COMPARATIVE REVIEW

WINDOWS XP

Matt Ham

Yet again the *Windows XP* comparative review is upon us, with the usual throng of products arriving to be tested and to test my patience. On this occasion two new products were submitted: *TrustPort Antivirus* and the rather more famous *Microsoft OneCare*. Rude comments and/or praise for these products can be found later in the review.

As this is the last review I will conduct for *Virus Bulletin*, I had hoped for an easy run overall – sadly this was not the case for several products. Although instability was less common than in previous tests, scanning speeds for some products were even slower than they have been in the past. There were also a number of products in this test whose feature sets can only have been designed by folk who are either totally ignorant of usability or bred for enhanced sadism.

THE TEST SETS

The test sets were aligned to the February 2006 WildList. As always, the contents of the WildList can be viewed at http://www.wildlist.org/.

When I first started anti-virus testing, the WildList consisted of some 300 different viruses, one third of which were boot sector types. I have none-too-fond memories of inserting 90 floppies into a machine for scanning on demand, then repeating the process on access. Thankfully for my successor, this month's tests saw a major, if long foreseen, change in that there are no longer any boot sector viruses that are considered to be in the wild. Similarly anticipated was the fact that all but a small number of macro viruses dropped out of the test sets this month, including all *Excel* and WM/ samples.

Numerous other files also dropped out of the test set this month – and, as ever, yet more were added to replace them. Overall numbers in the test set increased marginally; more than 100 samples were added and not quite as many removed. Samples of W32/Rbot, W32/Mytob and W32/Sdbot accounted for the majority of these changes and, together, these three fill around half of the space in the WildList.

AhnLab V3Pro 2004 6.0.0.574

ItW Overall	97.51%	**Macro**	98.94%
ItW Overall (o/a)	97.51%	**Standard**	96.45%
Polymorphic	83.60%		

Starting the line-up on this occasion, *AhnLab*'s *V3Pro* managed one of the slowest installation routines I have witnessed. It also demonstrated some odd logging behaviour, so that detection was performed ultimately by deletion of infected files.

Unfortunately, a false positive and a suspicious file in the clean test set were sufficient to deny *AhnLab* a VB 100% this month, though scanning of these files was notably speedy. In addition there were numerous misses of samples in the In the Wild (ItW) test set, which suggests that slow updates could be the problem here.

Alwil avast! 4.7.829

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.09%
Polymorphic	93.58%		

As ever, on-access detection for *avast!* was performed by copying the test set and deleting infected files – on-access scanning is not triggered simply by opening files. *avast!* also suffered from a round of false positives – a total of three being sufficient to dash any hopes of a VB 100%. However, there were no misses during the scanning of infected files in the ItW test set, and misses elsewhere were at the same low background level as ever.

Avira AntiVir 330 7.00.00.07

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

At first glance, *AntiVir* looked very much to be taking a step backwards in this version, since many options seemed no longer to be present. Happily, it turned out that these are merely somewhat hidden in the default interface view. With this minor hitch disentangled, *AntiVir* went on to detect all infected files in all test sets – a performance that earned the product a well-deserved VB 100% award.

CA eTrust (InoculateIT engine) 8.0.403.0 23.71.145.0

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	99.51%
Polymorphic	99.89%		

On-access tests	ItW		Macro		Polymorphic		Standard	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%
AhnLab V3Pro	19	97.51%	50	98.94%	2236	83.60%	63	96.45%
Alwil avast!	0	100.00%	18	99.56%	112	93.58%	18	99.09%
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%
CA eTrust (InoculateIT)	0	100.00%	4	99.90%	1	99.89%	4	99.51%
CA eTrust (Vet)	0	100.00%	10	99.88%	1	99.95%	3	99.84%
CAT Quick Heal	1	99.87%	86	97.96%	314	96.55%	153	92.81%
Central Command Vexira	3	99.61%	0	100.00%	126	92.58%	25	99.12%
Command Authentium	0	100.00%	0	100.00%	0	100.00%	4	99.67%
Doctor Web Dr.Web	0	100.00%	0	100.00%	0	100.00%	3	99.69%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet FortiClient	0	100.00%	0	100.00%	51	97.37%	6	99.79%
FRISK F-Prot	1	99.87%	0	100.00%	6	99.97%	6	99.49%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	3	99.93%	257	85.97%	31	98.35%
Hauri ViRobot	0	100.00%	44	98.82%	5785	69.52%	271	83.61%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Microsoft OneCare	0	100.00%	0	100.00%	31	97.67%	12	99.37%
MicroWorld eScanWin	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	175	92.96%	12	99.45%
NWI Virus Chaser	0	100.00%	0	100.00%	0	100.00%	3	99.69%
SOFTWIN BitDefender	0	100.00%	13	99.69%	7	99.77%	17	99.27%
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	15	99.30%
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
TrustPort Antivirus	22	97.47%	3	99.98%	14	99.24%	30	99.52%
VirusBuster VirusBuster	2	99.74%	0	100.00%	126	92.58%	25	99.12%

Having progressed to version 8, both the *eTrust* products now rejoice in a new interface. However, the new interface seems to prioritise looking new and trendy over being intuitive and easy to use.

Something I found to be particularly irritating was the fact that the interface is launched as HTML in a browser window which is almost unusable on any lower resolution screens.

I was hoping for an improvement in *eTrust*'s reporting of infections. However, hard to credit though it is, on-screen reporting proved to be even worse than it had been previously. In this version of the product infections are reported in a tiny text box which, by default, is truncated and cannot be resized.

It is thus impossible to tell which files are infected through the use of the on-screen display. This can be overcome by

printing the log file, though there is no obvious way of obtaining a useful version of this as a file.

As in previous comparative reviews, this version of *eTrust* is not eligible for a VB 100% award, since the *InoculateIT* engine is not the product's default.

CA eTrust (Vet engine) 8.0.403.0 12.4.2191.0

ItW Overall	100.00%	**Macro**	99.88%
ItW Overall (o/a)	100.00%	**Standard**	99.96%
Polymorphic	99.95%		

Of course, the comments made in the previous section also apply to this version of *eTrust*. As mentioned, the *Vet* engine is the default for use in scanning – in fact *eTrust* reverts back to *Vet* on each restart of the GUI.

Despite the interface woes, *eTrust*'s detection rates were up to their usual good levels, and since no false positives were detected in the clean test set a VB 100% is the result. Scanning speeds were also good for both of the engines.

CAT Quick Heal 2006 8.00

ItW Overall	99.87%	**Macro**	98.23%
ItW Overall (o/a)	99.87%	**Standard**	96.51%
Polymorphic	96.58%		

Problems for *CAT* started in the clean test sets, where the generation of a false positive denied the product any chance of a VB 100% immediately. On a truly bizarre front, *Quick Heal* reported internally that all scans of clean objects took exactly one hour each. In reality, scanning speeds were good. Unfortunately, there was a second major disappointment for *CAT* in that samples of W32/Bagle.X were missed in the ItW test set.

Central Command Vexira Antivirus 2006 5.002 33

ItW Overall	99.61%	**Macro**	100.00%
ItW Overall (o/a)	99.61%	**Standard**	99.27%
Polymorphic	90.27%		

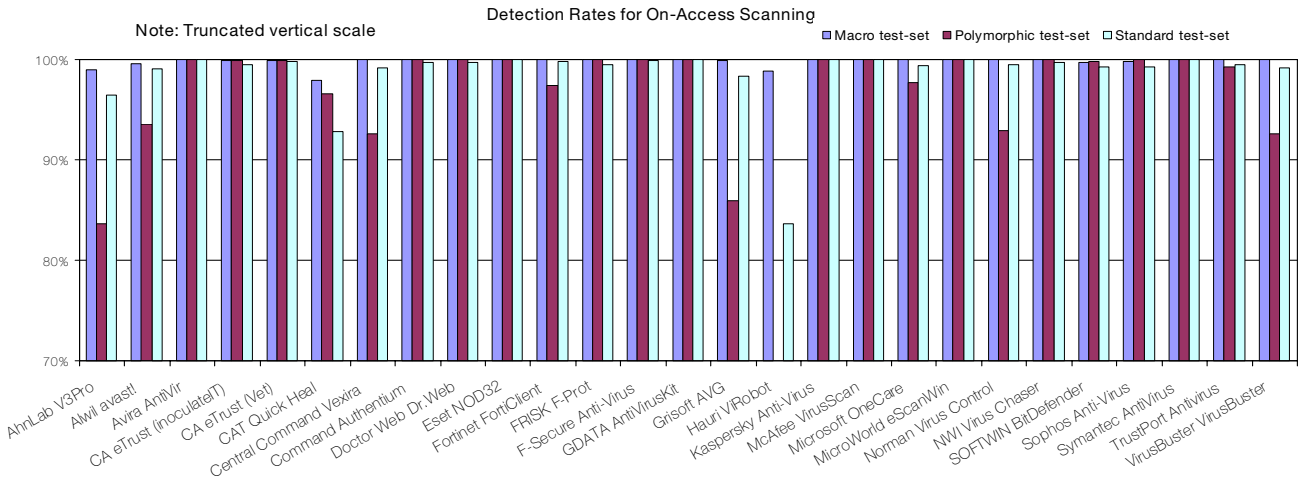
Vexira bears a very close resemblance to *VirusBuster* – which can be explained by the fact that it is a rebadged version of *VirusBuster*. Purists might point out that one product is red and the other blue, but my advanced skills of observation saw past this dissimulation.

Unfortunately stability was not a strength of this product, which caused a hang on the test machine after on-access scanning.

On demand, matters were substantially worse, with there being repeated crashes while scanning *PowerPoint* files. After this performance had been tolerated for long enough to obtain results, there remained a number of misses of samples in the ItW test set, thus the product was prevented from obtaining a VB 100%.

Command Authentium AntiVirus 4.93.7

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



Once again, the most irritating thing about this product was the log – which is available only in a very truncated RTF format. An extensive search of the machine did not help in finding a useful log, thus infected files were deleted to determine detection rates.

After having jumped through the appropriate hoops, the scanning results were good, with only very few, non-ItW, infected files being missed. As a result, *Authentium* earns itself a VB 100% award.

Doctor Web Dr.Web 4.33.2

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

On the negative side, *Dr.Web*'s on-access monitor *SpIDer Guard* lies about its configuration settings – option changes are only ever implemented after a reboot, a fact not reflected by the interface.

The story improved though, with scanning being perfect on demand, while missing only archived files on access. This performance was certainly ample for a VB 100% to be on its way to *Doctor Web*.

Eset NOD32 1.1517

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

NOD32 was the first product in this month's test with which I could find no real fault. Full detection across all test sets and a lack of false positives leave me little to comment on and earn *Eset* a well-deserved VB 100% to add to its collection.

F-Secure Anti-Virus Client Security 6.01

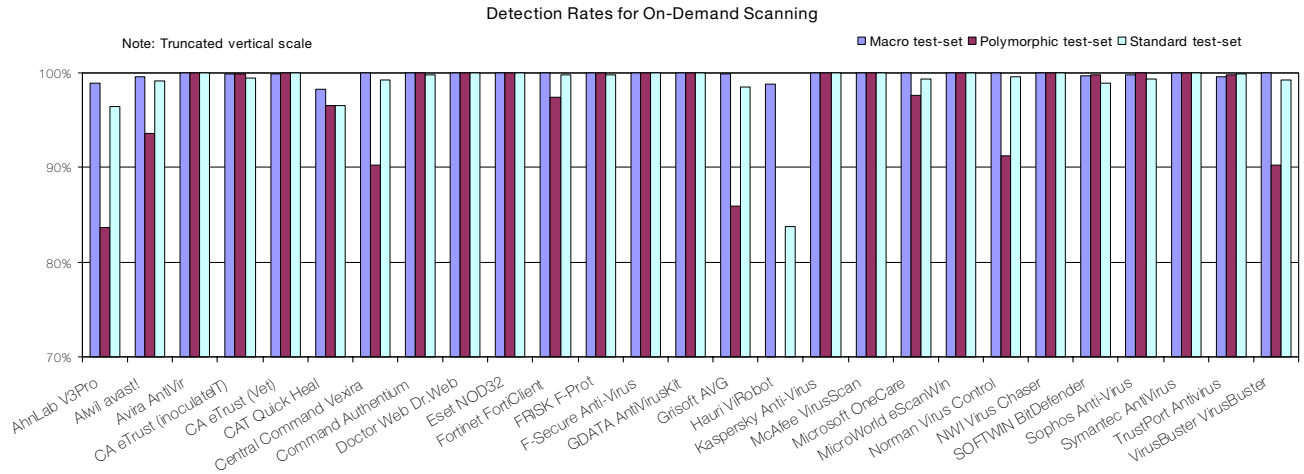
ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.98%
Polymorphic	100.00%		

Another product that displayed no remarkably bad or notably new features, *FSAV* also obtains a VB 100% for its performance. Misses here were limited to viral code, which is a stored rather than directly executable form.

Fortinet FortiClient 2.76 8.459

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.79%
Polymorphic	97.36%		

The trend of good results with few shocks is continued with *Fortinet*'s offering. Although the product missed a noticeable number of polymorphic files, detection results across other test sets were very strong. As a result, *FortiClient* adds another VB 100% to its collection.



On-demand tests	ItW		Macro		Polymorphic		Standard	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%
AhnLab V3Pro	19	97.51%	50	98.94%	2236	83.60%	63	96.45%
Alwil avast!	0	100.00%	18	99.56%	112	93.58%	18	99.09%
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%
CA eTrust (InoculateIT)	0	100.00%	4	99.90%	1	99.89%	4	99.51%
CA eTrust (Vet)	0	100.00%	10	99.88%	1	99.95%	1	99.96%
CAT Quick Heal	1	99.87%	73	98.23%	308	96.58%	98	96.51%
Central Command Vexira	3	99.61%	0	100.00%	624	90.27%	26	99.27%
Command Authentium	0	100.00%	0	100.00%	0	100.00%	1	99.82%
Doctor Web Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet FortiClient	0	100.00%	0	100.00%	55	97.36%	6	99.79%
FRISK F-Prot	0	100.00%	0	100.00%	0	100.00%	1	99.82%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1	99.98%
GDATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	3	99.93%	257	85.97%	28	98.50%
Hauri ViRobot	0	100.00%	44	98.82%	5785	69.52%	269	83.73%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Microsoft OneCare	0	100.00%	0	100.00%	31	97.67%	12	99.37%
MicroWorld eScanWin	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	179	91.25%	5	99.62%
NWI Virus Chaser	0	100.00%	0	100.00%	0	100.00%	0	100.00%
SOFTWIN BitDefender	0	100.00%	13	99.69%	7	99.77%	22	98.91%
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	15	99.30%
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
TrustPort Antivirus	4	99.95%	19	99.61%	5	99.76%	4	99.91%
VirusBuster VirusBuster	2	99.74%	2	99.98%	624	90.27%	26	99.27%

FRISK F-Prot Antivirus 3.16f

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

Unfortunately, the run of products displaying excellent results and few faults is cut short here, since all was not perfection for *F-Prot*. Scanning speeds were fair, but unfortunately a smattering of misses across the test sets included a sample of W32/Aimbot, which is classified as in the wild.

A VB 100% award therefore is out of the grasp of *FRISK* on this occasion.

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files		Dynamic	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
AhnLab V3Pro	51.0	12620.6	1	9.0	8814.9		150.0	1062.8	25.0	2984.3	6.0	8040.4
Alwil avast!	154.0	4179.5	3	42.0	1888.9		44.0	3623.1	21.0	3552.7	48.0	1005.1
Avira AntiVir	240.0	2681.9		8.0	9916.7		179.0	890.6	15.0	4973.8	108.0	446.7
CA eTrust (InoculateIT)	75.0	8582.0		10.0	7933.4		100.0	1594.2	21.0	3552.7	22.0	2192.8
CA eTrust (Vet)	91.0	7073.1		13.0	6102.6		100.0	1594.2	25.0	2984.3	17.0	2837.8
CAT Quick Heal	78.0	8251.9	1	25.0	3173.4		73.0	2183.8	27.0	2763.2	35.0	1378.4
Central Command Vexira	258.0	2494.8		39.0	2034.2		187.0	852.5	43.0	1735.1	70.0	689.2
Command Authentium	109.0	5905.0		5.0	15866.8		43.0	3707.4	5.0	14921.5	19.0	2539.1
Doctor Web Dr.Web	263.0	2447.3		11.0	7212.2		88.0	1811.6	14.0	5329.1	26.0	1855.5
Eset NOD32	37.0	17395.9		3.0	26444.6		31.0	5142.5	7.0	10658.2	16.0	3015.2
Fortinet FortiClient	235.0	2738.9		10.0	7933.4		145.0	1099.4	10.0	7460.7	16.0	3015.2
FRISK F-Prot	149.0	4319.8		6.0	13222.3		71.0	2245.3	8.0	9325.9	31.0	1556.2
F-Secure Anti-Virus	181.0	3556.1		16.0	4958.4		84.0	1897.8	21.0	3552.7	28.0	1723.0
GDATA AntiVirusKit	412.0	1562.3		32.0	2479.2		175.0	911.0	62.0	1203.3	61.0	790.9
Grisoft AVG	225.0	2860.7		7.0	11333.4		75.0	2125.6	9.0	8289.7	27.0	1786.8
Hauri ViRobot	457.0	1408.4	1+[1]	101.0	785.5		321.0	496.6	116.0	643.2	144.0	335.0
Kaspersky Anti-Virus	1272.0	506.0		17.0	4666.7		50.0	3188.3	18.0	4144.9	170.0	283.8
McAfee VirusScan	154.0	4179.5		9.0	8814.9		73.0	2183.8	17.0	4388.7	18.0	2680.1
Microsoft OneCare	419.0	1536.2		9.0	8814.9		246.0	648.0	14.0	5329.1	115.0	419.5
MicroWorld eScanWin	411.0	1566.1		34.0	2333.3		152.0	1048.8	64.0	1165.7	59.0	817.7
Norman Virus Control	944.0	681.8		7.0	11333.4		176.0	905.8	8.0	9325.9	148.0	326.0
NWI Virus Chaser	248.0	2595.4		12.0	6611.1		91.0	1751.8	14.0	5329.1	24.0	2010.1
SOFTWIN BitDefender	398.0	1617.2		13.0	6102.6		186.0	857.1	16.0	4663.0	66.0	730.9
Sophos Anti-Virus	99.0	6501.5		17.0	4666.7		55.0	2898.5	17.0	4388.7	21.0	2297.3
Symantec AntiVirus	176.0	3657.1		12.0	6611.1		65.0	2452.6	11.0	6782.5	11.0	4385.7
TrustPort Antivirus	1145.0	562.1		20.0	3966.7		325.0	490.5	24.0	3108.6	175.0	275.7
VirusBuster VirusBuster	288.0	2234.9	1	44.0	1803.0		191.0	834.6	49.0	1522.6	75.0	643.2

GDATA AntiVirusKit 2006 16.0.7

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

Despite a somewhat slow performance, *GDATA* managed full detection of all samples in all categories, with no false positives. *AVK*'s developers should be pleased with this performance, and a VB 100% should add to their contentment.

Grisoft AVG Anti-Virus 7.1.392

ItW Overall	100.00%	**Macro**	99.93%
ItW Overall (o/a)	100.00%	**Standard**	98.50%
Polymorphic	85.97%		

One of the more common user queries I have been faced with during my time at *Virus Bulletin* concerns how to delete infected files using *AVG*. Having tried to do so, the frequency of complaints no longer surprises me. Numerous files, although

flagged as infected, were not subject to any automated deletion or disinfection.

Apart from this there were no surprises in either the clean or infected test sets, with a VB 100% being the pleasing result for *Grisoft*.

Hauri ViRobot 5.0

ItW Overall	100.00%	**Macro**	98.82%
ItW Overall (o/a)	100.00%	**Standard**	83.73%
Polymorphic	69.52%		

Unfortunately, *Hauri*'s chances of gaining a VB 100% evaporated with a false positive and suspicious file noted in the clean set – and scanning rates were not particularly speedy here either.

Misses in detecting infected files were plentiful too, although looking on the brighter side, none of the missed detections occurred in the ItW set.

Kaspersky Anti-Virus 6.0.0.299

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

KAV includes various self-protection features which turn out to be a double-edged sword. The less-than-welcome aspect is that the virus definitions are so well protected that they are, by default, unable to be updated manually. Since the update function does not allow updates from a local folder, this is somewhat irritating.

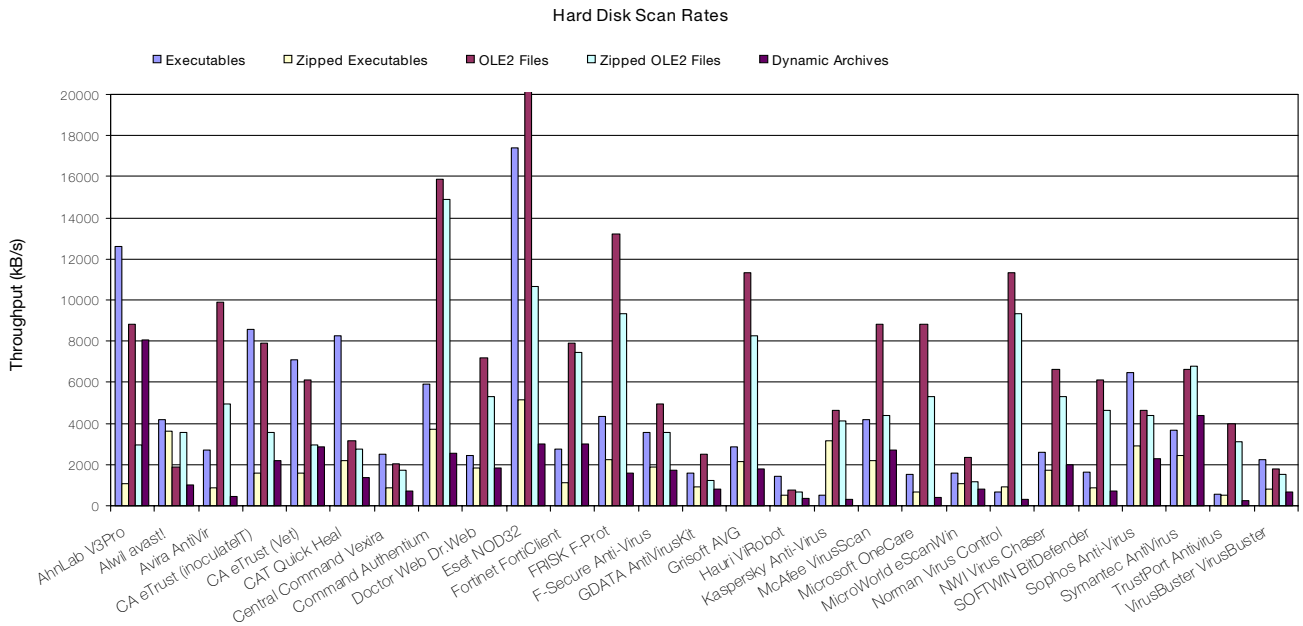
There also seem to have been some changes in scanning methods, the effects of which are particularly unpleasant. On-access scanning was seemingly interminable, while the clean set scanning rate is pretty indicative of the speeds seen while scanning the infected sets. This is not an effect of low scanning priorities however – during scanning *KAV* remained steadily at 99% processor usage.

All of this work was, at least, for good reason as all files in all test sets were detected and no false positives were produced. A VB 100% award thus acts as a distraction from the various problems encountered.

McAfee VirusScan Enterprise 8.0i 4400 4753

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

Happily, with *VirusScan* we return to a product that had no nasty surprises in store and gave a good performance with full detection of infected samples across all test sets. With no false positives noted in the



clean test sets either, *VirusScan* is awarded a well deserved VB 100%.

Microsoft Windows Live OneCare 1.0.0971.12

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.37%
Polymorphic	97.67%		

As might be expected of a *Microsoft* product, *OneCare* operates in the guise of paranoid nanny. The user is not trusted to make many decisions of their own, which made certain parts of the test process frustrating.

The progress counter that is displayed during scans is particularly laughable, reaching 99% in ten minutes and then remaining at that point for approximately another 20 minutes or so. This is a result of the automatic disinfection and quarantine (the user has no say in the matter). Indeed, *Microsoft*'s idea of quarantining is somewhat novel, consisting of appending what looks like a checksum to the end of the file name.

What with constantly resetting the areas to be scanned and hanging after the on-access scan, this product cannot be said to be one of my favourites. However, its detection rates were sufficient for a VB 100% to be in order.

MicroWorld eScanWin 8.0.659.1

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

eScan is a rebadged version of *GDATA*'s *AntiVirusKit*, so it should come as no great surprise that the results for *eScan* include full detection of samples across all test sets, a VB 100% award and no adverse comment.

With little else to say, let's move on to a product that behaved badly instead.

Norman Virus Control 5.81

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.62%
Polymorphic	91.25%		

Having been a source of frustration in previous reviews (see *VB*, April 2006, p.17), *Norman Virus Control* continued to manifest new problems on this occasion.

On-access scanning was subject to repeated crashes, whether dealing with infected or previously disinfected files. The effects were sufficient to reduce *Windows* to a state of complete paralysis, in which only a hard reboot had any effect on the test machines.

Upon reboot the splash screen displays the question 'Would you go for anything but green?' (green being *Norman*'s corporate colour). My answer would be that *anything* would be better than this.

Unfortunately for the forces of truth and justice, after strenuous efforts scanning results were sufficient to warrant a VB 100% for this shockingly behaved product.

New Technology Wave (NWI) Virus Chaser 5.09

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

Since *Virus Chaser* is a rebadged version of *Dr.Web*, it should come as little surprise that it shares both the irritations and praise of that product.

With faultless detection rates across all the test sets and no false positives noted in the clean test set, a VB 100% can be included in the shared experience.

SOFTWIN BitDefender 9 7.06632

ItW Overall	100.00%	**Macro**	99.69%
ItW Overall (o/a)	100.00%	**Standard**	98.91%
Polymorphic	99.77%		

There were few notable moments during the testing of *BitDefender*, though the scanning of clean executables was certainly slow enough to be tedious to oversee.

As far as detection was concerned, *BitDefender* had a small number of missed detections, although no real pattern was discernable among them. Happily for *SOFTWIN*, however, there were no misses in the ItW set and no false positives were picked up in the clean test set, thus *BitDefender* also earns a VB100%.

Sophos Anti-Virus 5.2.0

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

Sophos's product was as well behaved as ever. Whether it was practice with the GUI or some small changes in it, something made its use seem very much simpler than I can remember it having been recently, which is always a plus point. With an admirable performance across the test sets, a VB100% is in order for the *Sophos* product.

Symantec AntiVirus 10.0.0.359

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

The *Symantec* GUI has remained the same for many years and on this occasion the product's full detection rate across all test sets leaves little scope for discussion. Not even my pathological hatred of the colour yellow can detract from the fact that the product's performance was ample for *SAV* to be awarded a VB 100%.

TrustPort Antivirus 1.6.0.807

ItW Overall	99.95%	**Macro**	99.61%
ItW Overall (o/a)	97.47%	**Standard**	99.91%
Polymorphic	99.76%		

Since this product is based on a combination of *BitDefender* and *Norman* scanning engines, I was fearful, when I first launched *TrustPort*, that its scanning performance would resemble blue whales forced into pogo-stick races. Thankfully, scanning speeds were not absolutely terrible, just pretty bad.

The combination of the two engines may be responsible for one of *Trustport*'s oddities, namely that it reported many more files as having been scanned than actually existed in the test sets. A further mystery was the variation in the actions taken upon detection of a virus. Using the default settings, samples were deleted, disinfected, quarantined, renamed and simply left to fester, all in the course of one scan.

All this aside, the detection rates demonstrated by the product came close to decent, but there were a sufficient number of ItW misses to deny *TrustPort* a VB 100%.

VirusBuster Professional 2006 5.2 33

ItW Overall	99.74%	**Macro**	99.98%
ItW Overall (o/a)	99.74%	**Standard**	99.27%
Polymorphic	90.27%		

Not surprisingly, *VirusBuster* suffered some of the same woes as *Vexira*, though thankfully to a lesser extent. Instability on demand resulted in scanning simply not being available after existing scans aborted while in progress. Only a reboot solved this broken state. Misses of samples in the ItW test set merely added to these woes, meaning that *VirusBuster* was denied a VB 100% on this occasion.

As a side note, after discussion with the developers, the reason for the scanning speed issues which plagued *VirusBuster* in the *Linux* comparative review (see *VB*, April 2006, p.13) was determined to be the handling of alert messages. In the default setting, alerts are sent to the client and if the client is set such that it will not accept these alerts, then the sending will wait until it times out. Since the client is set, by default, not to accept these alerts, this causes a dramatic slowdown in scanning rates. Clearly this problem can be solved easily by some simple changes in the client or scanner configuration.

CONCLUSION

My final words should be statements, grave judgements and moments of prescience, so as to leave a lasting memory of the quality of my reviews. Unfortunately for this line of thinking, the only thoughts I have to offer are of a cynical nature.

The names and descriptions of the threats may change, but the anti-virus industry remains pretty much the same as it ever has been. The major companies are the same, user ignorance is unchanged and the hyperbolic press releases are the same. Even the claims that 'soon all will change' are simply repeats of the past. If I should return to the anti-virus field in the future, I really don't think it would take more than a few minutes to become re-acclimatised – I just hope that *NetWare* is extinct by then.

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 SP2*.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/WinXP/2006/test_sets.html.

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

NEARLY VB 100%

In the recent *Windows XP* comparative review (see *VB*, June 2006, p.11), *VB* reported that *VirusBuster* failed to achieve the results required for a VB 100% award. After discussion with the developers, it was discovered that out-of-date virus identities had been provided with the product and that *VB*'s tester had failed to acknowledge the warning messages suggesting that an update of the virus database was in order. While the results remain valid for the version of the product tested, *VB* has since tested the product using what would have been the most recent identities for the submission deadline of the test. The two ItW viruses that prevented the product from achieving a VB 100% at the time were caught – meaning that if the correct data had been supplied originally, *VirusBuster* would easily have achieved a VB 100%.