COMPARATIVE REVIEW

WINDOWS NT

Matt Ham

I seem to remember having been aware in the last comparative review on this platform (see *VB*, February 2004, p.12) of a sense of impending doom that accompanied *Windows NT 4* – a sense of doom which is rather more pronounced a year later. With *Microsoft* having decided to remove support for *NT 4*, it must have been tempting for other developers to do much the same, if only to save on back-compatibility testing resources. However, it seems that *Trend Micro* is the only vendor that has opted to remove support at this stage – which explains the absence of a *Trend* product in the review.

I would not be willing to suggest that many other companies will follow suit. Having seen some veritably antique hardware and software in use, even in supposedly high-end research environments, I suspect there will continue to be a market for *NT* products for years to come. With large customers being able to blackmail legacy support from the vendors, it can be hard simply to terminate support for an otherwise unattractive platform.

Of the products submitted, *Hauri*'s proved to be the most beset with problems. An initial version had severe issues with resources, rendering it incomprehensible to mortal man. A replacement version proved to cause sufficient instability on access that testing was all but impossible. Therefore the product was left alone after these tribulations. A host of new product arrivals, however, pushed the number of contenders in this review to 28 – an all-time record for *VB*'s comparatives.

THE TEST SETS

The test sets were aligned to the Real-Time WildList from October 2004, the newer WildList arriving, as luck would have it, a day after the deadline for product submissions.

The additions to the set were, as is becoming rather a predictable occurrence, all immutable worms and far larger in number than the more interesting specimens that no longer appear in the wild. If ever a file infector comes into the wild again, I will at least find the process of replicating the test sets a degree more interesting.

AhnLab V3 VirusBlock 6.0.0.312

ItW Overall	99.75%	**Macro**	98.97%
ItW Overall (o/a)	100.00%	**Standard**	96.18%
ItW File	99.75%	**Polymorphic**	63.81%

Reappearing after a brief absence from *VB*'s comparative reviews, *V3* came very close to achieving a VB 100% award this month, missing only one sample of W32/Bagle.BB on demand. Elsewhere, *V3*'s polymorphic performance is still somewhat weak, though detection in the other sets has improved since the last tests.

Alwil avast! 4.5.555

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.36%
ItW File	100.00%	**Polymorphic**	93.58%

In a repeat performance of other recent tests of the product, the *avast!* review started with the on-access service failing due to the blank password on the test platform. One changed password later, however, all problems had vanished and avast! earned itself a VB 100%.

ArcaBit ArcaVir 2005

ItW Overall	99.64%	**Macro**	98.52%
ItW Overall (o/a)	99.71%	**Standard**	97.87%
ItW File	99.64%	**Polymorphic**	85.48%

ArcaVir has appeared in *Virus Bulletin*'s tests before, albeit under the name of *MKS*. The product has been rebadged, retuned and re-released, with the intention of marketing it to a more international audience. A handful of misses in the ItW set and a false positive blemished an otherwise impressive debut. Since the missed files were, in many cases, missed as a result of extension issues, the result should be improved upon in forthcoming reviews.

Less impressive, however, was the requirement to find and install MFC42.DLL manually before the program would operate.

Authentium Command 4.92.7

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	99.95%

Unlike the previous product, *Command* is a long-standing and familiar name. Seeming to work just as well on *NT* as on the rather newer *XP*, another VB 100% award goes to *Authentium*.

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3 VirusBlock	0	100.00%	0	100.00%	100.00%	47	98.97%	5549	63.81%	54	96.18%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	112	93.58%	17	99.18%
ArcaBit ArcaVir 2005	2	99.70%	0	100.00%	99.71%	33	99.47%	1402	85.48%	33	97.94%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	5	99.58%
Avira Avira	0	100.00%	0	100.00%	100.00%	0	100.00%	4	99.63%	6	99.91%
BLC Win Cleaner	0	100.00%	0	100.00%	100.00%	86	97.96%	1477	91.03%	473	72.47%
CA eTrust Antivirus (InoculateIT)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	4	99.51%
CA eTrust Antivirus (Vet)	0	100.00%	0	100.00%	100.00%	12	99.82%	1	99.92%	5	99.60%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	5	99.60%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	86	97.96%	1477	91.03%	473	72.47%
Doctor Web Dr.Web	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.69%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	200	95.85%	5656	61.54%	63	97.90%
FRISK F-Prot Antivirus	1	99.96%	0	100.00%	99.96%	0	100.00%	6	99.97%	10	99.19%
F-Secure Anti-Virus	3	99.24%	0	100.00%	99.24%	0	100.00%	0	100.00%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	19	99.53%	757	83.64%	33	98.35%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	0	100.00%	7	99.59%	5	99.92%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.88%
McAfee VirusScan	1	99.75%	0	100.00%	99.75%	0	100.00%	0	100.00%	3	99.79%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	181	91.03%	12	99.45%
NWI Virus Chaser	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.69%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	35	99.17%	6	99.73%	14	99.05%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	0	100.00%	15	99.30%
SR Resolution Antivirus	17	97.79%	3	0.00%	97.05%	20	99.58%	1014	88.96%	28	99.17%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
UNA UNA	414	16.79%	3	0.00%	16.67%	247	94.23%	15140	0.00%	22	97.43%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	96	92.79%	16	99.17%

Avira Avira 1.00.00.61

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.78%
ItW File	100.00%	**Polymorphic**	99.67%

Another product arriving in hopes of a new international audience, *Avira* will be better recognised by many readers as a prettier version of *H+BEDV*'s *AntiVir*.

With a few previous reviews from which to learn the ropes, the results achieved by this ostensibly new product were good indeed – and were certainly sufficient to be rewarded with a VB 100%.

BLC Win Cleaner 7.03

ItW Overall	100.00%	**Macro**	98.00%
ItW Overall (o/a)	100.00%	**Standard**	96.39%
ItW File	100.00%	**Polymorphic**	92.85%

Continuing in the same vein, *Win Cleaner* is, as assiduous readers will remember, a rebadged version of *CAT*'s *Quick Heal*. The physical resemblance here is very great indeed, as is the detection quality. Another VB 100% results.

CA eTrust Antivirus (I) 7.1.192

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	99.89%

This is the non-default version of *eTrust*, using the *InoculateIT* engine. After a slight hiccough in the last test, the product returned to put in a good performance on this occasion. Since this is the non-default version of *eTrust*, and its inclusion in the tests is for reasons of comparison with its *Vet*-engined counterpart, no VB 100% is awarded.

CA eTrust Antivirus (V) 7.1.192

ItW Overall	100.00%	**Macro**	99.82%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	99.87%

Not to be outdone by its different-engined sibling, the *Vet*-powered version of *eTrust* also put in a good performance and this, the default version of the product, is awarded a VB 100%. Sadly, the two products share what is, in my opinion, the most feeble and useless logging system ever devised by an otherwise reliable developer.

CA Vet Anti-Virus 10.6.4.0.9

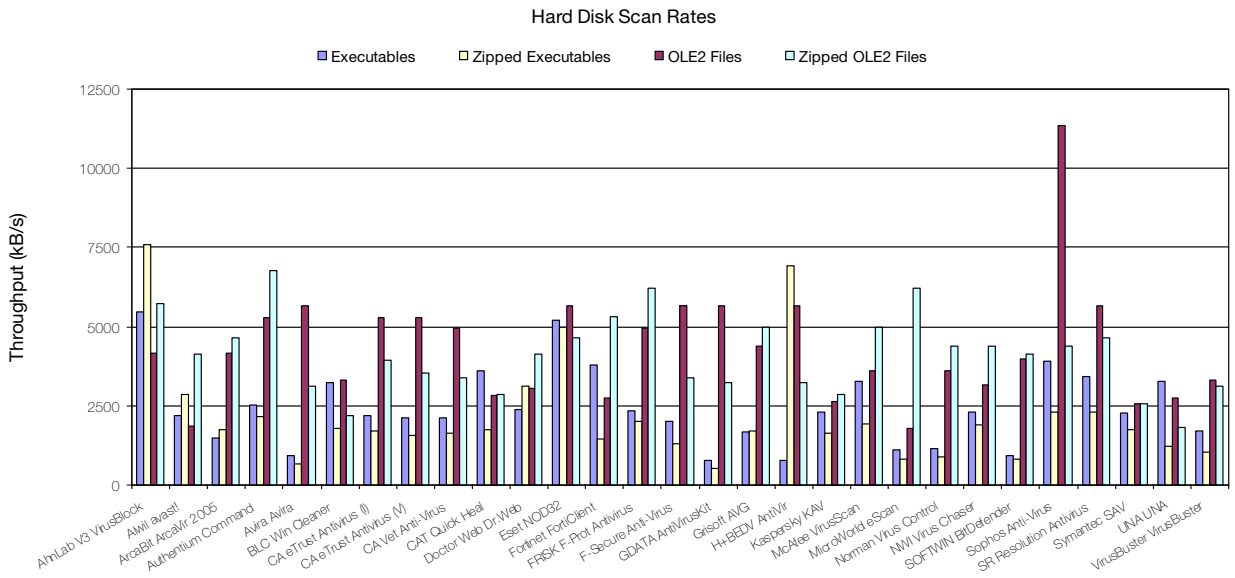
ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	99.87%

Using the same engine as the previous contender, the all-*Vet* product rejoices in a rather better logging system. Happily, in gaining this advantage it has lost no efficiency, and it too receives a VB 100% award.

CAT Quick Heal 7.03

ItW Overall	100.00%	**Macro**	98.00%
ItW Overall (o/a)	100.00%	**Standard**	96.39%
ItW File	100.00%	**Polymorphic**	92.85%

Since its 'offspring' has already received a VB 100% award in this test, it should come as little surprise that *CAT* does too. The interface remains somewhat sparse, but certainly contains all the functionality required.



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)
AhnLab V3 VirusBlock	100	5469.3		19	4175.5		21	7591.3	13	5739.0
Alwil avast!	251	2179.0		43	1845.0		56	2846.7	18	4144.9
ArcaBit ArcaVir 2005	365	1498.4	1	19	4175.5		92	1732.8	16	4663.0
Authentium Command	215	2543.9		15	5288.9		74	2154.3	11	6782.5
Avira Avira	579	944.6		14	5666.7		232	687.1	24	3108.6
BLC Win Cleaner	169	3236.3		24	3305.6		89	1791.2	34	2194.3
CA eTrust Antivirus (InoculateIT)	249	2196.5		15	5288.9		93	1714.2	19	3926.7
CA eTrust Antivirus (Vet)	256	2136.5		15	5288.9		101	1578.4	21	3552.7
CA Vet Anti-Virus	257	2128.1		16	4958.4		98	1626.7	22	3391.2
CAT Quick Heal	152	3598.2		28	2833.3		91	1751.8	26	2869.5
Doctor Web Dr.Web	228	2398.8		26	3051.3		51	3125.8	18	4144.9
Eset NOD32	105	5208.9		14	5666.7		32	4981.8	16	4663.0
Fortinet FortiClient	144	3798.1		29	2735.6		110	1449.2	14	5329.1
FRISK F-Prot Antivirus	232	2357.5		16	4958.4		80	1992.7	12	6217.3
F-Secure Anti-Virus	270	2025.7		14	5666.7		121	1317.5	22	3391.2
GDATA AntiVirusKit	695	787.0		14	5666.7		300	531.4	23	3243.8
Grisoft AVG	329	1662.4		18	4407.4		93	1714.2	15	4973.8
H+BEDV AntiVir	705	775.8		14	5666.7		23	6931.2	23	3243.8
Kaspersky KAV	239	2288.4		30	2644.5		97	1643.5	26	2869.5
McAfee VirusScan	167	3275.0		22	3606.1		83	1920.7	15	4973.8
MicroWorld eScan	497	1100.5	1	44	1803.0		191	834.6	12	6217.3
Norman Virus Control	482	1134.7		22	3606.1		180	885.6	17	4388.7
NWI Virus Chaser	237	2307.7		25	3173.4		84	1897.8	17	4388.7
SOFTWIN BitDefender	591	925.4		20	3966.7		198	805.1	18	4144.9
Sophos Anti-Virus	140	3906.7		7	11333.4		69	2310.4	17	4388.7
SR Resolution Antivirus	160	3418.3		14	5666.7		69	2310.4	16	4663.0
Symantec SAV	240	2278.9		31	2559.2		91	1751.8	29	2572.7
UNA UNA	167	3275.0		29	2735.6		131	1216.9	41	1819.7
VirusBuster VirusBuster	319	1714.5	[1]	24	3305.6		154	1035.2	24	3108.6

Doctor Web Dr.Web 4.32b

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

Having recently changed ownership, there was potential for changes in the *Dr.Web* product, for better or for worse. However, since the new owner is the active developer of the product, it is not surprising that there have not been sweeping changes. A solid performance earns the product a VB 100% award.

Eset NOD32 1.956

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

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3 VirusBlock	1	99.75%	0	100.00%	99.75%	47	98.97%	5549	63.81%	54	96.18%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	112	93.58%	15	99.36%
ArcaBit ArcaVir 2005	5	99.64%	0	100.00%	99.64%	92	98.52%	1402	85.48%	32	97.87%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	2	99.72%
Avira Avira	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.67%	11	99.78%
BLC Win Cleaner	0	100.00%	0	100.00%	100.00%	82	98.00%	1086	92.85%	101	96.39%
CA eTrust Antivirus (InoculateIT)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	0	100.00%
CA eTrust Antivirus (Vet)	0	100.00%	0	100.00%	100.00%	12	99.82%	2	99.87%	3	99.72%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	3	99.72%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	82	98.00%	1086	92.85%	101	96.39%
Doctor Web Dr.Web	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%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	157	96.65%	5648	61.57%	87	97.55%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.72%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	1	99.98%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	20	99.51%	257	85.97%	27	98.56%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.67%	7	99.90%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	1	99.75%	0	100.00%	99.75%	0	100.00%	0	100.00%	3	99.79%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	180	91.24%	6	99.66%
NWI Virus Chaser	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	1	99.82%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	34	99.12%	6	99.73%	22	99.23%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	0	100.00%	15	99.30%
SR Resolution Antivirus	0	100.00%	3	0.00%	99.24%	2	99.93%	1015	88.95%	14	99.63%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
UNA UNA	32	93.05%	3	0.00%	92.35%	1914	54.54%	14266	20.19%	517	75.89%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	98	92.78%	13	99.31%

With its usual admirable performance, *NOD32* once again leaves little room for comment and achieves its latest VB 100% award with predictable ease.

Perhaps a revamp of the product's GUI is in order, complete with Easter egg functionality for those reviewers at a loss for sensible comment.

Fortinet FortiClient 1.2.1134

ItW Overall	100.00%	**Macro**	96.65%
ItW Overall (o/a)	100.00%	**Standard**	97.55%
ItW File	100.00%	**Polymorphic**	61.57%

Although still often tricked by polymorphic samples,

FortiClient continues to improve its performance in other areas. Now that VB 100% status looks to be achievable by the product on a regular basis, it seems likely that the developers will be pushed towards working on the matter of detecting those polymorphics.

FRISK F-Prot Antivirus 3.16 a

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	99.96%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	100.00%

Matters with *F-Prot* were much the same as ever, even down to the miss of W32/Nimda in its .EML form, due to the decision not to scan such files on access. This is clearly a decision that has been based upon speed of scanning being regarded as an important feature, since large email files will by their nature be most scanners' worst nightmare.

F-Secure Anti-Virus 5.43

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	99.24%	**Standard**	99.98%
ItW File	100.00%	**Polymorphic**	100.00%

F-Secure Anti-Virus seemed something of a changed product this month, in comparison with its performance on other platforms. On several occasions the test machine blue-screened on boot, though on the occasions when a blue screen did not occur, the product was working at close to its usual level of efficiency. There were, however, misses on some of the newer worms in the test set, which denied *FSAV* a VB 100%.

GDATA AntiVirusKit 14.1.

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

It came as something of a surprise when *AVK* delivered two blue screens while on-access scanning was in progress. The problem seemed to be dissipated when logging was disabled, though admittedly the sample set was not large enough to make definite pronouncements.

Despite this momentary excitement, detection was as good as usual and a VB 100% was the due reward for *GDATA*.

Grisoft AVG 7.0.290

ItW Overall	100.00%	**Macro**	99.51%
ItW Overall (o/a)	100.00%	**Standard**	98.56%
ItW File	100.00%	**Polymorphic**	85.97%

With *AVG* version 7 now firmly in place, all momentary problems from interface changes are well and truly over. The result is a product which is simple to review and, rather more happily for the developers, gains another VB 100%.

H+BEDV AntiVir 6.29.00.03

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.90%
ItW File	100.00%	**Polymorphic**	99.67%

Much like its progeny, *Avira*, *H+BEDV* performed amply well enough to receive a VB 100% award. The future of *H+BEDV* is something of a mystery though – will it remain as a free product or will it be subsumed by *Avira*? Only time will tell.

Kaspersky KAV 5.0.277

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

Kaspersky seems, in this latest version, to have removed the emission of annoying noises by default upon virus detection. Deprived of this perennial complaint, I shall be forced to revert to commenting on more technical matters. The product behaved impeccably and gained a VB 100% award.

McAfee VirusScan 8.0.0 4415

ItW Overall	99.75%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.79%
ItW File	99.75%	**Polymorphic**	100.00%

Usually a stalwart on the matter of detections, it came as something of a surprise when *VirusScan* failed to detect one of the newer worms in the test set. With the multitudes of such creations produced each day, such a miss is not

surprising on occasion, though the developers at *McAfee* will not, I suspect, take a great deal of comfort from this fact.

MicroWorld eScan 1.2.7

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

Since *eScan* is based on *AVK*, it was of interest to see whether the unusual behaviour displayed by *AVK* in this test would be repeated. There were no blue screens here, however – making *AVK*'s problem even more perplexing. As a problem of its own, *eScan* produced a false positive in the clean sets. This effectively denied the product a VB 100%

Norman Virus Control 5.7.0

ItW Overall	100.00%	**Macro**	99.95%
ItW Overall (o/a)	100.00%	**Standard**	99.66%
ItW File	100.00%	**Polymorphic**	91.24%

As with several other products in the test, *Norman*'s sole weakness lies in the polymorphic test set. This seems rather strange, since *Norman* does have available some much-vaunted heuristic techniques.

Despite this weakness, however, good detection rates and a lack of false positives combined earn *NVC* a VB 100% on this occasion.

NWI Virus Chaser 5.0

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

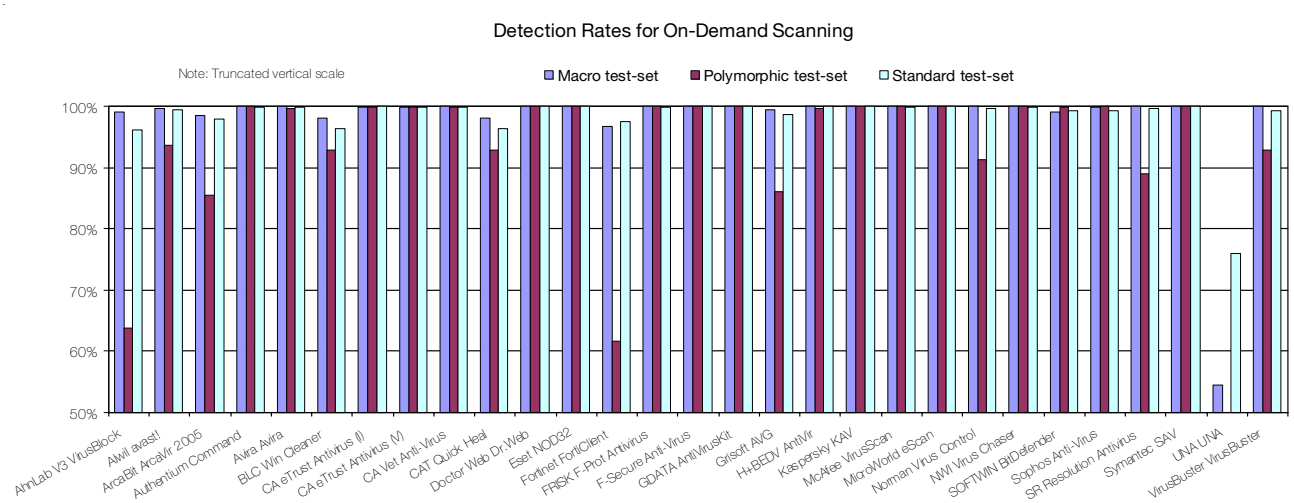
As a rebadged version of *Dr.Web*, the excellent detection rates of this product come as no surprise.

The overbearing rigidity of the user interface, however, makes it unpleasant to use. One good feature, though, is that, unlike *Dr.Web*'s interface, it is possible to change on-access settings without rebooting the machine. It is possible, however, that this is simply due to the more limited changes available.

SOFTWIN BitDefender 8.0.137

ItW Overall	100.00%	**Macro**	99.12%
ItW Overall (o/a)	100.00%	**Standard**	99.23%
ItW File	100.00%	**Polymorphic**	99.73%

Although currently rather annoyed by the fact that parts of their program have been declared spyware by *Microsoft*, the developers at *SOFTWIN* should at least be consoled by the fact that a solid performance by the *BitDefender* product this month has earned them a new VB 100% award to place upon their virtual mantelpiece.



Sophos Anti-Virus 3.88.0

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Standard**	99.30%
ItW File	100.00%	**Polymorphic**	100.00%

Sophos Anti-Virus produced all but identical results to those it has produced in the previous tests. A VB 100% was thus awarded. After a burst of welcome improvements to the product in the middle part of 2004 it remains to be seen whether the improvements continue in 2005.

SR Resolution Antivirus

ItW Overall	99.24%	**Macro**	99.93%
ItW Overall (o/a)	97.05%	**Standard**	99.63%
ItW File	100.00%	**Polymorphic**	88.95%

This rebadged *Panda* product fared reasonably well in most aspects. Floppy scanning, however, was either ineffective on access, or ineffective and caused the program to shut down while producing large error warnings. Non-floppy scanning was better, though with extensionless and PIF files remaining unscanned on access, there is room for easy improvement here.

Symantec SAV 9.0.0.338

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

Having harped on somewhat about the slowness of scanning in previous *Symantec* tests I embarked on some limited experiments on this occasion. By disabling the screen updates for scanning progress and all requirements to process files after scanning, the delays during scanning were banished completely. It seems, therefore, that any slowness is at least partially GUI-related rather than an issue with the engine itself. These matters enlivened the otherwise predictable arrival of another VB 100% for *Symantec*.

UNA UNA 1.83

ItW Overall	92.35%	**Macro**	54.54%
ItW Overall (o/a)	16.67%	**Standard**	75.89%
ItW File	93.05%	**Polymorphic**	20.19%

On this occasion *UNA* certainly wins the prize for the most disparate set of results on access and on demand. Although the statistics show great differences, the underlying details were even more perplexing. The number of potential variables here makes hazarding an explanation rather futile.

VirusBuster VirusBuster 4.7.22

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.31%
ItW File	100.00%	**Polymorphic**	92.78%

With a suspicious file in the clean sets, *VirusBuster* teetered perilously close to missing out on a VB 100%. The file was not declared to be viral, however and so full detection in the ItW sets was ample to earn *VirusBuster* a further VB 100%.

CONCLUSION

The results from this test brought two totally unrelated thoughts to my mind. The first is the nature of the test sets. The increase in very similar worm additions to the WildList, identified by checksums rather than names, is the result of a vast flood of similar files entering into circulation. Detecting these files is not usually an issue – a good archive-handling engine is a great help, admittedly, but by and large they are not a massive challenge. Gathering these files is, however, much more of an issue – the burden upon the developers is ever more veering towards a logistic problem rather than a detection challenge.

The second thought relates to the nature of older platforms. On *XP* I very rarely see any problems with anti-virus programs. The reasons for this are probably split between extra development effort being expended on this platform and the rather more robust *XP* structure. With *NT,* however, there were several occasions where products simply curled up and died in a sea of blue. Overcoming such problems on an aged platform, while not breaking newer platforms, is a challenge that will give coders a few sleepless nights.

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/2005/test_sets.html.

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

ERRATA: FEBRUARY 2005 WINDOWS NT COMPARATIVE REVIEW

Virus Bulletin regrets that the *Windows NT Workstation* comparative review published in the February 2005 issue of *VB* (see *VB*, February 2005, p.12) contained two errors.

First, *AhnLab V3 VirusBlock* was noted as having missed a single file in the In the Wild (ItW) test set. However, the apparent miss proved to have been caused by an error in the parsing of the product's log files. *V3 VirusBlock* is thus owed a VB 100% award.

Secondly, *F-Secure Anti-Virus 5.43* was noted as having missed several files in the ItW test set. However, subsequent investigation indicated that the product's update process had not completed before the test. After further testing, allowing longer delays after updating, all ItW files were detected. *F-Secure Anti-Virus* is thus entitled to a VB 100%.

Virus Bulletin apologises for the errors and points readers to http://www.virusbtn.com/vb100/about/ for an up-to-date summary of the results of recent comparative reviews.