COMPARATIVE REVIEW

WINDOWS XP PROFESSIONAL

Matt Ham

This month we revisit *Windows XP*. The last *XP* review (see *VB*, June 2002, p.16) was the first time the current testing machines were employed. Since both operating system and hardware were identical to a previous, fairly uneventful, comparative, this review seemed likely to go ahead without major hitches. Sure enough, the number of problems encountered with the products was at an all-time low. It is almost unheard of for no product to have caused the machines to freeze or crash. The greatest hurdle in this review was the sheer number of products on offer: 25 in all.

AhnLab V3 VirusBlock SP2

ItW Overall	99.96%	**Macro**	97.76%
ItW Overall (o/a)	99.96%	**Standard**	86.29%
ItW File	99.96%	**Polymorphic**	44.63%

As far as detection was concerned, *V3* was very mixed in its performance. *V3*'s detection of polymorphics was relatively poor, though detection of samples in the standard and macro test sets was good, if not astounding. Detection of ItW viruses is clearly the developer's primary concern, with detection here being all but perfect. However, the default engine settings did not allow detection of the extensionless copy of O97M/Tristate.C in this test set. This was sufficient to disbar *V3* from a VB 100% award. On the clean test set the results were much better. No false positives were generated in the clean sets and the scan rate on the non-archived files was at the fast end of the scale. Scanning of archives is not enabled by default and was slower.

Alwil avast! 4.0 Professional 4.0.208

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.57%
ItW File	100.00%	**Polymorphic**	91.21%

Alwil's developers have been hard at work recently, producing new features and entire new products. This has not prevented them from applying their time to the *XP* platform, however. *avast!* has a new appearance, the giant looming beetles of old having been replaced by a more conventional look. However, the new look did not seem to affect detection. Although there were slightly more missed detections on demand than on access, detection rates were perfect for viruses in the ItW test set. This, combined with the fact that no false positives were generated on the clean sets, earns *Alwil* a VB 100% award.

One problem was encountered during the testing of *avast!* Despite being set to overwrite and delete infected files, it seems that *avast!* is configured to back up all files in the Virus Chest. This should not prove a problem on a real-world machine – although, drive capacity seemed not to be checked, which led rapidly to the usage of all space on the partition where *avast!* was installed. This slowed down processing of files considerably, but was easily remedied, by deleting the archived infected files manually.

CAT Quick Heal X Gen 6.09

ItW Overall	100.00%	**Macro**	97.54%
ItW Overall (o/a)	100.00%	**Standard**	80.67%
ItW File	100.00%	**Polymorphic**	91.08%

Quick Heal has a tendency towards better detection of more recent viruses or those which are currently in the wild. This selectivity is commonly associated with a fast throughput rate for clean files, as was indeed the case for *Quick Heal*. With such selectivity the chance of false positives is reduced – *Quick Heal* generated none. With complete detection of viruses in the ItW test set, a VB 100% is netted by *CAT*.

Returning to old woes, the report files produced by *Quick Heal* were brimming with annoyances. In common with several other companies the report was in 8+3 format rather than using long file names. Rather more annoyingly, the logs also had extensions which changed case randomly, despite the names of all the test samples being upper case. Quite what is the reasoning behind such changes is anyone's guess; they certainly do not seem helpful under any circumstance that I can imagine.

Command AntiVirus for Windows 4.80.3

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.78%
ItW File	100.00%	**Polymorphic**	95.21%

Command AntiVirus proved its usual friendly self as far as testing was concerned, although the logging proved as intractable as ever. Logs were available only in rtf format, which is impenetrable to the scripts that are used for processing plain-text files. In such cases logs can often be obtained by choosing to print the log from within the program and diverting the printer output to a text file. However, this method resulted in a very truncated report and deletion of infected files was used to obtain results. When the results were processed there were few surprises. The misses were dominated by a selection of polymorphics, with W32/Heidi.A being missed only on access in its archive embedded form. None of the misses were within the ItW test set or the macro test set. When scanning clean files, *Command AntiVirus* proved to be among the faster products, especially on OLE files. With no false positives, the third VB 100% award of this review goes to *Command*.

Computer Associates eTrust Antivirus 7.0.139

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

Although an old-timer in the *VB* Comparatives, this was the first test for version 7 of *eTrust* on *Windows XP*. The new version had one major advantage as far as installation was concerned, in that only one update file was needed rather than the accumulation of patches required in the past. Detection rates for *eTrust* were also good. No files were missed in the ItW test set and, combined with no false-positives in the clean set, another VB 100% award is earned by *CA*. *eTrust*'s scanning rates were at the more speedy end of the scale.

Computer Associates Vet Anti-Virus Protection 10:58.0.3

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

Vet has a history of ease of installation and testing which was displayed again in this test. *Vet* is unusual in that it still supplies updates on floppy disk, in addition to the main CD media – most other products rely on the user to obtain electronic updates on first installation. *Vet's* performance on the clean test set was good, with fast overall scanning speed and no false positives. There were no misses in the ItW test set, meaning that *Vet Anti-Virus* gains another VB 100% award.

DialogueScience Dr.Web for Windows 95-XP 4.29c

ItW Overall	99.52%	**Macro**	100.00%
ItW Overall (o/a)	99.52%	**Standard**	100.00%
ItW File	99.51%	**Polymorphic**	100.00%

DialogueScience suffered a rare miss of a VB 100% award in last month's *Linux* tests, in which W95/Bodgy.A proved

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	1	99.96%	0	100.00%	99.96%	95	97.76%	8830	44.63%	304	86.29%
AlwilI avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	157	91.18%	13	99.57%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	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 Quick Heal	0	100.00%	0	100.00%	100.00%	104	97.51%	0	100.00%	718	62.15%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	91	95.21%	11	99.64%
DialogueScience Dr.Web	5	99.51%	0	100.00%	99.52%	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	0	100.00%	0	100.00%	100.00%	0	100.00%	4	99.82%	4	99.73%
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%	35	97.61%	3	99.70%
Ggreat ZMW32	-	-	-	-	-	-	-	-	-	-	-
Grisoft AVG	0	100.00%	0	100.00%	100.00%	23	99.44%	425	83.72%	43	97.44%
HAURI ViRobot	0	100.00%	0	100.00%	100.00%	43	98.84%	10795	33.63%	530	73.69%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	4	99.70%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	178	91.27%	11	99.64%
NTW Virus Chaser	5	99.51%	0	100.00%	99.52%	0	100.00%	0	100.00%	5	99.61%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	17	99.59%	45	95.11%	72	97.57%
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%	215	95.77%	7	99.84%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	159	89.13%	11	99.55%

to be a bugbear for the product. Discussions with the product's developers revealed that all samples received by *DialogueScience* had been non-replicable and therefore the virus had been classified as an intended threat, rather than an actual threat. With a very short span of time between the *Linux* and *XP* tests, this hitch was redressed the day after

the submission deadline for this review – not quite in time to be reflected in these results. Thus *Dr.Web* missed the offending samples of W95/Bodgy.A in this test and miss out on a VB 100% award as a result. Newer versions of the software do not have this problem.

In other respects the product performed admirably, with fewer suspicious files than usual occurring in the clean test set. The on-access scan did show some slight quirks, however – it seemed that files containing embedded information bypassed the 'automatic action setting' and required user intervention. Since there are few of these files in the test set, this was only a momentary distraction.

Eset NOD32 Anti-virus 1.405

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

It seems that the developers of several products have opted for a change in interface. *NOD32* is no exception. The version reviewed was noted as being the last in its current form – the alien-esque imagery being consigned to history. With this impending change it seemed likely that the current version would be subject to a freeze in features and development, and indeed its appearance was identical to that which it has had for the last two years or so. *NOD32*'s performance was also all but identical to its past performances: fast scanning, no false positives and full ItW detection combining to earn *NOD32* yet another VB 100% award.

FRISK F-Prot Antivirus 3.13a

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.73%
ItW File	100.00%	**Polymorphic**	99.82%

Before reporting on *FRISK*'s performance, a comment about last month's *Linux* comparative (see *VB*, May 2003, p.20). In the *Linux* comparative it was stated that the *F-Prot Antivirus* on-access scanner scans only HTTP GET requests. This statement was incorrect, having been the result of a misinterpretation of the documentation. The product is currently undergoing re-testing in consultation with the developers.

Back to the current tests and no problems were apparent for *F-Prot Antivirus*. The product ran quickly through the clean set scans without incident or false positives of any sort. With less than a dozen misses overall, none of which were in the ItW test set, *F-Prot Antivirus* qualifies for a VB 100% award.

F-Secure Anti-Virus 3.12.410

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

Since it incorporates the *F-Prot* engine, the fact that *FRISK*'s product earned a VB 100% boded well for *F-Secure*'s performance – the inclusion of *Kaspersky*'s engine being an additional line of defence. Sure enough, detection rates were similar, though slightly improved by the additions inherent in *F-Secure*'s multi-engined product. There was, however, an oddity in the *F-Secure* scan settings. Despite being set to leave all infected files and simply log results, several disinfected files were left after scanning was completed. Test sets are refreshed from images after each scan has been performed, so the results cannot be affected by such behaviour, but this activity certainly rates as unexpected. As mentioned, detection rates were good, with only a handful of misses, none of which were in the ItW test set. Scanning speeds on clean files were respectable, and no false positives were seen. As a result, *F-Secure Anti-Virus* is the recipient of a VB 100% award.

GDATA AntiVirusKit Professional 12.0.4

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

AntiVirusKit is, like *F-Secure Anti-Virus*, a multi-engined beast and it too features *Kaspersky* technology – this time alongside the *RAV* engine. This pairing performed well in detection, with one sample of W32/Etap being the only miss across all the test sets. No false positives were generated in the clean test sets, thus *AVK* achieves a VB 100%. The double layer of detection does not come without a price, however. *AVK*'s scanning speed was slower than the average by a considerable degree, most noticeably on the executable test sets.

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**	97.61%

Misses for *RAV* were again few in number, although W32/Etap was undetected in this case, rather than partially detected. None of the files that were missed were in the ItW test set,

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	99.96%	0	100.00%	99.96%	95	97.76%	8830	44.63%	304	86.29%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	153	91.21%	13	99.57%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	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 Quick Heal	0	100.00%	0	100.00%	100.00%	101	97.54%	1543	91.08%	367	80.67%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	91	95.21%	8	99.78%
DialogueScience Dr.Web	5	99.51%	0	100.00%	99.52%	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%	4	99.82%	4	99.73%
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%	35	97.61%	2	99.88%
Ggreat ZMW32	99	83.67%	9	0.00%	82.29%	1550	62.90%	14737	10.37%	525	74.31%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	20	99.51%	257	85.97%	22	99.21%
HAURI ViRobot	0	100.00%	0	100.00%	100.00%	43	98.84%	10795	33.63%	530	73.69%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.92%	0	100.00%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	4	99.70%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	178	91.27%	9	99.76%
NTW Virus Chaser	5	99.51%	0	100.00%	99.52%	0	100.00%	0	100.00%	0	100.00%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	17	99.59%	45	95.11%	62	97.93%
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%	215	95.77%	7	99.84%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	4	99.90%	160	89.13%	9	99.64%

however. Clean set scanning proved *RAV* to be slightly slower than the average, with a default setting of archives remaining unscanned. However, there were no false positives, and *RAV* adds to its collection of VB 100% awards. Despite an admirable performance as far as detection was concerned, there were some peculiarities with

the product's interface. Whenever launched the software reverted to its simple configuration, rather than the advanced interface that had been selected. This was probably related to a number of error messages that appeared on launching the program – problems appeared to be related to configuration rather than engine difficulties and certainly did not impair scanning performance.

Ggreat ZMW32 Virus Scan M7.5+

ItW Overall	82.29%	**Macro**	62.90%
ItW Overall (o/a)	n/a	**Standard**	74.31%
ItW File	83.67%	**Polymorphic**	10.37%

Ggreat's *ZMW32* remains the only program in this review with no on-access component in the traditional sense. It does contain amail and http filters which operate in real time, although these do not fall under the functionality tested in these comparatives. The rather spartan command set proved a slight hindrance to testing: files may only be disinfected, there being no option to delete. The program has seen much improvement since its earlier versions were reviewed – on previous occasions the product suffered from general instability and logging did not appear to work fully. These problems now seem fully solved.

Detection rates saw an improvement too – although there was a certain degree of unpredictability. The test sets were scanned several times with slightly different results being obtained on each occasion. In the end disinfection was used repeatedly and a log taken of those files still noted as infected. Disinfected files, counted as detections, were discovered by the use of CRCs. All in all, the product has improved, though it still has a long way to go until it can qualify for a VB 100%.

Grisoft AVG Anti-Virus System 6.0.478 275

ItW Overall	100.00%	**Macro**	99.51%
ItW Overall (o/a)	100.00%	**Standard**	99.21%
ItW File	100.00%	**Polymorphic**	85.97%

Grisoft's *AVG* is another of those products which continue to put in stalwart performances. Misses were, as usual, mostly in the polymorphic test sets, with a small number in the standard and macro test sets. However, no misses were noted in the ItW test set. In the clean set *AVG* found five suspicious files, but there were no outright declarations of infection, thus *AVG* achieves a VB 100% award.

In the *Windows 2000 Advanced Server* comparative (see *VB*, November 2002, p.16) *AVG* was noted to have missed an ItW sample of W32/Zoek.D (in addition to one other file which denied the product a VB 100% award). Investigation has since shown the Zoek file to be a dropped backdoor portion of the virus, rather than an infective object. As a result, the file has been removed from the test sets and *AVG* should not have been logged as missing W32/Zoek.D.

HAURI ViRobot Expert 4.0

ItW Overall	100.00%	**Macro**	98.84%
ItW Overall (o/a)	100.00%	**Standard**	73.69%
ItW File	100.00%	**Polymorphic**	33.63%

The last time *HAURI*'s *ViRobot* appeared in a comparative review, the product was among the speedier entrants in the clean test sets, and the state of affairs this time was much the same. It was noted on the last occasion that the product's speed could, in part, be attributed to *ViRobot*'s non-detection of a number of older viruses. The same lack of detection of older viruses was seen this time, with large numbers of the polymorphic viruses being missed en masse. Despite these misses, *ViRobot* performed well on newer viruses and missed none of the samples in the ItW test set. In the clean sets one suspicious file was noted, though it was not declared infected, and thus *HAURI* is awarded a VB 100%.

Kaspersky Anti-Virus 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**	99.92%

Kaspersky Anti-Virus (*KAV*) was tested with high hopes for good detection rates. Sure enough, just the one missed sample of W32/Etap was noted (the same sample that was missed by *GDATA*'s product).

However, the impressive detection rate was rather spoiled by the presence of a false positive in the clean test sets. The problem file was declared to be a rebooting Trojan – in fact it is designed as a rebooting utility. The old adage (in computer terms at least) that renaming format would be enough to make it a Trojan, is brought to mind. Although this was an understandable misdiagnosis on the part of *Kaspersky Anti-Virus*, it was sufficient to deny a VB 100% award on this occasion.

MicroWorld Services eScan 2003 10.1.02 (2.6.198.6)

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

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	35	15626.6		11	7212.2		134	1189.7	28	2664.6
Alwil avast!	112	4883.3		24	3305.6		64	2490.9	21	3552.7
CA eTrust Antivirus	94	5818.4		4	19833.4		43	3707.4	8	9325.9
CA Vet Anti-Virus	77	7103.0		5	15866.8		50	3188.3	10	7460.7
CAT Quick Heal	56	9766.6		12	6611.1		44	3623.1	13	5739.0
Command AntiVirus	103	5310.0		4	19833.4		49	3253.4	5	14921.5
DialogueScience Dr.Web	226	2420.1	[12]	14	5666.7		84	1897.8	15	4973.8
Eset NOD32	27	20256.7		3	26444.6		27	5904.3	6	12434.6
FRISK F-Prot	102	5362.1		5	15866.8		57	2796.8	6	12434.6
F-Secure Anti-Virus	208	2629.5		8	9916.7		118	1351.0	18	4144.9
GDATA AntiVirusKit	457	1196.8		12	6611.1		209	762.8	26	2869.5
GeCAD RAV	276	1981.6		5	15866.8		130	1226.3	5	14921.5
Ggreat ZMW32	29	18859.7	4	18	4407.4		2070	77.0	400	186.5
Grisoft AVG	57	9595.3	[5]	7	11333.4		60	2656.9	12	6217.3
HAURI ViRobot	35	15626.6	[1]	21	3777.8		81	1968.1	27	2763.2
Kaspersky KAV	188	2909.2	1	12	6611.1		110	1449.2	30	2486.9
MicroWorld eScan	149	3670.7		18	4407.4		90	1771.3	30	2486.9
NAI VirusScan	105	5208.9		14	5666.7		72	2214.1	18	4144.9
Norman Virus Control	190	2878.6		8	9916.7		103	1547.7	12	6217.3
NTW Virus Chaser	139	3934.8	[12]	8	9916.7		58	2748.6	10	7460.7
SOFTWIN BitDefender	862	634.5	[1]	6	13222.3		416	383.2	17	4388.7
Sophos Anti-Virus	69	7926.6		9	8814.9		38	4195.2	11	6782.5
Symantec AntiVirus	138	3963.3		20	3966.7		59	2702.0	21	3552.7
Trend PC-cillin	77	7103.0		4	19833.4		43	3707.4	12	6217.3
VirusBuster VirusBuster	170	3217.2		7	11333.4		105	1518.3	14	5329.1

eScan is yet another product that is derived from third-party engines – this one being a derivative of the *GDATA* product, which, in turn, incorporates the *Kaspersky* and *RAV* engines. What was surprising about *eScan* lay in the matter of scanning speeds on the clean test sets. In most cases, the further from the ultimate source of the engine, the slower the product becomes. In this case, however, scanning speeds were faster than for any of the other products involved. On the less positive side, however, the detection of boot sector

viruses on access was (although complete eventually) rather a hit and miss affair. Detection rates for *eScan* were identical to those seen in the *GDATA* product, as was the lack of false positives in any clean set. In combination, this performance was sufficient to gain *eScan* a VB 100%.

NAI VirusScan Enterprise 7.00 4.2.40 4261

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.70%
ItW File	100.00%	**Polymorphic**	100.00%

NAI was notable by its absence in last month's *Linux* review and makes a welcome return this month. It should be pointed out that *NAI*'s lack of submission in last month's review was a result of a combination of errors on the part of both *VB* and *NAI*, rather than a deliberate absence from the testing line-up on the part of the developer. This month the review process for *VirusScan* started smoothly enough, although initial scanning tests were thwarted by the non-appearance of logs if the default log location and name were used. Changing these resolved the problem, and scanning progressed unhindered. No false positives were noted on the clean set tests, while scanning rates remained around the average. Misses of infected files were limited to the archived versions of W32/Heidi.A and the now defunct JS/Unicle. This performance was sufficient to earn *VirusScan* a VB 100% award.

New Technology Wave Inc. Virus Chaser 5.0

ItW Overall	99.52%	**Macro**	100.00%
ItW Overall (o/a)	99.52%	**Standard**	100.00%
ItW File	99.51%	**Polymorphic**	100.00%

Virus Chaser is another rebadged product – in this case *DialogueScience* is the engine developer. The product's detection rates and behaviour in the clean sets were all but identical to those exhibited by *Dr.Web*. Unfortunately this included the missed samples of W32/Bodgy.A and thus *Virus Chaser* does not obtain a VB 100% award this month.

Norman Virus Control 5.50 5.40.42

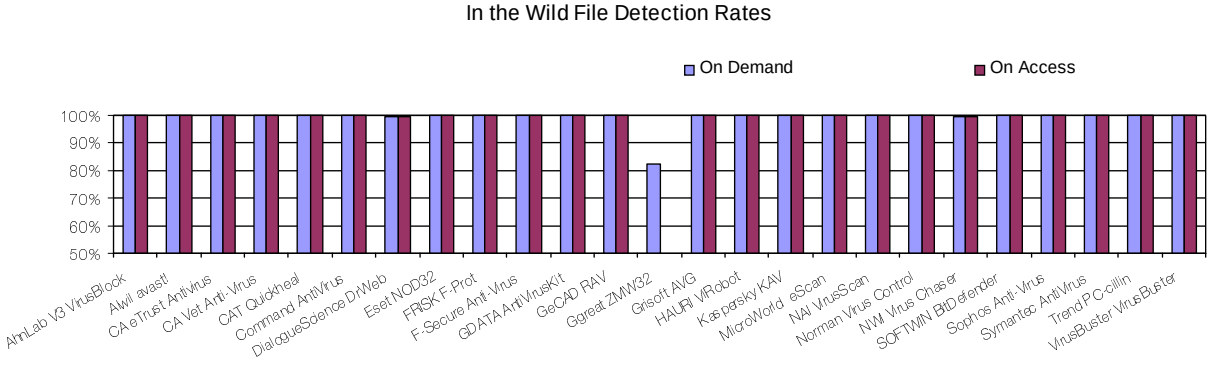
ItW Overall	100.00%	**Macro**	99.95%
ItW Overall (o/a)	100.00%	**Standard**	99.76%
ItW File	100.00%	**Polymorphic**	91.27%

Norman Virus Control has been notable over the last year for its changing log file status. Configurations have moved through no logs, logs of both missed and detected files, and have now stabilised at logs of infected files only. The log files proved easy enough to parse in this form and showed *NVC* to have strong detection rates against all but some modern polymorphics, none of which have yet entered into the ItW test set. The clean set files were scanned without any problems or false positives, thus *NVC* earns a VB 100% award. *NVC* suffered the same problem in last month's *Linux* comparative as *AVG* suffered in the previous review: *NVC* should not have been logged as having missed W32/Zoek.D. However, the lack of an on-access scanner means that *NVC* still did not qualify for a VB 100%.

SOFTWIN BitDefender Standard Edition 7 72112

ItW Overall	100.00%	**Macro**	99.59%
ItW Overall (o/a)	100.00%	**Standard**	97.93%
ItW File	100.00%	**Polymorphic**	95.11%

BitDefender has had a few ups and downs in its performance over the years. On this occasion the product showed perfect detection of ItW samples in addition to good detection rates in the other test sets. There was only one disappointment, this concerning the speed of scanning. Although by no means



the worst upon OLE files or zipped executables, the scanning rate of non-archived executables was sluggish. No false positives were obtained, however, and thus *BitDefender* earns a VB 100% award.

Sophos Anti-Virus 3.69

ItW Overall	100.00%	**Macro**	99.73%
ItW Overall (o/a)	100.00%	**Standard**	99.31%
ItW File	100.00%	**Polymorphic**	95.79%

Sophos Anti-Virus has, in the past, lagged somewhat behind the pack in fully-automated daily update technology and currently its developers are working on various projects to lessen this gap. It was therefore a happy surprise to be presented with a new option for updating the product, in the form of an executable file. However, it was merely a self-extracting zip file, rather than an updating tool as such – it was still necessary to position the update files by hand and to restart the *Sophos Anti-Virus* application. With this process complete, the application performed in its usual smooth fashion. Results were good, with perfect detection of ItW files and misses elsewhere comprising a selection of files which have been missed more or less constantly for several months. With no false positives, and a fairly speedy rate of scanning, *Sophos* takes home a VB 100% award.

Symantec AntiVirus Corporate Edition 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%

Symantec AntiVirus did not disappoint on this occasion. With no false positives and full detection of all files in the ItW test set a VB 100% award is earned. There was one less than ideal feature of the product, however. On samples of W32/CTX and W32/SK variants the scanning speed was very slow indeed, with delays of several seconds between the scanning of some files. This is not a problem which is exhibited on clean files, however, so is more than likely a side-effect of the fact that exact virus identification is regarded as important by the developers.

Trend Micro PC-cillin 2003 10.02 1072

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.84%
ItW File	100.00%	**Polymorphic**	95.77%

Where detection was concerned, *PC-cillin*'s misses were confined exclusively to various polymorphic viruses, including some which are also located within the standard test set. On-access scanning revealed one rather bizarre piece of behaviour – after a short time the display became rather garbled in those areas where screen refreshes were not being forced. However this seemed to affect neither the performance of *PC-cillin* nor that of other applications on the machine. Performance in both detection and the clean set tests was ample for *Trend* to gain a VB 100% award.

VirusBuster VirusBuster for Windows Antivirus Solution 4.2 build 16

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	99.64%
ItW File	100.00%	**Polymorphic**	89.13%

VirusBuster displayed few faults or pieces of outstanding behaviour. The test procedures all ran smoothly, with no untoward false positives in the clean set, and misses of infected samples were mostly among the polymorphic samples. There was a smattering of misses in the macro test set, but none in the ItW set. *VirusBuster* deservedly gains a VB 100% award.

CONCLUSION

In comparison with the non-*Windows* test of the last comparative reivew, this month's results show a large number of VB 100% awards being achieved.

Of course, *Windows XP* is sufficiently similar to *NT* that lessons learned on products for that platform have helped in the smooth production of products for *XP*. What remains to be seen, however, is whether those lessons are specific to the architecture or whether they can be applied more generally within any *Microsoft*-designed environment. The answer to that question will come in due course, when 64-bit *Windows* operating systems move from being strapped-on afterthoughts to mainstream platforms in their own right. How soon that will be is anyone's guess, but the tests should make for interesting reading.

Technical details:

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-Rom and 3.5-inch floppy drive running *Windows XP Professional*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/WinXP/2003/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.