially on any *NT* system. One warning was produced on the clean test set, though this was not a full-scale infection alert. On a very positive note, *ViRobot* was the fastest scanner over the uncompressed clean-executable test-set.

Kaspersky KAV 4.0.5.37

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.79%

Gratifyingly for *Kaspersky Lab*, *KAV*'s results were amply sufficient for *Kaspersky* to walk away with a VB 100% award. Misses were few in number and confined to the usual suspects: two samples of W32/Etap.A and a single sample of W32/Zmist.D.

MicroWorld Software Services eScan 10.1.0.0

ItW Overall	84.29%	Macro	100.00%
ItW Overall (o/a)	99.01%	Standard	97.64%
ItW File	83.50%	Polymorphic	99.57%

eScan is part of a rather wider suite of programs, most of which were ignored for the purposes of this test. On-access scanning proceeded smoothly, and results were not far off the equivalent tests of *AVK* – from which the scanning portion of the software seems to be derived in appearance, as well as engine. Results on demand, however, were distinctly odd. A large number of more recent worms were missed altogether, despite being detected perfectly on access. This mysterious behaviour was replicated several times in the name of curiosity. *eScan* would have failed to attain a VB 100% regardless of this behaviour, by dint of missing samples In the Wild of O97M/Tristate-C, W32/Benjamin.A and W32/Frethem.F. Given the strength of the underlying engine this is clearly a product with promise, which has been somehow subverted in the process of rebadging.

NAI McAfee VirusScan 4.51 sp1 4.0.4240

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.80%
ItW File	100.00%	Polymorphic	100.00%

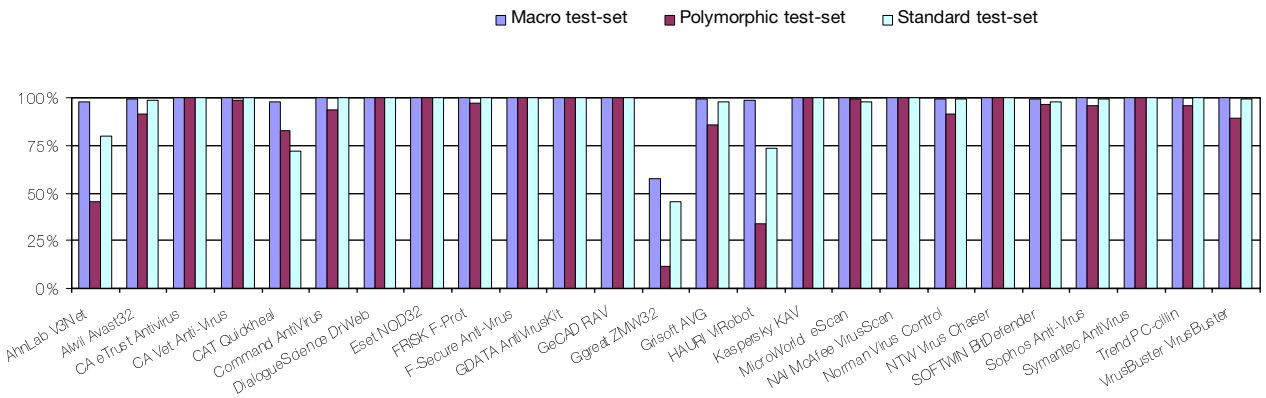
VirusScan was among those programs whose results were identical both on access and on demand, with the exception of the detection of the ZIP archived copies of W32/Heidi.A. The samples that were missed were examples of those where valid reasons can be given for taking the decision not to detect the viruses: the .TMP sample of W32/Nimda.A contains only a stored version of the virus, while JS/Unicle.A is reliant upon a non-existent website in order for its HTA portions to be of any concern. With no misses other than these, *VirusScan* gains a VB 100% award.

Norman Virus Control 5.40.33

ItW Overall	100.00%	Macro	99.55%
ItW Overall (o/a)	100.00%	Standard	99.62%
ItW File	100.00%	Polymorphic	91.25%

In the past few tests *NVC* has been notoriously slow in scanning, a problem which I was delighted to note had vanished on this occasion. Misses for *NVC* were scattered through the macro, polymorphic and standard test sets, some of which were of samples that, overall, are rarely missed. This said, none of the misses occurred in the ItW test set, and another VB 100% award is due to the *Norman* team.

Detection Rates for On-Demand Scanning



On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	4	99.83%	0	100.00%	99.84%	110	97.58%	8627	45.58%	414	80.05%
Alwil Avast32	1	99.75%	0	100.00%	99.76%	18	99.56%	153	91.21%	35	98.39%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	0	100.00%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	437	98.50%	2	99.90%
CAT Quickheal	1	99.75%	0	100.00%	99.76%	89	97.83%	2788	82.94%	555	72.10%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	128	93.21%	9	99.76%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	1	99.75%	0	100.00%	99.76%	0	100.00%	35	97.41%	3	99.82%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	3	99.86%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	7	99.86%	2	99.88%
Ggreat ZMW32	269	56.33%	10	0.00%	53.65%	1776	57.46%	14772	11.73%	1063	45.36%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	23	99.44%	257	85.97%	57	97.88%
HAURI ViRobot	1	99.83%	0	100.00%	99.84%	42	98.87%	10795	33.63%	534	73.58%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	3	99.79%	0	100.00%
MicroWorld eScan	36	83.50%	0	100.00%	84.29%	0	100.00%	6	99.57%	18	97.64%
NAI McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.80%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	18	99.55%	180	91.25%	12	99.62%
NTW Virus Chaser	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	17	99.59%	109	96.10%	49	98.08%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	11	99.73%	60	95.79%	14	99.34%
Symantec AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.82%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	172	89.07%	9	99.64%

New Technology Wave Inc. Virus Chaser 5.0

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

Derived from *DrWeb*'s *DialogueScience* product, *Virus Chaser* is another new entry into the comparative review process. The overall appearance of *Virus Chaser* was slightly more aesthetically polished than that of *DrWeb*, though this was countered by some missing features.

On access *Virus Chaser* failed to detect two samples of Cruncher, the two archived copies of W32/Heidi.A and the EML copy of W32/Braid.A, all located in the standard set.

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time(s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	Time(s)	Throughput (MB/s)
AhnLab V3Net	83	6589.5		10	7933.4		137	1163.6	43	1735.1
Alwil Avast32	226	2420.1		7	11333.4		56	2846.7	14	5329.1
CA eTrust Antivirus	189	2893.8		15	5288.9		93	1714.2	25	2984.3
CA Vet Anti-Virus	136	4021.6		15	5288.9		84	1897.8	23	3243.8
CAT Quickheal	123	4446.6		11	7212.2		84	1897.8	25	2984.3
Command AntiVirus	197	2776.3		13	6102.6		75	2125.6	14	5329.1
DialogueScience DrWeb	225	2430.8	[15]	15	5288.9		81	1968.1	15	4973.8
Eset NOD32	93	5881.0		13	6102.6		69	2310.4	25	2984.3
FRISK F-Prot	182	3005.1		15	5288.9		88	1811.6	12	6217.3
F-Secure Anti-Virus	366	1494.4		21	3777.8		158	1009.0	25	2984.3
GDATA AntiVirusKit	614	890.8		15	5288.9		261	610.8	36	2072.4
GeCAD RAV	473	1156.3		15	5288.9		196	813.3	24	3108.6
Ggreat ZMW32	76	7196.5	4	16	4958.4		2125	75.0	113	660.2
Grisoft AVG	306	1787.4	[5]	20	3966.7		106	1503.9	20	3730.4
HAURI ViRobot	69	7926.6	[1]	31	2559.2		58	2748.6	15	4973.8
Kaspersky KAV	223	2452.6		8	9916.7		113	1410.8	30	2486.9
MicroWorld eScan	121	4520.1		12	6611.1		117	1362.5	35	2131.6
NAI McAfee VirusScan	181	3021.7		15	5288.9		37	4308.6	12	6217.3
Norman Virus Control	243	2250.7		21	3777.8		110	1449.2	8	9325.9
NTW Virus Chaser	312	1753.0	[15]	29	2735.6		113	1410.8	22	3391.2
SOFTWIN BitDefender	852	641.9	[1]	9	8814.9		452	352.7	24	3108.6
Sophos Anti-Virus	148	3695.5		20	3966.7		70	2277.4	20	3730.4
Symantec AntiVirus	161	3397.1		30	2644.5		89	1791.2	28	2664.6
Trend PC-cillin	145	3771.9		13	6102.6		70	2277.4	18	4144.9
VirusBuster VirusBuster	237	2307.7		19	4175.5		124	1285.6	23	3243.8

The samples in the ItW test set were all detected and with 15 warnings but no full false positives in the clean set, *Virus Chaser* obtains a VB 100% award at first try.

SOFTWIN BitDefender Professional 6.5

ItW Overall	100.00%	Macro	99.59%
ItW Overall (o/a)	99.96%	Standard	98.08%
ItW File	100.00%	Polymorphic	96.10%

The detection rates of *BitDefender* were somewhat different on access from those on demand, which seems to be due to a decision not to scan certain extensions on access. Presumably the reasoning behind this is to remove overhead, though it carries with it the chance that some files with unusual extensions may pass through the net of detection.

Unfortunately, this is exactly what happened, with the extensionless version of W32/Tristate.C ItW going undetected. As a result, *BitDefender* misses out on a VB 100%

award. Although false positives have become mercifully rare in the recent comparative reviews, *BitDefender* did generate a false positive, though this was rated only as a potential infection rather than a definite problem.

More disturbing (for the *SOFTWIN* developers at least) will be the speed of scanning in the clean test set, which was the slowest of those products reviewed on uncompressed executable files.

Sophos Anti-Virus 3.65

ItW Overall	100.00%	Macro	99.73%
ItW Overall (o/a)	100.00%	Standard	99.34%
ItW File	100.00%	Polymorphic	95.79%

Sophos AntiVirus, like the previous product, opts not to scan certain file types by default in order to reduce overhead – though *Sophos* extends this to cover both on-access and on-demand scanning. This resulted in the product missing samples of the (admittedly not particularly threatening) A97M/Accessiv family. However, the selection of file types that go unscanned has been chosen with sufficient cunning as to have no effect upon detection rates In the Wild. *SAV* therefore receives a VB 100% award.

Symantec AntiVirus 8.00.9374 4.1.0.15

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

In a confusing development the removal of Peter Norton's paid endorsement of *Symantec AntiVirus* has changed the acronym of choice for this product from *NAV* to *SAV* – resulting in two widely available '*SAV*' products.

Ignoring this minor frustration for the moment and concentrating on the detection rates, *Symantec*'s product missed no infected samples either on access or on demand, leaving *Symantec AntiVirus* with a VB 100% award.

Trend Micro PC-cillin 10.01 1020 6.53

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.82%
ItW File	100.00%	Polymorphic	95.77%

Trend's product continues to show perfect detection rates in all areas save the pesky polymorphics. With some polymorphics being present in the standard set, this weakness is apparent in two rather than one test set, though the In the Wild and macro test sets were detected in their entirety. Such a performance is, of course, the prerequisite for *PC-cillin* to be awarded a further VB 100%.

VirusBuster VirusBuster for Windows Antivirus Solution 4.1.4

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.64%
ItW File	100.00%	Polymorphic	89.07%

VirusBuster's results on access and on demand showed distinctly different detection rates on a number of viruses. While, in some cases, the explanations applied to previous products may be applied, in other cases *VirusBuster* managed to be simply perplexing in its behaviour. However mysterious the misses in the polymorphic set, though, none occurred in the ItW set, thus *VirusBuster* is eligible for a VB 100% award.

Conclusions

A number of products in this comparative have achieved a VB 100% award without extensive detection rates in test sets other than In the Wild. In the past some products have been unable to detect certain polymorphics due to engine limitations, however, the aged and simplistic nature of some of the files that were missed does not justify this as a blanket explanation. The merits of removing detection of some older DOS viruses from AV products has been a topic of conversations I have held with developers from a number of AV vendors. Several researchers held the view 'it must be detected if it can infect'. Others were more pragmatic and pointed to the added overheads required for the detection of files which pose a minimal threat to the majority of users. It seems that some of the newer products have implemented this pragmatism – they have the ability to detect old DOS file viruses, but it is not worth their while.

I suspect that it is unlikely that other products will join the newcomers in this practice. A product which instituted this step would instantly lose percentage detection ratings in a number of tests, including those performed here. Not only that, but numbers quoted in 'this product detects xxx viruses' claims would drop dramatically as DOS virus generators are responsible for thousands of viruses detected. There would be howls of outrage, not so much from the users but from the marketing departments, falling upon this as 'evidence' of defective detection. So there you have it, when your machine slows down as a result of your scanner you know who to blame: our tests and those who market the products you rely upon.

Technical Details

Test environment: Three 1.6 GHz Intel Pentium 4 workstations with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, all running *Windows NT 4 Workstation Service Pack 6*.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/WinNT/2003/test_sets.html.

A complete description of the results calculation protocol can be found at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

SUBSCRIPTION RATES

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

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

Editorial enquiries, subscription enquiries, orders and payments:

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

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

US subscriptions only:

VB, 6 Kimball Lane, Suite 400, Lynnfield, MA 01940, USA

Tel (781) 9731266, Fax (781) 9731267

END NOTES AND NEWS

The Black Hat Windows Security 2003 Briefings take place 26–27 February 2003 in Seattle, WA, USA. The Briefings comprise six tracks across two days and follow two days of Black Hat Windows Security Training (24–25 February). See http://www.blackhat.com/.

The 12th Annual SysAdmin, Audit, Networking and Security Conference (SANS) takes place 7–12 March 2003 in San Diego, USA. The conference will feature 12 tracks, night activities, a vendor exhibition, and additional special events. See http://www.sans.org/.

Infosecurity Italy will be held in Milan, Italy, 12–14 March 2003, for details see http://www.infosecurity.it/.

CeBIT, one of the world's largest information technology trade fairs, runs for one week in Hannover, Germany from 12–19 March 2003. All aspects of IT are catered for, with well over 7,000 exhibitors. For full details see http://www.cebit.de/.

SACIS Expo (Security, Audit & Control of Information Systems) takes place 25–26 March 2003 in Istanbul, Turkey. Hear about the latest information security and audit developments from IT security professionals, and meet with product developers and academics. Early registrations qualify for a discount of up to 20%. For details see http://www.smartvalley.net/sacis/.

RSA Conference 2003 takes place 13–17 April 2003 at the Moscone Center, San Francisco, CA, USA. General sessions feature special keynote addresses, expert panels and discussions of general interest. Optional tutorials and immersion training sessions will provide the basics of e-security technology, enterprise security and security development techniques. For more information and booking details see http://www.rsaconference.net/.

Information Security World Asia takes place 23–25 April 2003, at Suntec Singapore. For details of what is claimed to be Asia's largest and most dedicated security technology and solutions exhibition see http://www.informationsecurityworld.com/2003/iswa_SG/.

Infosecurity Europe 2002 takes place 29 April to 1 May 2003, at Olympia, London. A free keynote and seminar programme alongside almost 200 exhibitors is expected to attract more than 7,000 dedicated security visitors. See http://www.infosec.co.uk/.

EICAR 2003 will take place 10–13 May 2003 in Copenhagen, Denmark. The 12th Annual EICAR Conference combines academia, industry and media, as well as technical, security and legal experts from civil and military government, law enforcement and privacy protection organisations. Call the conference hotline +45 4055 6966/ +44 709 211 1950 or check http://conference.eicar.org/ for details.

Black Hat Europe 2003 takes place 12–15 May 2003 at the Grand Krasnapolsky, Amsterdam, the Netherlands. For more details see http://www.blackhat.com/.

The DallasCon Wireless Security Conference takes place 24–25 May 2003 in Plano, Texas. A two-day wireless security course precedes the conference, including hands-on lab experience and lectures. For full details see http://www.DallasCon.com/.

The Thirteenth *Virus Bulletin* International Conference and Exhibition (VB2003) takes place 25–26 September 2003 at the Fairmont Royal York hotel in Toronto, Canada. Those interested in sponsorship or exhibiting at the event should contact Bernadette Disborough on +44 1235 555139 or email vb2003@virusbtn.com (for details of how to submit a paper for the conference see p.3). More information can be found at http://www.virusbtn.com/conference/.

***Trend Micro Inc*. has released a range of new messaging security product versions**: *InterScan Messaging Security Suite 5.1* for *Windows*, UNIX and *Linux*, *ScanMail for Exchange versions 6.1* and *3.81* and *ScanMail for Lotus Notes 2.6*. The products support *Trend*'s 'Enterprise Protection Strategy'. For full details visit http://www.trendmicro.com/.

***DialogueScience, Inc.* has introduced a new installation kit for its *Dr.Web for Windows 95-XP* product**. The installation kit contains a new component: the SpIDer Mail utility which, until now, has been supplied as a separate package. The installation kit is available for downloading from http://www.dials.ru/english/download/.

Aladdin Knowledge Systems* has added anti-spam features to version 3.5 of *eSafe Mail* and e*Safe Gateway. In addition, several features have been upgraded, and version 3.5 now fully supports *Windows 2000*. For more information see http://www.eAladdin.com/.