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%

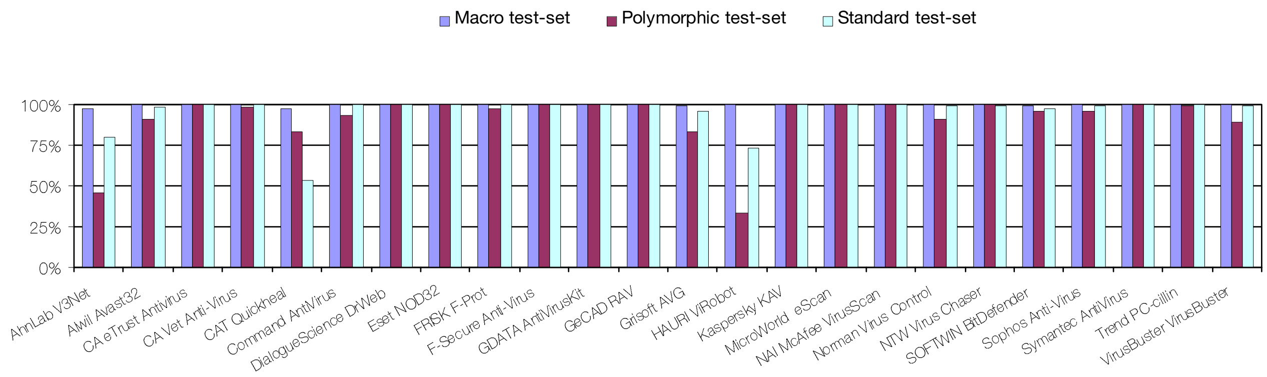
As noted in the last review, *Ggreat*'s product does not implement an on-access file scanner, rendering it ineligible for a VB 100% award. The product displayed a degree of instability, which seemed related to functions other than those tested but was an annoyance nevertheless. As for results, *ZMW32* 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%

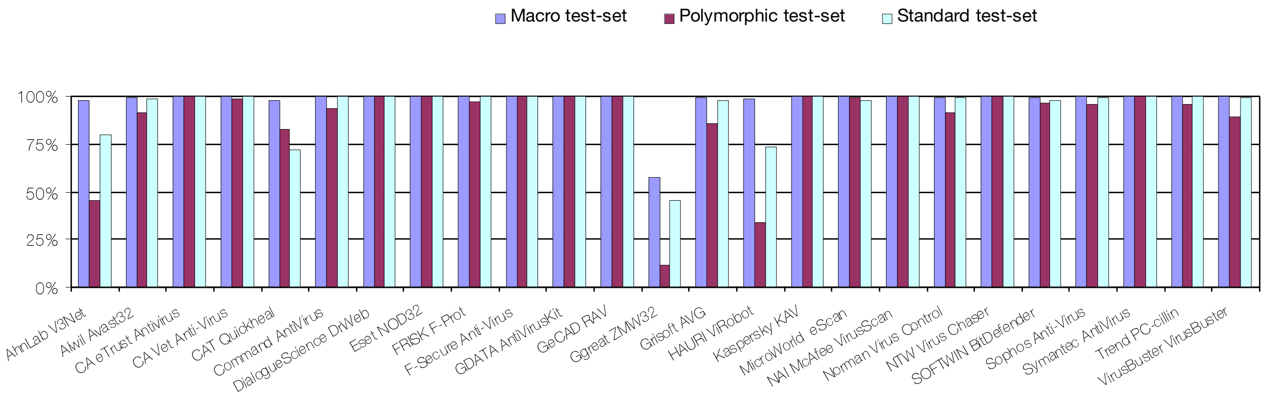
VirusScan was among those programs whose results were identical both on access and on demand, with the exception of the detection of the ZIP archived copies of W32/Heidi.A. The samples that were missed were examples of those where valid reasons can be given for taking the decision not to detect the viruses: 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.