COMPARATIVE REVIEW

Look at ME!

Matt Ham

Since the last Comparative in these hallowed pages, back in the November issue, there has been change in the world. Most noticeably, to the outside world at least, a relative host of executable viruses descended upon the WildList in a plague of biblical proportions, replacing the recent deluge of script viruses. These introduced an extra extension to scan – the .CHM used by the W32/BleBla worm – an event which always brings uncertainty into the results of the Comparative tests. For further possibilities of the unexpected, the platform tested this month – *Windows ME* – is one which has never before been used in *VB* testing.

The general scientific method of testing is of changing only one variable at a time, though having changed two thus far it seemed a good time to change everything else as well. In truth, the change of hardware was inevitable, since the venerable test machines have been taking an intolerable length of time to complete tests recently, and did not have sufficient hard drive space to install *Windows ME* and all the required test-sets. Details of the exact hardware used can be found, as ever, at the end of this review.

Test Procedures

With all this remodelling out of the way the test procedure itself was the final area where changes occurred, though in this case perhaps codification was more the order of the day. The overall gist of the VB 100% testing regime has been clear since its inception – test the software in its default settings for detection and false positives. With the addition of several new parts to the test, however, combined with there being many different ways to prove that a product can detect a virus in a specific file, there have been several occasions when this has been too vague – thus the following clarification.

In order to be given a VB 100% award a product must detect, in its default setting, all viruses on the top half of the WildList during the month prior to its test. 'Default setting' refers to such selectable affairs as sensitivity of detection, scanned extensions and the use of heuristics. Settings not related to detection *may be changed* in order to facilitate the production of realistic results. This full detection must be demonstrated both on-access and on-demand.

For on-demand testing, results are preferably taken by parsing of log files, with the setting of 'report only' selected. Network and CD scanning has been seen to introduce sporadic errors into the test results and thus this is performed upon a copy of the test-sets on a local hard drive. It has, however, been the case in many products of late that log files are either useless for *VB* results or that the taking

of log files causes the scanner to crash after a certain size is reached. In such cases, the preferred method is to run a scan selecting 'delete' as the option, followed by another choosing 'quarantine' and another scan to check that no further files are being detected as viral. Those files remaining are regarded as misses.

For on-access testing, a tool is used which seeks through the test-sets recursively, opening each file in turn. Scanners are set to block access on opening of an infected file and a tool generates a log of those files opened. For products which scan on 'file close' rather than 'open' a different method is used. Under operating systems where such a function is available natively, the test-set is copied using a command which allows the blocking of individual copy operations. In this test the XCOPY command was used for this purpose.

For false positive detection, the scanners are required to produce no false positives on the OLE and Clean test-sets. Many products declare files to be suspicious which is *not* considered to be a false positive but is registered as having occurred in the table of results. If archive scanning is implemented it is activated, if 'off' by default it is only run during the scans involving archived files. These latter tests are not used for the determination of false positives.

A healthy dose of preamble out of the way, the results are to come. With despair, frustration and explosions in store for the reader, who could resist the wonders that await ?

Aladdin eSafe Desktop v3

ItW Overall	99.6%	Macro	96.8%
ItW Overall (o/a)	31.3%	Standard	97.0%
ItW File	99.6%	Polymorphic	89.3%

A strange set of results from *Aladdin* saw an impressive improvement in the on-demand results in comparison with the November tests on *NT*, with only two files undetected in the wild and overall several hundred more viruses detected.

There was, however, a downside to this with macro detection seeming to be partially disabled on-access. This was most noticeable with *Word 97* files, with other macro containing objects being somewhat affected. Though it is probably fair to assume this to be a momentary, if worrying, blip in the detection, the developers have reasons to be both pleased and displeased alike with this result.

Also of interest was *eSafe's* behaviour on the scan speed tests. On several occasions the scanner gave the message 'skipped xx files' where xx was a number ranging from 2 to 32. This behaviour was not explained further in any way and was in addition to three false positives.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	2	99.65%	99.66%	125	96.80%	322	89.32%	73	97.01%
Alwil AVAST32	0	100.00%	2	99.53%	99.55%	25	99.32%	8	95.36%	12	99.03%
CA InoculateIT	0	100.00%	2	99.53%	99.55%	0	100.00%	9	98.87%	2	99.61%
CA Vet Ant-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	2	99.96%
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	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	8	99.15%
GDATA AntiVirusKIt	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	1	99.77%	99.77%	0	100.00%	0	100.00%	1	99.90%
Grisoft AVG	0	100.00%	2	99.53%	99.55%	8	99.79%	124	92.01%	30	98.67%
HAURI ViRobot	10	52.38%	194	78.14%	77.42%	1229	67.56%	10904	27.83%	735	58.23%
Kaspersky Lab KAV	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	1	99.91%	99.91%	0	100.00%	19	97.86%	7	99.86%
Norman Virus Control	0	100.00%	1	99.77%	99.77%	0	100.00%	618	92.43%	23	98.87%
Sophos Anti-Virus	0	100.00%	2	99.53%	99.55%	13	99.65%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	0	100.00%	16	99.46%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	2	99.93%	15	98.70%	5	99.61%

Alwil AVAST32 v3.0

ItW Overall	99.5%	Macro	99.3%
ItW Overall (o/a)	100.0%	Standard	99.0%
ItW File	99.5%	Polymorphic	95.3%

The first to fall victim to samples of W32/Blebla.B and .C, *Alwil's AVAST32* failed to detect the two .CHM files in the ItW set. Detecting these would not have been enough to gain a VB 100% award, however, due to the scanner's behaviour in the OLE Clean set. The scanner hung repeatedly on an *Excel* file.

In any case a true speed of scanning figure could not be determined and *AVAST32* is rated as 'not tested' for the two OLE-related speed tests. It also proved impossible on several occasions to stop a scan job permanently; only pausing seemed to work and this prevented exiting the application via any normal means as this paused job was pending. *AVAST32* also gained frustration points due to its somewhat impenetrable interface, which has an impressive number of controls yet manages to hide away some of those required for logging or actions to take on infection.

On-access scanning was performed by means of XCOPY, as there is no detection on 'file open'. The on-access scanner did manage, however, to deny reboots based upon a non-bootable CD being in the drive.

CA InoculateIT v4.53 build 524

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	96.2%	Standard	99.6%
ItW File	99.5%	Polymorphic	98.8%

InoculateIT seemed to be having problems adapting to the new operating system, showing a downturn in detection since the latest *Windows NT* and *Windows 98* tests. Most surprising was the non-detection of Michaelangelo in the on-access sets. There were also extension list problems on-access with .SCR files being passed over.

One possible cause for alarm here was the patch supplied with the product which claimed to address VBS security hazards. This resulted in declaring all files with the .VBS extension to be possibly viral. While not a totally outra-

In the Wild File Detection Rate

■ On-demand   ■ On-access

Note: Truncated vertical scale
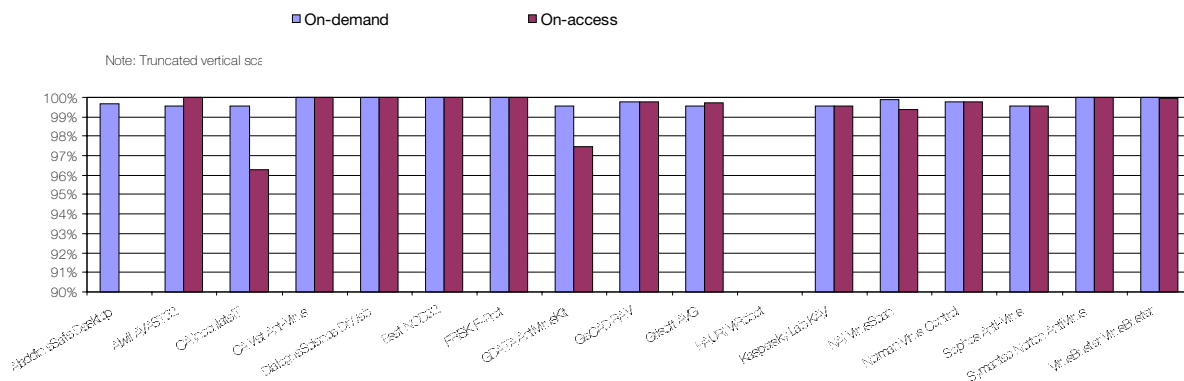
geous idea, it must be noted that standard *Windows ME* installations contain six .VBS files by default, and thus this patch almost guarantees false positives on a basic machine. Although the Clean set does not currently contain .VBS files, this particular patch seems destined to spur the addition of visual basic scripts to the Clean set.

CA Vet Anti-Virus v10.2.5.2

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	99.9%
ItW File	100.0%	Polymorphic	93.7%

Faring rather better in this test than its sister product *Vet* claims another VB 100% award as a result of its consistency. This was one of the first products examined and the first to demonstrate the blue screen warning from the OS upon removal of a disk from a floppy drive when *Windows ME* is not expecting it, in the same way that CDs cause this effect in *Windows 98*. This obvious change in the handling of floppy accesses did not, however, alter *Vet's* behaviour.

Misses for *Vet* were almost entirely to be found within the Polymorphic set, though small differences in on-access and on-demand scanning saw a slight advantage emerge for the former. One area where *Vet* has definitely lost ground is scan speed. Where once it was undisputed king of speed it now puts in a good performance on the OLE files but is only average on the executable Clean set.

DialogueScience DrWeb v4.22

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

The second product to offer no default on-access scanning for 'file opens', *DrWeb* was tested using XCOPY. The on-access scanner showed a smattering of misses in the Standard set, though elsewhere and on-demand detection was perfect. That a certain degree of *DrWeb's* efficiency was due to

heuristics was hinted at by the only fly in the ointment, a large number of warnings of suspicious files in the speed tests. These were not quite at the level of false positives, and thus a VB 100% was deserved and granted.

On an aesthetic note the alerts for on-access scanning are of a decidedly DOS-inspired nature and both unpleasant to look at and obtrusive. This cannot be held against *DrWeb* as alerts should be difficult to avoid – other products were cursed with 'ignorable alerts', a much greater problem.

Eset NOD32 v1.58

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

A product which does not change is often a bad thing, though in the last Comparative *NOD32* took a turn for the worse by missing out on a VB 100% award. This review showed a return to what *Eset* must consider the good old days with full detection across the board combined with a lack of any false positives – worthy of a VB 100% award again.

With no misses and an excellent overall scanning speed, there is little in the way of comment to make which is not blatantly obvious to even the most myopic observer. The interface does, in the hunt for notable changes, appear to have undergone some minor tweaking. This results in more control available than in the deep and distant past, while the artwork still ranks as a personal favourite.

FRISK F-Prot v3.08

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	99.1%
ItW File	100.0%	Polymorphic	99.9%

It has been some time since *F-prot* has been seen in its naked form, rather than clothed in the garments of *F-secure*. Given *F-Prot's* good reputation for its macro detection capabilities

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	634	29.42%	31.38%	3475	10.81%	690	73.54%	75	96.76%
Alwil AVAST32	0	100.00%	0	100.00%	100.00%	17	99.53%	28	95.36%	11	99.08%
CA InoculateIT	1	95.24%	28	96.28%	96.25%	17	99.64%	255	98.00%	59	97.22%
CA Vet Ant-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	0	100.00%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	1	99.98%	0	100.00%	9	99.81%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	22	98.84%
GDATA AntiVirusKIt	21	0.00%	8	97.44%	94.73%	0	100.00%	0	100.00%	4	99.64%
GeCAD RAV	0	100.00%	1	99.77%	99.77%	0	100.00%	292	89.47%	2	99.71%
Grisoft AVG	21	0.00%	2	99.73%	96.95%	29	99.31%	292	89.47%	47	97.11%
HAURI ViRobot	21	0.00%	194	78.14%	75.96%	1229	67.56%	10904	27.83%	735	58.23%
Kaspersky Lab KAV	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	4	99.40%	99.42%	3	99.97%	34	97.69%	10	99.63%
Norman Virus Control	0	100.00%	1	99.77%	99.77%	0	100.00%	616	92.44%	23	98.87%
Sophos Anti-Virus	0	100.00%	2	99.53%	99.55%	14	99.60%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.55%	0	100.00%	16	99.46%
VirusBuster VirusBuster	3	85.71%	1	99.96%	99.56%	8	99.82%	15	99.44%	5	99.61%

there was potential for a surprise if results for the scanner were not good. Surprises were not to be had – *F-Prot* easily qualified for the fourth VB 100% award in this review. The misses for *FRISK's* offering were a handful of standard and polymorphic files with no real shocks among them.

The only odd behaviour of note came in the on-access floppy scan tests, where the declaration of infection was made twice for each disk scanned. This made for a confusing test, but again, too many alerts is substantially better than too few.

proved to be unsurprisingly undetectable. More odd was that the .EXE parts of this worm, in its .B and .C variants, were detected on-demand but not on-access, the on-access scanner also failing to detect a pair of W32/MSInit variants also in the wild.

No other problems were encountered except in the matter of log files, which at first appeared to be as required, but failed due to the inclusion of page numbers interspersed with the scan data. On-demand detection ratings were thus judged by the deletion and quarantine method.

GDATA AntiVirusKit v10.0.1.0

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	94.7%	Standard	100.0%
ItW File	99.5%	Polymorphic	100.0%

Having recovered from its non-scanning of macros in the last Comparative, or perhaps having slyly transferred this problem to *Aladdin*, *AVK* had a much better showing on this outing. ItW on-demand the two W32/Blebla.CHM files

GeCAD RAV v8.1.5.28

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

Though in the final stages of beta in the last review, *RAV* was definitely finished and in an improved state in this test. Like several other products, *RAV* sports a dual mode, with 'advanced' and 'simple' being freely interchangeable once

Detection Rates for On-Access Scann

■ Macro test-set   ■ Polymorphic test-set   ■ Standard test-set

Note: Truncated vertical scale
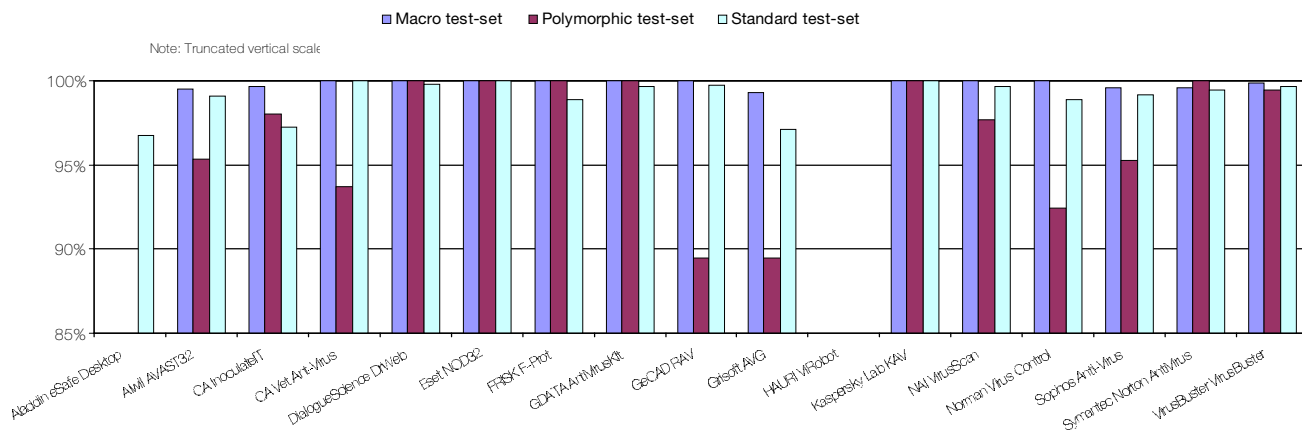
the relevant button has been located. On the detection front for files, results were impressive, only JS/Unicle preventing 100% detection ItW.

On-access there were problems – with a full log and monitor enabled the scanner was not entirely stable, while the floppy scans verged on the invisible on occasion due to being non-modal and not always in the foreground. On-demand, the floppy scans managed to declare two scans for each disk, one of which always declared 'no infection' while the other proved accurate. A worthy product, it seems likely that these small issues will be attended to by the next review, though the heuristics are still more than a little fierce during the scan speed tests.

Grisoft AVG v6.0.226

ItW Overall	99.5%	Macro	99.7%
ItW Overall (o/a)	96.9%	Standard	98.6%
ItW File	99.5%	Polymorphic	92.0%

The ancient adversary that is JS/Unicle was also the only file missed in the wild for *AVG* – another in a long line of steady improvements. The *Grisoft* scanner also shared a predeliction for finding viruses where there were none in the Clean set, mostly in cases where the scanned files would be decompressed upon execution.

Floppy scanning is the prime area of concern for *AVG* – absent in the on-access field and very cumbersome in the on-demand scanner. On speed of scanning of OLE files, however, *AVG* is the undisputed champion and can boast a good detection rate in addition to raw speed.

HAURI ViRobot 2000 v3.0

ItW Overall	77.4%	Macro	67.5%
ItW Overall (o/a)	75.9%	Standard	58.2%
ItW File	78.1%	Polymorphic	27.8%

The arrival of a newcomer to the *VB* Comparatives is always a nervous time. As far as ease of operation and scan

speed went, however, *ViRobot* was a pleasant product and an early sigh of relief was breathed. There were some ominous signs though – a very small extension list and a scan rate almost too fast to be true being the main concerns.

Analysis of the results showed these concerns to be valid, with heavy misses across the board. Detection rates were slightly better for wild viruses than in other sets, and *Excel* files were better detected than the other *Office* formats. This is not surprising – *Word* is not at all popular in *HAURI's* native Korea, being supplanted by local products better able to deal with the hangul character set. *Excel*, on the other hand, is as popular as elsewhere. There is definitely room for improvement, and other developers will testify that inauspicious beginnings can be overcome in time.

Kaspersky Lab KAV v3.5.133.0

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

A nominally new product that will nevertheless be recognised by all regular readers, *KAV* once more falls short of a VB 100% award by the slightest of margins. This is again an extension issue, with the W32/Blebla .CHM files proving *KAV's* undoing. The 'scanner formerly known as AVP' presence of *KAV* was made more obvious by the parenthetic insertion of *AVP* in the 'help about' field of the program, though other than the name, few changes seem to have been made to the application itself.

As with other products though, there were some oddities with *Windows ME's* floppy operations, with disk changes causing strange messages to pop up on occasion, though this had no effect upon detection rates.

NAI VirusScan v5.15.0002.1

ItW Overall	99.9%	Macro	100.0%
ItW Overall (o/a)	99.4%	Standard	99.8%
ItW File	99.9%	Polymorphic	97.8%

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
Aladdin eSafe Desktop	885	618002	3	24	3305574		300	531389	32	2331484
Alwil AVAST32	535	1022303		n/t	n/t	1	197	809221	n/t	n/t
CA InoculateIT	121	4520101		9	8814863		74	2154278	17	4388676
CA Vet Ant-Virus	356	1536326		14	5666698		105	1518253	21	3552738
DialogueScience DrWeb	334	1637521	[25]	35	2266679	[1]	147	1084467	25	2984300
Eset NOD32	80	6836652		16	4958360		71	2245304	14	5329107
FRISK F-Prot	200	2734661		22	3606080		95	1678069	33	2260833
GDATA AntiVirusKIt	495	1104913		37	2144156		103	1547734	23	3243804
GeCAD RAV	1308	418144	2[47]	20	3966688		187	852495	39	1913013
Grisoft AVG	262	2087527	4 [2]	115	689859		99	1610269	18	4144861
HAURI ViRobot	62	8821487		39	2034199		147	1084467	47	1587394
Kaspersky Lab KAV	181	3021725		27	2938288		88	1811552	19	3926710
NAI VirusScan	156	3505975		21	3777798		108	1476080	29	2572672
Norman Virus Control	366	1494350		21	3777798		159	1002620	19	3926710
Sophos Anti-Virus	185	2956390		24	3305574		73	2183789	20	3730375
Symantec Norton AntiVirus	438	1248704		68	1166673		444	359046	35	2131643
VirusBuster VirusBuster	408	1340520		28	2833349		221	721342	14	5329107

A host of problems were noted in the *NT* Comparative relating to *VirusScan's* performance, which are still clearly evident in the current, more retail-oriented product tested this time round. Scanning of infected files was atrociously slow, despite the upgraded hardware. A scan which took at the most an hour on any of the other products (barring *Norton AntiVirus*, of which later) was still meandering its merry way along on *VirusScan* some *forty* hours later. This seemed almost certainly due to the log file, recompiled after every few detections, and as a result detection was ultimately performed by deletion. Even then, time problems were not solved totally, with W97M/Splash proving more time-consuming for each sample than some scanners found the entire test-set.

The scanning engine staff might rightly blame the front-end designers for the first of the problems, and vice versa for the second affliction. Whatever the burden of responsibility, there will be many years in Beelzebub's company for those responsible if there is any justice in the afterlife.

The infected files which caused *VirusScan's NT* incarnation to crash still did so, incidentally, so that I feel justified in ignoring the very decent detection rates in order to be harsh about *VirusScan's* shortcomings.

Norman Virus Control v5.00.18

ItW Overall	99.7%	Macro	100.0%
ItW Overall (o/a)	99.7%	Standard	98.8%
ItW File	99.7%	Polymorphic	92.4%

In contrast to the last product, the developers at *Norman* apologised in advance for any instability or detection problems that might arise from their new release – and, thankfully, none were at all apparent. ItW detection stood at 100% but for the .CHM sample of W32/Blebla.B, which was all that denied a VB 100% award to *Norman Virus Control* (*NVC*).

The new design of *NVControl* was not all milk and honey, though. The construction of tasks is a somewhat drawn out and less than intuitive affair, and tasks are required for all but the simplest procedure.

Scanning of floppies required numerous actions, with no chance of a continuous scan, while other tasks had to be constructed in one place and activated from another. There may be a simpler way through all of this, though it is not obvious, but hopefully these are constraints which will be overcome as the product matures.

Detection Rates for On-Demand Scanr

■ Macro test-set   ■ Polymorphic test-set   ▢ Standard test-set

Note: Truncated vertical scale
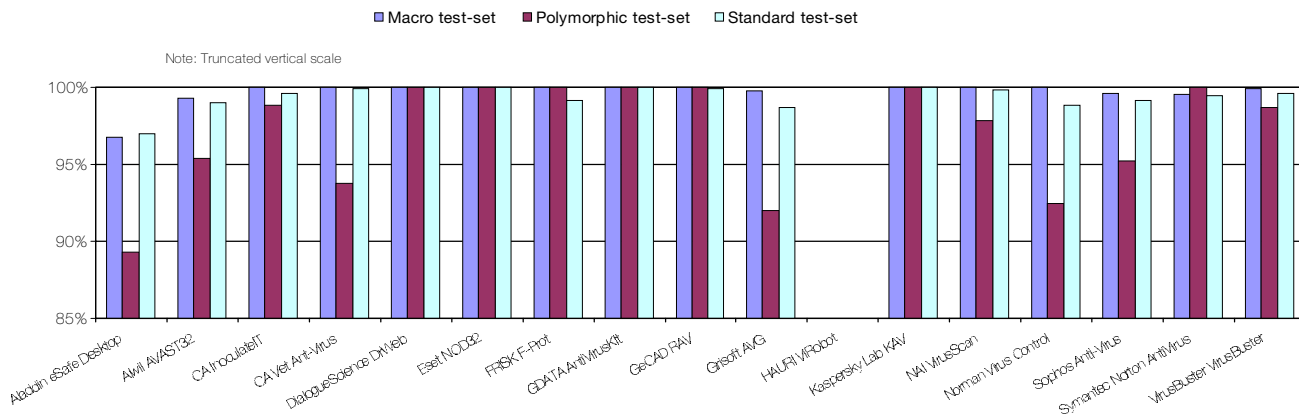
Sophos Anti-Virus v3.41

ItW Overall	99.5%	Macro	99.6%
ItW Overall (o/a)	99.5%	Standard	99.1%
ItW File	99.5%	Polymorphic	95.2%

Sophos Anti-Virus suffered in the last review from having an extension list a week or so out of date, and thus lacking .PIF files, and repeated this with .CHM files on this occasion, again just missing out on a VB 100% award by this one omission. Other than the two W32/Blebla.CHM files, the misses were the traditional few for *SAV*, encompassing the ACG.A and ACG.B polymorphics and a collection of files in the Standard set.

With the product having had much the same front-end for a considerable time now, there are few other areas to comment upon, though lovers of trivia might wish to know that of the products tested *SAV* is the only one to record files in its log in 8+3 format rather than as long file names.

Symantec Norton AntiVirus v7.50.846

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

Such was the power of *Norton AntiVirus* that shortly after testing the product one of the machines gave up the ghost in a manner which involved smoke, flashes and loud noises. Not wishing to be afflicted with the same end, I'll tread lightly and state that *NAV's* problems with stability and logging apparent in the *NT* comparative remained in this review.

Instability was decidedly rampant on the on-demand scan and thus detection was performed by deletion on the test-set. The on-demand floppy scan did not provide relief, as it involved a tedious rigmarole which might well prove a fitting activity for those found worthy of a cruel and unusual punishment. These problems aside, *NAV's* detection rates were again more than admirable, and the product picks up another VB 100%.

VirusBuster VirusBuster v3.0

ItW Overall	100.0%	Macro	99.9%
ItW Overall (o/a)	99.5%	Standard	99.6%
ItW File	100.0%	Polymorphic	98.7%

An admirable achiever on-demand, *VirusBuster* was let down by its on-access woes which, as luck would have it, were concentrated in the ItW set. The primary cause for concern, however, was in the on-access boot tests, where detection was very difficult to achieve. Operating system changes are consistently responsible for such problems and the tests performed involved all those permutations which allow feisty scanners to detect boot sector infectors on-access. Despite this, misses remained. One can hope that these are easily remedied, for if they are *VirusBuster* will be in with a good chance of a VB 100% in the near future.

Conclusions

All the changes mentioned in the introduction taken into account showed that the products themselves remained the one real constant. Improving products continued to improve, though in some cases there is little room for it; unlucky products missed out on VB 100% awards by the slightest of margins; the 'big two' (*VirusScan* and *NAV*) continued to be beset with problems of overzealous logging; many products suffered on-access boot problems.

Ever in search of some thrill to titillate the jaded appetite, the next Comparative will focus on *Windows 2000*. Will that be different enough to shake things up? I for one certainly hope so, though the developers might be less keen.

Technical Details

Test Environment: Three 750 MHz AMD Duron workstations with 64 MB RAM, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, all running *Windows ME*. The workstations were rebuilt from image back-ups and the test-sets restored from CD after each test.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/2000/11test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.