COMPARATIVE REVIEW

WINDOWS XP PROFESSIONAL

Matt Ham

Another *Windows* platform sees a collection of the usual suspects ready to be put to the test – 25 products were submitted for this month's *Windows XP* review. The recent *Windows NT 4* comparative (see *VB*, February 2004, p.12) saw all but one of the same products submitted, the odd man out being *NWI*'s *Virus Chaser*. With such a recent test on a similar platform, only a small number of technical problems was expected, and indeed all products proved to be testable both on access and on demand. That is not to say that performances were perfect – but the vast majority of niggles were related to design, rather than application.

TEST SETS

Changes to the test sets this month were limited to the addition of samples to the In the Wild (ItW) test set – though this was quite enough replication for one review. Rather than the usual 10 or 20 additions to the list, there were in excess of 60 on this occasion. The majority of these were samples of W32/Bagle and W32/Netsky. Smaller numbers of W32/Mydoom, W32/Dumaru, W32/Mimail and W32/Sober were also added, together with the usual collection of viruses which do not occur in a plethora of versions and varieties. The test sets were aligned with the Real Time WildList as of 5 May 2004, with the products being supplied on 7 May 2004. With new versions of viruses entering the WildList close to the deadline, this might have been expected to cause problems for a few products.

AhnLab V3 VirusBlock 2005 IS

ItW Overall	99.67%	**Macro**	98.28%
ItW Overall (o/a)	99.67%	**Standard**	85.53%
ItW File	99.67%	**Polymorphic**	44.99%

VirusBlock was notably fast on scanning the clean executable test set, the throughput here being the highest of the products tested this month. Log files were the most irritating aspect of the review process for this product, coupled with an inability to block file access effectively during the on-access testing. *VirusBlock* failed to reach the grade for a VB 100% award, having missed the .HTM sample of W32/Lovelorn.A.

Alwil Avast! 4.1.399

ItW Overall	99.67%	**Macro**	99.56%
ItW Overall (o/a)	99.67%	**Standard**	99.36%
ItW File	99.67%	**Polymorphic**	93.58%

As is often the case with *Avast!*, the creation of files in the virus vault area caused a considerable slowdown during on-access scanning. This appears to be due to the number of files created – in excess of 4,000 – and the deletion of these files quickly restored the speed of file access. Despite coming close to a VB 100% award, *Alwil*'s product fell short by one file – the .HTM sample of W32/Lovelorn was missed from the ItW test set. The DLL version was also missed, though this is present only in the standard test set, being a non-executable encoded version of the worm, rather than a true DLL.

Authentium Command Anti Virus 4.91.0

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	99.91%

The performance of *Authentium*'s product remains solid, with little to fault it. Misses were of the single samples of W32/Fosforo and W32/Zmist.D, both of these being members of multiple sets of the respective polymorphic file infectors. Lack of scanning within archives and non-executable files on access caused some minor misses in the standard test set, but no misses of ItW samples, leaving *Command* with a VB 100% award for its trophy cabinet.

CA eTrust Antivirus 7/0.0402 23.65.11

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	99.89%

eTrust is notable for its rate of scanning OLE files, both archived and in their raw state. Although *Eset*'s *NOD32* is speedy where the uncompressed versions are concerned, *eTrust* has a marginal lead where compressed files are concerned. The log files for *eTrust* remain an abomination, saved only by the ability to log the thankfully very few missed files, rather than the detected samples. Despite continuing to miss the rather aged W97M/Pain.A macro virus, detection is good and certainly sufficient to lead to a new VB 100% award to add to *eTrust*'s collection.

CA Vet Anti-Virus 10.63.0.1 11.5.00 8323

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

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	99.67%	0	100.00%	99.67%	75	98.28%	9163	44.99%	305	85.53%
Alwil Avast!	1	99.67%	0	100.00%	99.67%	18	99.56%	112	93.58%	15	99.36%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	2	99.72%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	1	99.82%
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%	103	97.49%	1044	95.12%	300	83.56%
DialogueScience 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%	35	99.15%	5065	64.28%	107	96.57%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	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%	28	99.52%	522	87.18%	34	98.42%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
MicroWorld eScan	1	99.67%	0	100.00%	99.67%	0	100.00%	0	100.00%	0	100.00%
NAI McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	112	96.53%	1	99.82%
NWI Virus Chaser	1	99.89%	0	100.00%	99.89%	0	100.00%	0	100.00%	1	99.82%
SOFTWIN BitDefender	1	99.94%	0	100.00%	99.95%	13	99.69%	4	99.78%	48	98.28%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	0	100.00%	16	99.12%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend Internet Security	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	9	99.63%
UNA UNA Pro	92	81.78%	3	57.10%	81.21%	796	80.96%	14229	17.50%	682	67.79%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	102	91.45%	10	99.45%

The *Vet* product was supplied as an electronic version, rather than as a physical copy – which led to some oddities upon installation. Without an update the application will not activate scanning in any way, shape or form. Since it is claimed that only Internet updates are supported, this poses rather a problem where a secure lab is concerned. However, manually-applicable updates are available from the *Vet* website (despite claims to the contrary), so this problem was overcome. Missed samples remained exactly the same as for the last few reviews – with no misses occurring in the ItW test set, thus *Vet* earns another VB 100% award.

CAT QuickHeal X Gen 7.01

ItW Overall	100.00%	**Macro**	97.49%
ItW Overall (o/a)	100.00%	**Standard**	83.56%
ItW File	100.00%	**Polymorphic**	95.12%

Entering a somewhat predictable category, *QuickHeal* once again demonstrated a non-trivial number of misses where some mostly-ignorable viruses were concerned, while retaining good detection on more recent threats. Scanning speed was well within the middle of the pack. With no ItW misses and no false positives, *CAT* gains a VB 100 % award for its growing collection.

DialogueScience Dr.Web 4.31b

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

As has been noted on previous occasions, while only one file was flagged as suspicious in the clean sets, a number of files were flagged as suspicious when in zipped archives. The product's heuristic sensitivity is clearly finely-tuned, since the rebadged version of *Dr.Web*, *Virus Chaser*, detects all of these as suspicious, even when not in an archived state. The single file which remains suspicious to *Dr.Web* is, itself, contained within a self-extracting archive. There were few misses in detection, though they included one significant file – the .HTM sample of W32/Capside, which is in the ItW test set – thus *Dr.Web* is denied a VB 100% award by the narrowest of margins.

Eset NOD32 1.753

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

While neck-and-neck with *CA eTrust*, *NOD32* maintains its reputation for speed in the OLE test set (admittedly with only marginal time advantages over the *Trend* and *H+BEDV* products). Upon compressed executables, however, *NOD32* is comfortably the fastest product on test. Like several other products, *NOD32* does not detect the DLL-extensioned W32/Lovelorn sample, but does detect this in those samples within the ItW test set. The result, as might be suspected, is a VB 100% award for *Eset*.

Fortinet FortiClient 1.0.115

ItW Overall	100.00%	**Macro**	99.15%
ItW Overall (o/a)	100.00%	**Standard**	96.57%
ItW File	100.00%	**Polymorphic**	64.28%

FortiClient made its debut in the *VB* comparatives in a less than stellar fashion in the February 2004 *NT* test (see *VB*, February 2004, p.12). Since then, there has clearly been some feverish activity where In the Wild samples are concerned. Despite numerous misses in other test sets, *FortiClient* detected all samples in the ItW test sets this time. Such an improvement is to be applauded. However, four files in the *VB* clean test set were logged as being viruses – this being sufficient to deny *FortiClient* a VB 100% award. *FortiClient* also has the dubious honour of being the slowest scanner when faced with uncompressed clean OLE files, though its performance on archived files was far more respectable.

FRISK F-Prot Antivirus 3.14e

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	99.91%

Reaching the write-up of *F-Prot Antivirus* in a review always poses something of a problem, the rebadged *Authentium* version of the engine generally having shown identical results and thus leaving little that has not already been discussed. This is the case again on this occasion, with the award of a VB 100% being among the things *F-Prot* has in common with the *Authentium* product.

F-Secure Anti-Virus 5.52

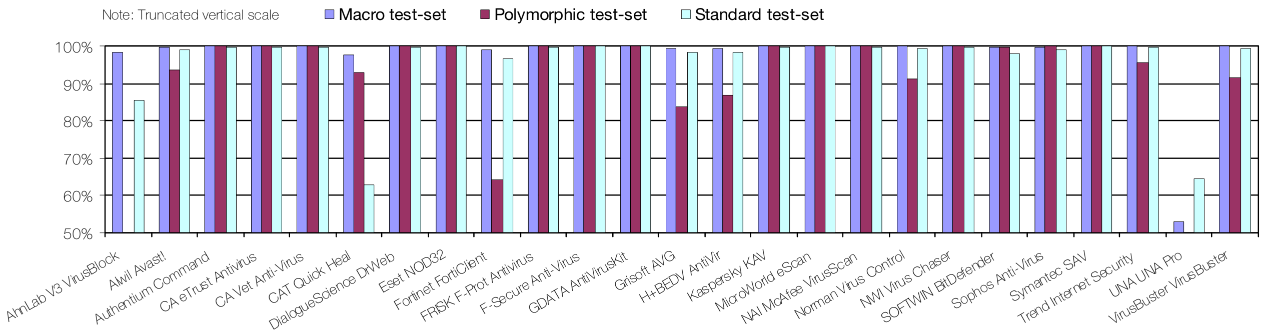
ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.98%
ItW File	100.00%	**Polymorphic**	100.00%

Like *FRISK*'s offering, if *Command* has achieved a VB 100% award it is usually likely that *F-Secure* will do so too, since all three

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	99.67%	0	100.00%	99.67%	75	98.28%	9168	44.97%	305	85.53%
Alwil Avast!	1	99.67%	0	100.00%	99.67%	18	99.56%	112	93.58%	18	99.12%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	5	99.58%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	6	99.86%	1	99.89%	4	99.51%
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%	103	97.54%	1085	92.86%	647	62.82%
DialogueScience Dr.Web	1	99.89%	0	100.00%	99.89%	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%	35	99.15%	5065	64.28%	107	96.57%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	4	99.60%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	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%	23	99.44%	757	83.64%	34	98.17%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	56	99.27%	622	86.72%	35	98.24%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	11	99.69%
MicroWorld eScan	1	99.67%	0	100.00%	99.67%	0	100.00%	0	100.00%	0	100.00%
NAI McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	180	91.24%	12	99.45%
NWI Virus Chaser	1	99.89%	0	100.00%	99.89%	4	99.90%	0	100.00%	3	99.69%
SOFTWIN BitDefender	2	99.58%	0	100.00%	99.59%	13	99.69%	4	99.78%	49	98.10%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	0	100.00%	16	99.12%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend Internet Security	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	9	99.63%
UNA UNA Pro	104	80.72%	7	0.00%	78.88%	1986	53.06%	14284	16.34%	755	64.62%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.45%	13	99.30%

products have used the *FRISK* engine for some years. However, rumour has it that it is now only the macro detection capability that is provided by *FRISK* technology within the *F-Secure* product. On this occasion, the missed files gave no evidence in either direction and a VB 100% is duly awarded.

Detection Rates for On-Access Scanning



GDATA AntiVirusKit 14.0.5

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

AVK flagged one file as suspicious – it would seem that the suspicion had been elicited by the *BitDefender* engine, since the same file was subsequently flagged by that product. The downside of using two engines was demonstrated in the scanning throughput tests, where *AVK* was among the slower products, especially on compressed files. However, the combination of scanning engines did have one major benefit: all files were detected in all test sets, thus *AVK* earns a VB 100% award for its efforts.

Grisoft AVG 7.0.241

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

After the difficulties experienced in the last *Windows* comparative as a result of *AVG 7*'s new interface (see *VB*, February 2004. p.12), *AVG* returned to being an easy product to review and it obtains a VB 100% award. The files the product did miss were mainly complex polymorphic viruses, none of which have been seen in the wild as yet.

H+BEDV AntiVir 6.24.01.06

ItW Overall	100.00%	**Macro**	99.52%
ItW Overall (o/a)	100.00%	**Standard**	98.42%
ItW File	100.00%	**Polymorphic**	87.18%

The weakness on detection of polymorphic samples is also a feature of *H+BEDV*'s *AntiVir*, now firmly re-established in the *VB* testing lineup after an extended absence. *AntiVir* is soon to be joined or replaced by a new product line from *H+BEDV*, which is expected to arrive in time for the next *Windows* review in November 2004.

In the meantime, *AntiVir* paves the way for the *H+BEDV* newcomer with a VB 100%.

Kaspersky KAV 4.0.2.8

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

Kaspersky's product is, by and large, a pleasure to work with – although there are two recurring irritations. The first is a feature of reviewing, in that applying all definition updates from scratch is quite a long-winded affair, with many individual files needing to be downloaded. This will, of course, be mitigated in reality since the product is not reinstalled every time it is used. The second issue is with the hell-spawned sound effects which erupt, by default, on detecting a virus. Again, this is less likely to be an issue to a real-world user. The detection rate of the product was good – only .VXD samples of W32/Navrhar being missed, and these misses only on access [*thus not affecting the 100.00% scores listed above - Ed*]. As a result, *Kaspersky* earns a VB 100% award.

MicroWorld eScan 1.18

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

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	37	14782.0		7	11333.4		126	1265.2	31	2406.7
Alwil Avast!	104	5259.0		24	3305.6		33	4830.8	22	3391.2
Authentium Command	113	4840.1		5	15866.8		44	3623.1	5	14921.5
CA eTrust Antivirus	143	3824.7		3	26444.6		62	2571.2	4	18651.9
CA Vet Anti-Virus	137	3992.2		8	9916.7		70	2277.4	8	9325.9
CAT Quick Heal	59	9270.0		10	7933.4		47	3391.8	18	4144.9
DialogueScience Dr.Web	277	1974.5	[1]	20	3966.7		108	1476.1	20	3730.4
Eset NOD32	39	14023.9		3	26444.6		22	7246.2	5	14921.5
Fortinet FortiClient	240	2278.9	4	37	2144.2		52	3065.7	27	2763.2
FRISK F-Prot Antivirus	139	3934.8		5	15866.8		61	2613.4	6	12434.6
F-Secure Anti-Virus	175	3125.3		16	4958.4		103	1547.7	25	2984.3
GDATA AntiVirusKit	823	664.6		21	3777.8		380	419.5	32	2331.5
Grisoft AVG	114	4797.7	[1]	7	11333.4		56	2846.7	7	10658.2
H+BEDV AntiVir	156	3506.0		4	19833.4		101	1578.4	13	5739.0
Kaspersky KAV	152	3598.2		14	5666.7		77	2070.3	20	3730.4
MicroWorld eScan	206	2655.0		17	4666.7		94	1695.9	20	3730.4
NAI McAfee VirusScan	101	5415.2		12	6611.1		70	2277.4	18	4144.9
Norman Virus Control	451	1212.7		8	9916.7		151	1055.7	11	6782.5
NWI Virus Chaser	147	3720.6	[12]	9	8814.9		62	2571.2	9	8289.7
SOFTWIN BitDefender	629	869.5	[1]	7	11333.4		296	538.6	12	6217.3
Sophos Anti-Virus	67	8163.2		9	8814.9		38	4195.2	10	7460.7
Symantec SAV	164	3335.0		20	3966.7		64	2490.9	20	3730.4
Trend Internet Security	69	7926.6		4	19833.4		40	3985.4	19	3926.7
UNA UNA Pro	78	7012.0	6 [8]	22	3606.1	[12]	120	1328.5	37	2016.4
VirusBuster VirusBuster	191	2863.5		7	11333.4		120	1328.5	14	5329.1

Being, in part, a rebadged version of *GDATA*'s *AntiVirusKit*, the test results for *eScan* might be expected to follow those of *AVK*. This was true to a certain extent – however, it seems that updates had been somewhat slower to reach the *MicroWorld* product than to be applied to the source product. Not surprising, but this proved rather unfortunate news for *MicroWorld*, since the result was that the product missed a sample of W32/Netsky.X in the ItW test set, and thus *eScan* misses out on a VB 100% award on this occasion.

NAI McAfee VirusScan 7.1.0 4.3.20 4358

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

With yet another name change approaching for the producers of the *McAfee* product line, the underlying product remains much the same as ever. With no detection implemented by default for archives, the samples of W32/Heidi.A are automatic misses, to which is added the single .HTA sample of JS/Unicle.A. There were no misses of samples In the Wild and, with no false positives, a VB 100% award is appropriate.

Norman Virus Control 5.70.09

ItW Overall	100.00%	**Macro**	99.95%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	96.53%

Having had a few troublesome issues over the course of the last few comparative reviews, *NVC* returned to form on this occasion. Initial results on demand seemed strange, but turned out to be the result of a problem with reporting, rather than with detection. Results thereafter were better than expected, with some files detected for the first time by this product. None of the newly-added In the Wild files were missed, and thus *NVC* achieves a VB 100% award.

NWI Virus Chaser 5.0

ItW Overall	99.89%	**Macro**	100.00%
ItW Overall (o/a)	99.89%	**Standard**	99.82%
ItW File	99.89%	**Polymorphic**	100.00%

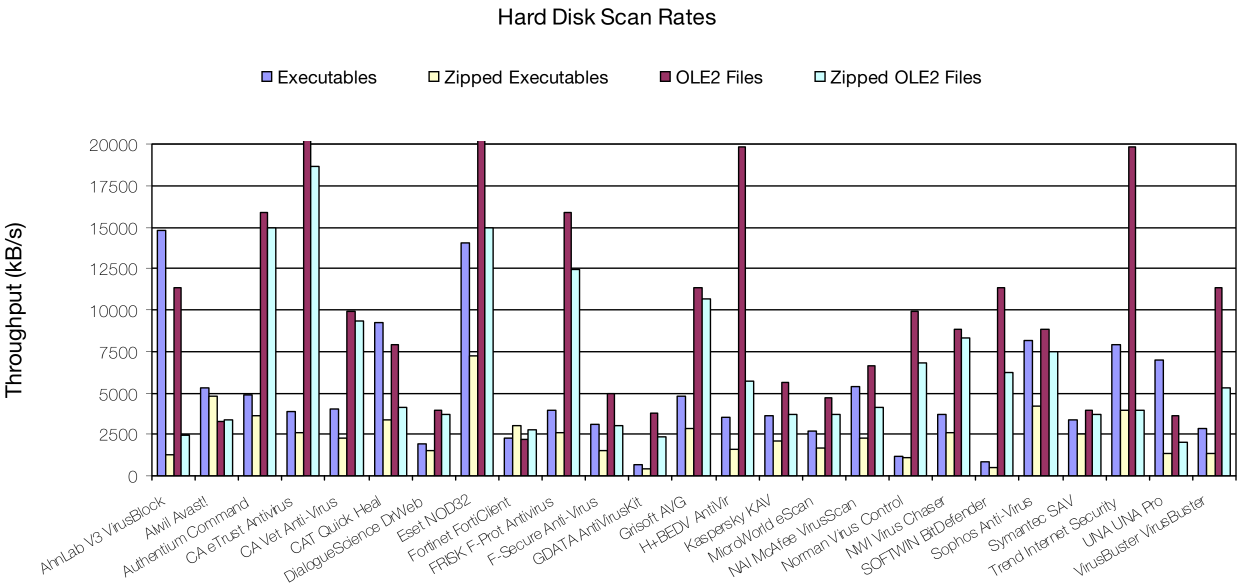
A quirk of *Virus Chaser* is that on-demand scanning for boot sectors is not performed when a standard scan of the drive is performed. Instead, it is necessary to select a separate option from the tray, which scans boot-sectors only. This is not a particularly intuitive location and would, perhaps, be better located within the main GUI. In addition, on-access scanning remains active during on-demand scanning, which was the cause of irritations when performing on-demand re-tests.

Virus Chaser is a rebadged version of *Dr.Web* and thus it was not a great surprise that it fell at the same hurdle. The .HTM sample of W32/Capside was not detected and thus no VB 100% can be awarded.

SOFTWIN BitDefender 7.2

ItW Overall	99.95%	**Macro**	99.69%
ItW Overall (o/a)	99.59%	**Standard**	98.28%
ItW File	99.94%	**Polymorphic**	99.78%

BitDefender remains the slowest product in the test on the clean executable test set, the numbers of self-extracting archives present here being a likely reason for this problem. Aside from this, detection was generally good, though some



problems in the ItW set led to non-complete detection. Missed files in this set were from W32/Lovegate.Q and the .HTM sample of W32/Nimda.A. *BitDefender* comes close to a VB 100%, but not quite close enough.

Sophos Anti-Virus 3.81

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Standard**	99.12%
ItW File	100.00%	**Polymorphic**	100.00%

Having recently improved its detection in the polymorphic test sets, *Sophos*'s product seems likely to remain at similar detection levels for a long period of time, since those remaining misses have been undetected since time immemorial. The lack of urgency in detecting these files is understandable, however, as none are particularly likely to be a concern for users. None of these files are located in the ItW test set and no false positives were detected, so the reward of a VB 100% goes to *Sophos* for its product.

Symantec SAV 8.1.0.825

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

SAV continues to be a solid performer with, once more, a detection for all samples in the *VB* test sets. This, combined with no false positives and a scanning rate which has overcome past hiccups, is good news for developer and users alike. A VB 100% award is duly added to *Symantec*'s collection.

Trend Internet Security 11.20 1311 7.100 1.885.00

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.63%
ItW File	100.00%	**Polymorphic**	95.77%

The *Internet Security* package is new to *VB* testing, being more of an integrated security suite than a pure anti-virus application. However, the underlying detection ability of the product is unchanged from that of *PC-cillin* or *ServerProtect*. Despite a number of misses in the polymorphic set, therefore, *Trend*'s *Internet Security* earns a VB 100% award.

UNA UNA Pro 1.83.250

ItW Overall	81.21%	**Macro**	80.96%
ItW Overall (o/a)	78.88%	**Standard**	67.79%
ItW File	81.78%	**Polymorphic**	17.50%

Once again, *UNA* scoops the prize for the largest number of false positives – a grand total of 20 suspicious and six fully viral files having been declared to exist in the clean set. Of these, 12 suspicious files were located in the clean OLE test set (in which no other products detected anything amiss).

UNA also has the worst detection rate by some margin, though there do appear to be improvements which bode well for developments in the months to come.

VirusBuster VirusBuster 4.006 9 7.965

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.45%
ItW File	100.00%	**Polymorphic**	91.45%

VirusBuster is a solid product – a slight weakness in the detection of polymorphic samples is the only negative point that can be mentioned. With full detection of all the ItW samples, and no false positives *VirusBuster* does, of course, gain a VB 100%.

CONCLUSION

A review with a large number of predictable results, and a few stray surprises thrown in for good measure. The shorter gap between WildList publication and testing caused fewer problems than were feared, though the addition of W32/Capside with its tricky .HTM sample more than made up for this. The most pleasant surprise was the improvement in the performance of *Fortinet*'s product, the results being accompanied by a slightly smoother experience while testing. Both this product and *UNA Pro* will be worth watching over the next few reviews.

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 can be found at http://www.virusbtn.com/Comparatives/WinXP/2004/test_sets.html.

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