COMPARATIVE REVIEW

WINDOWS 2000 SERVER

John Hawes

My second time running the *Virus Bulletin* comparative review offered a wildly different experience from the first; whereas August's *Novell NetWare* test drew a mere eight entries, this month saw a bumper 26 products vying for the award. Many of these were entirely new to me, and two were first-timers in the *VB* tests. Both from China, newcomers *Kingsoft AntiVirus* and *Greatsoft Virusclean* were added to the rash of more familiar names with a mixture of excitement and trepidation on my part.

TEST SETS AND PLATFORM

The platform for the test was *Windows 2000 Server*, just barely on the edge of supported status and almost certainly seeing its last outing in the *VB* lab. The aging operating system was succeeded several years ago by *Windows 2003 Server* – which will, apparently, soon be made obsolete itself by the forthcoming and much hyped *Windows Vista*. Patched with the most recent service pack (the three-year-old SP4), setting up the test machines with *Windows 2000* was a familiar and trouble-free experience.

The In the Wild (ItW) test set was aligned with the June 2006 WildList, which saw the addition of a sprinkling of familiar Mytob and Bagle variants, along with a few new names. W32/Areses, W32/Rontokbro and W32/Banwarum are fairly standard email worms with a few nasty AV-disabling and general anti-tampering devices thrown into some variants.

On top of the additions to the WildList, the clean set was expanded somewhat, but the most significant change this month was a handful of new viruses in the polymorphic test set, all of which have been around for some time, and rarely trouble users these days. However, although most are limited to older operating systems, as infectious viruses they all have the chance of making a nuisance of themselves should they ever make their way onto a vulnerable machine. Of the batch, the venerable W95/Zmorph is perhaps the most notable, with its highly metamorphic nature aimed at baffling the detection engines of its day. Let's see how the modern-day versions fared.

AhnLab V3Net for Windows Server 6.0

ItW	100.00%	**Macro**	98.97%
ItW (o/a)	100.00%	**Macro (o/a)**	98.97%
Standard	97.13%	**Polymorphic**	90.48%

AhnLab's product installed in a straightforward fashion, but I found the GUI a little uncomfortable at first, as I made copies of the default jobs available in order to tweak the configuration to suit my needs.

The progress screen for the on-demand scanner amused me, with its row of folder icons progressing past a magnifying glass, which sucked green bugs out of them as they went by. I was less amused by the logging, which seemed not to record the paths of infected files, and by the on-access scanner, which appeared not to block any files from being opened. However, when configured to delete infected items it did the job – after slowly building a list of all infections spotted, and then going through deleting them once the delete option had been selected.

After all this, although much was missed in the zoo collections, all the WildList viruses were spotted, and no false positives were alerted on in the clean set, thus earning *V3Net* a VB 100% award. The product also did rather well in the speed tests.

Alwil avast! v.4.7

ItW	100.00%	**Macro**	99.56%
ItW (o/a)	100.00%	**Macro (o/a)**	99.56%
Standard	98.74%	**Polymorphic**	89.90%

The piratical note in *avast!*'s title warned me to expect no mercy, and the greyed-out 'Back' button preventing me from retracing my steps after accepting the EULA felt a little like stepping out onto the plank. The multi-pane GUI was reasonably usable, and the on-demand and speed tests were carried out with ease and reasonable success, although several of the new polymorphic viruses were missed. On-access testing proved more difficult, as files were not blocked on opening, but copying them onto the machine and having them deleted brought results. On several tries the product got snarled up with the large numbers of warnings it was issuing and its GUI froze, requiring forcible shutting down. In the real world, however, such a problem is unlikely to occur, and with only a single file in the clean set labelled a 'Joke' to report, *avast!* qualifies comfortably for the VB 100% award.

Avira AntiVir Windows Server 2003/2000/NT v.6.35

ItW	100.00%	**Macro**	99.93%
ItW (o/a)	100.00%	**Macro (o/a)**	99.93%
Standard	100.00%	**Polymorphic**	96.37%

Avira's product was one of the plethora I was trying for the first time, and it rather pleased me.

The installation process offered no difficulties, although an image of what seemed to be a man holding a red umbrella indoors gave me reason to wonder how lucky *Avira* would be. The GUI reassured me with its pared-down, vaguely techie feel, simple icon-style graphics and text-heavy displays and menus. The progress display, updating itself every 50–100 files scanned, gave an impression of thoroughness, and results in the first few tests were admirable.

A few of the new polymorphic viruses went unrecognised, but this was not too surprising. It was in the clean set that *Avira*'s luck ran out, however, and with two false positives recorded, *AntiVir* misses out on its VB 100%.

BitDefender Antivirus v.10

ItW	100.00%	**Macro**	96.69%
ItW (o/a)	100.00%	**Macro (o/a)**	96.69%
Standard	99.27%	**Polymorphic**	97.02%

BitDefender was another product I sampled for the first time this month, and I was pleased to see mention of the VB 100% award proudly presented on the second screen of the installation process, as well as in the readme. I also found the slick, simple, oddly flat-looking GUI easy on the eye and untaxing on the brain, although the little black block indicating that the on-access component is functioning was a little spooky.

The product did well in both the WildList and zoo collections, missing nothing in the ItW test set and not a great deal in the other sets, but sadly it was let down by yet another false positive in the clean test set, which spoiled *BitDefender*'s chances of adding another VB 100% award to its collection.

CA eTrust 8.0.403.0 (InoculateIT engine)

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	99.51%
Standard	99.82%	**Polymorphic**	97.23%

eTrust's professional-looking installation, with its requirement to scroll through several lengthy EULA segments and a lengthy survey of personal information, was familiar to me from the *NetWare* tests last time around, as was the browser-based GUI. This didn't work as well as I remembered, indeed refusing to initiate an on-demand scan, which rather scuppered me until I learned that the browser installed with *Windows 2000 – Internet Explorer 5.0* – was not supported by the product, and *IE* version 6 SP1 was required.

With the required version of *IE* installed, the only remaining issue was with the logs – which, being large and filled with notices of infections, were rather slow to open up in the display window. They were also not exportable to plain text for parsing, but that annoyance was soon worked around to find good scores all round. Of course, since *InoculateIT* is not the default for the product, it does not qualify for the VB 100% award.

CA eTrust 8.0.403.0 (Vet engine)

ItW	100.00%	**Macro**	99.82%
ItW (o/a)	100.00%	**Macro (o/a)**	99.84%
Standard	99.96%	**Polymorphic**	94.26%

When run with the *Vet* engine, *eTrust* missed slightly more of the new polymorphic viruses than when run using the *InoculateIT* engine, and was also a fraction slower in some of the throughput tests, but still put in a strong performance, amply qualifying for another VB 100% award.

CAT Quick Heal 2006 v.8.0

ItW	100.00%	**Macro**	98.23%
ItW (o/a)	100.00%	**Macro (o/a)**	97.96%
Standard	96.51%	**Polymorphic**	87.07%

Quick Heal surprised me during installation by carrying out an automatic scan of memory and system files, before requesting a reboot to complete the installation.

Once installed, the GUI presented to me was simple and slick, although it seemed to offer no method of disabling the on-access protection; this, I soon found, was achieved by right-clicking the icon in the system tray.

On checking the scan results, I was a little confused that the timings seemed to have had an hour added to each, resulting in many scans claiming to have finished 55 minutes in the future. However, I was soon able to correct for this, and found the scanning speeds reasonable enough to justify the product's title. Despite missing a fair chunk of the zoo viruses, *Quick Heal* detected everything in the ItW test set, while generating no false positives in the scan of the clean set, thereby earning its VB 100% award comfortably.

Command Authentium AntiVirus for Windows 4.93.8

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.98%	**Polymorphic**	99.93%

Authentium's product installed zippily, and presented me with a small and simple GUI. Things seemed to be progressing nicely with on-demand scanning until I attempted to save the log produced; while a log was indeed saved, it seemed to include only the last 1,000 lines of the full scan report – all of which were still viewable within the product's GUI. Resorting once more to the deletion method, *Authentium* did excellently on the infected files, but was let down when a file in the clean set was flagged as suffering an infection, which it suggested was possibly a new variant of a known threat. This was enough to deny the product the VB 100% award this time around.

Doctor Web Dr.Web Scanner for Windows v.4.33.2

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	98.08%

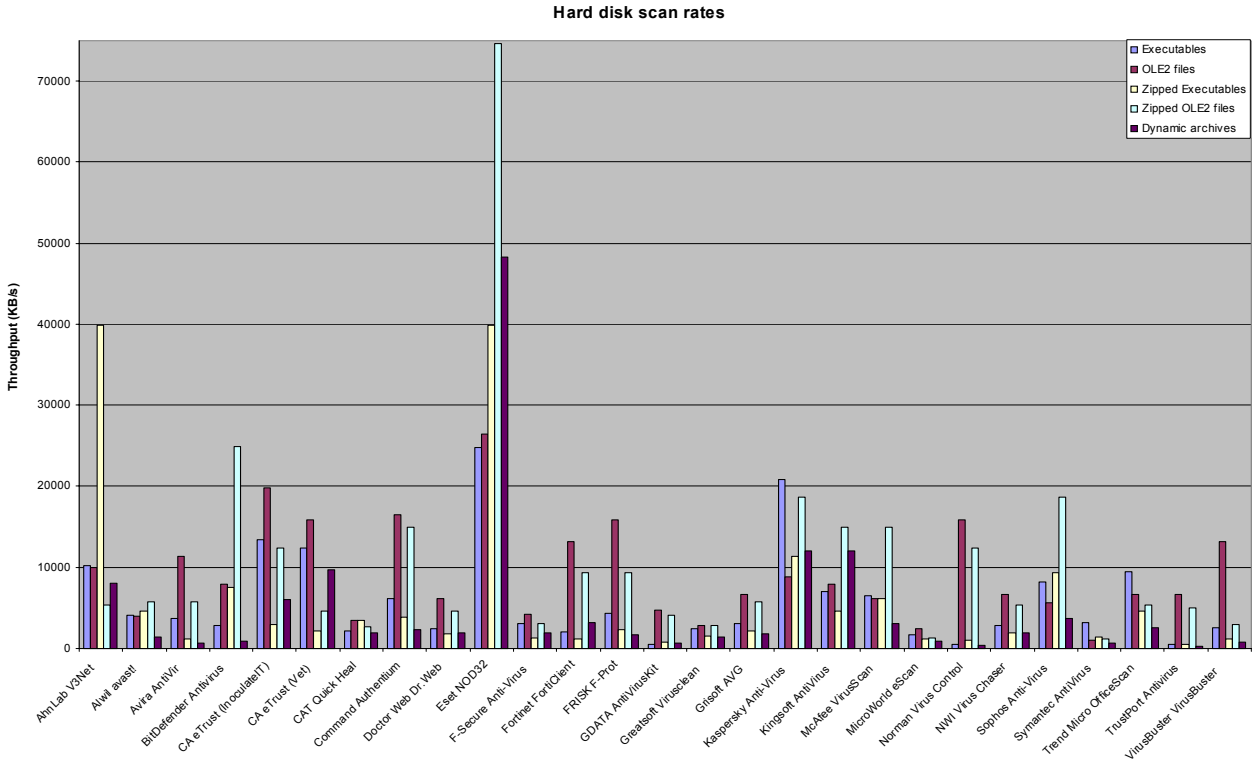
Dr.Web installed in a sleek and stylish fashion, and after a reboot and several automatic scans of memory and system files, I found the GUI equally slick. I found my way around it quickly – although the 'SpIDerGuard' on-access component of the product seemed not to have started itself – and it charged through the tests with little difficulty.

With only a single set of polymorphic samples missed, and a few zips in the standard set ignored on access, *Dr.Web* put in an impressive performance – no false positives were produced in the clean set, allowing *Dr.Web* to gain its VB 100% award with ease.

ESET NOD32 2.5

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

NOD32 also impressed me, with a very simple and rapid installation process and a simple, clear GUI – although I imagine anyone who isn't familiar with the product may be a little baffled by the numerous modules labelled only as 'AMON', 'IMON' etc.



Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables			Zipped OLE Files			Dynamic files		
	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	FPs [susp]
AhnLab V3Net for Windows Servers 6.0	63.0	10216.6		8.0	9916.7		4.0	39854.1		14.0	5329.1		6.0	8040.4	
Alwil avast! v.4.7	158.0	4073.7	[1]	20.0	3966.7		35.0	4554.8		13.0	5739.0		34.0	1418.9	
Avira AntiVir Windows Server 2003/2000/NT v. 6.35	176.0	3657.1	1	7.0	11333.4		132.0	1207.7	1	13.0	5739.0		81.0	595.6	
BitDefender Antivirus v.10	224.0	2873.4	1	10.0	7933.4		21.0	7591.3		3.0	24869.2		54.0	893.4	
CA eTrust 8.0.403.0 (InoculateIT)	48.0	13409.3		4.0	19833.4		55.0	2898.5		6.0	12434.6		8.0	6030.3	
CA eTrust 8.0.403.0 (Vet)	52.0	12377.9		5.0	15866.8		75.0	2125.6		16.0	4663.0		5.0	9648.5	
CAT Quick Heal 2006 v.8.0	288.0	2234.9		23.0	3449.3		46.0	3465.6		28.0	2664.6		25.0	1929.7	
Command Authentium AntiVirus for Windows 4.93.8	105.5	6102.1	1	4.8	16527.9		41.7	3822.9		5.0	14921.5		20.5	2353.3	
Doctor Web Dr.Web v.4.33.2	264.0	2438.1		13.0	6102.6		90.0	1771.3		16.0	4663.0		25.0	1929.7	
Eset NOD32 2.5	26.0	24755.7		3.0	26444.6		4.0	39854.1		1.0	74607.5		1.0	48242.6	
F-Secure Anti-Virus for Windows Servers v.5.52	213.0	3021.8		19.0	4175.5		129.0	1235.8		24.0	3108.6		25.0	1929.7	
Fortinet FortiClient 3.0.001	318.0	2024.1		6.0	13222.3		139.0	1146.9		8.0	9325.9		15.0	3216.2	
FRISK F-Prot v.3.16f	147.0	4378.6	[1]	5.0	15866.8		68.0	2344.4		8.0	9325.9		28.0	1723.0	
GDATA AntiVirusKit 16.0.7	1208.0	532.8	1	17.0	4666.7		192.0	830.3		18.0	4144.9		73.0	660.9	
Greatsoft Virusclean v.2.0.3286.3	260.0	2475.6	5	28.0	2833.3	1	101.0	1578.4	2	27.0	2763.2	1	35.0	1378.4	2
Grisoft AVG Anti-Virus 7.1	207.0	3109.4		12.0	6611.1		72.0	2214.1		13.0	5739.0		27.0	1786.8	
Kaspersky Anti-Virus 5.0 for Windows File Servers v. 5.0.77.0	31.0	20762.8		9.0	8814.9		14.0	11386.9		4.0	18651.9		4.0	12060.7	
Kingsoft AntiVirus 2006 v.7.1	91.0	7073.1	3	10.0	7933.4		35.0	4554.8	2	5.0	14921.5		4.0	12060.7	
McAfee VirusScan Enterprise 8.0	99.0	6501.5		13.0	6102.6		26.0	6131.4		5.0	14921.5		16.0	3015.2	
MicroWorld eScan Internet Security for Windows 8.0.673.1	392.0	1642.0		32.0	2479.2		143.0	1114.8		60.0	1243.5		55.0	877.1	
Norman Virus Control v.5.82	1211.0	531.5		5.0	15866.8		154.0	1035.2		6.0	12434.6		123.0	392.2	
NWI Virus Chaser v.5.0a	227.0	2835.5		12.0	6611.1		82.0	1944.1		14.0	5329.1		25.0	1929.7	
Sophos Anti-Virus v.6.03	79.0	8147.4		14.0	5666.7		17.0	9377.4		4.0	18651.9		13.0	3711.0	
Symantec AntiVirus 10.0.0.359	205.0	3139.7	[1]	79.0	1004.2		115.0	1386.2		67.0	1113.5		77.0	626.5	
Trend Micro OfficeScan Corporate Edition v.7.3	68.0	9465.4		12.0	6611.1		35.0	4554.8		14.0	5329.1		19.0	2539.1	
TrustPort Antivirus 2.01.855	1129.0	570.1	1	12.0	6611.1		302.0	527.9		15.0	4973.8		180.0	268.0	
VirusBuster VirusBuster 2006 for Windows Servers v.5.2	256.0	2514.3	[1]	6.0	13222.3		143.0	1114.8		25.0	2984.3		59.0	817.7	

I also spent some moments figuring out how to export logs, as the 'log' section of the GUI seemed to have no function. This brief dithering on my part took up most of the testing time, as the product powered through the scans in stunning time, and effortlessly detected everything offered to it without false positives, earning yet another VB 100% award for its work.

F-Secure Anti-Virus for Windows Servers v.5.52

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.85%	**Polymorphic**	100.00%

On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net for Windows Servers 6.0	0	100.00%	47	98.97%	626	90.48%	57	97.13%
Alwil avast! v.4.7	0	100.00%	18	99.56%	385	89.90%	34	98.14%
Avira AntiVir Windows Server 2003/2000/NT v. 6.35	0	100.00%	3	99.93%	0	96.37	150	100.00%
BitDefender Avtivirus v.10	0	100.00%	13	96.69%	37	97.02%	10	99.27%
CA eTrust 8.0.403.0 (InoculateIT)	0	100.00%	4	99.51%	42	97.23%	1	99.82%
CA eTrust 8.0.403.0 (Vet)	0	100.00%	3	99.84%	103	94.26%	1	99.96%
CAT Quick Heal 2006 v.8.0	0	100.00%	86	97.96%	602	87.07%	153	93.00%
Command Authentium AntiVirus for Windows 4.93.8	0	100.00%	0	100.00%	2	99.93%	4	99.67%
Doctor Web Dr.Web v.4.33.2	0	100.00%	0	100.00%	9	98.08%	3	99.69%
Eset NOD32 2.5	0	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus for Windows Servers v.5.52	0	100.00%	0	100.00%	0	100.00%	3	99.85%
Fortinet FortiClient 3.0.001	0	100.00%	0	100.00%	277	84.47%	0	100.00%
FRISK F-Prot v.3.16f	1	99.85%	0	100.00%	8	99.91%	4	99.49%
GDATA AntiVirusKit 16.0.7	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Greatsoft Virusclean v.2.0.3286.3	1	99.85%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG Anti-Virus 7.1	0	100.00%	3	99.93%	414	82.59%	30	98.41%
Kaspersky Anti-Virus 5.0 for Windows File Servers v. 5.0.77.0	0	100.00%	0	100.00%	0	100.00%	2	99.69%
Kingsoft AntiVirus 2006 v.7.1	2	99.78%	358	78.31%	14043	14.70%	871	54.70%
McAfee VirusScan Enterprise 8.0	0	100.00%	0	100.00%	46	99.01%	0	100.00%
MicroWorld eScan Internet Security for Windows 8.0.673.1	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control v.5.82	0	100.00%	0	100.00%	309	92.76%	12	99.45%
NWI Virus Chaser v.5.0a	0	100.00%	4	99.90%	14	98.06%	12	99.14%
Sophos Anti-Virus v.6.03	0	100.00%	8	99.80%	1	99.86%	14	99.33%
Symantec AntiVirus 10.0.0.359	0	100.00%	0	100.00%	4	99.91%	0	100.00%
Trend Micro OfficeScan Corporate Edition v.7.3	0	100.00%	13	99.68%	851	94.42%	30	98.76%
TrustPort Antivirus 2.01.855	0	100.00%	0	100.00%	25	98.88%	0	100.00%
VirusBuster VirusBuster 2006 for Windows Servers v.5.2	0	100.00%	0	100.00%	128	93.92%	25	99.12%

Having heard much about the Finnish company, I was eager to try out its product, and was not disappointed by the experience.

The installation splash screen contrasted a funky blaze of colour in one corner with an expanse of chilly white, after which the product set itself up rapidly without need for a reboot (although I was warned after applying the update that it might need a few minutes to settle in).

It strode comfortably through the on-demand tests, presenting me with a usable HTML log, but indulged in some odd blocking behaviour on access, forcing me to resort once more to deletion. This went just as well as the on-demand scan, and with the only samples missed being in

file types not scanned by default, *F-Secure*'s excellent performance amply justifies a VB 100% award.

Fortinet FortiClient 3.0.001

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	84.47%

FortiClient added yet another new product to my rapidly broadening experience – one which left more good impressions.

Stylish good looks, ease of use and a comprehensive range of functions, all controlled from a central interface, were added to decent speeds and solid detection rates, although many of the new polymorphic samples were missed. *FortiClient* also earns a VB 100% award.

FRISK F-Prot v.3.16f

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	99.85%	**Macro (o/a)**	100.00%
Standard	99.69%	**Polymorphic**	99.93%

F-Prot provided another of the more techie-looking GUI experiences, oozing reliability and solidity. As *FRISK* provided the engine for the false-positiving *Authentium*, I feared this product may suffer the same problem, but fortunately the alert system described the problem file merely as a 'suspicious file' – which is permissible under the rules of the VB 100% award – before recording the same infection message displayed by *Authentium*.

However, in a bizarre twist, a sample of W32/Aimbot was consistently ignored on-access, despite equally consistent detection on demand, so *F-Prot* misses out on the award this time round.

GDATA AntiVirusKit 16.0.7

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

GDATA's installation featured a rather scary swirly cog on its splash screen, and set itself up with two separate desktop shortcuts, both featuring its red-and-white logo. After a reboot, the product – which combines *BitDefender* and *Kaspersky* detection technology with its own user experience – presented a handy desktop gizmo featuring a clock, a news ticker, virus alerts, a virus info lookup system, and a set of handy links, with *Virus Bulletin* placed second behind *GDATA* itself.

The scanner GUI itself was reasonably user-friendly, although the 'protocol only' option in the actions list confused me somewhat, and the logging was a little over complicated and slow to display. Despite excellent detection throughout the infected test sets, results were marred by what eagle-eyed readers will be expecting – a false alarm in the clean set from the *BitDefender* engine, which was enough to deny the product the VB 100% award.

Greatsoft Virusclean v.2.0.3286.3

ItW	99.85%	**Macro**	100.00%
ItW (o/a)	99.85%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	100.00%

Receiving offers of new products for the comparative review was an exciting experience – I responded to preliminary enquiries from developers with a mix of hope and worry. *Greatsoft*'s web presence revels in the URL viruschina.com, which was reassuringly clear and slick. The installation process, although in need of a little proof reading, was equally smooth, and the GUI offered several useful tools, including a system for backing up and restoring boot records.

Using the product was a less happy experience, however. My first worry came when I found the 'Select Folders' window of the scanner only had options for the floppy and network drives; this was mitigated by a handy toolbar where folders could be typed in manually for scanning.

With speed tests and on-demand scans completed in this manner, I came to the on-access tests, only to find little information about the on-access scanner. Fearing my discussions with the developers had been less than clear, I thought at first this must be an on-demand only scanner. Eventually, however, I discovered that the on-access component, the 'monitor', was enabled for some routes of ingress to the machine but not locally – options for 'file' and 'big file' monitoring needed to be enabled to make this happen. The system did not seem to be in place by default, and indeed was only active when the scanner GUI was, but also seemed to require a reboot to activate configuration changes.

After several false starts and confusing results however, an accurate set of statistics was obtained, with impressive detection in the zoo sets, but a sample of W32/Eyeveg missed in the ItW test set and a rash of false positives spoiled *Greatsoft*'s chance of a VB 100% award first time out of the blocks.

On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net for Windows Servers 6.0	0	100.00%	47	98.97%	626	90.48%	57	97.13%
Alwil avast! v.4.7	0	100.00%	18	99.56%	385	89.90%	30	98.74%
Avira AntiVir Windows Server 2003/2000/NT v. 6.35	0	100.00%	3	99.93%	0	96.37	150	100.00%
BitDefender Antivirus v.10	0	100.00%	13	96.69%	37	97.02%	10	99.27%
CA eTrust 8.0.403.0 (InoculateIT)	0	100.00%	4	99.90%	42	97.23%	1	99.82%
CA eTrust 8.0.403.0 (Vet)	0	100.00%	12	99.82%	103	94.26%	1	99.96%
CAT Quick Heal 2006 v.8.0	0	100.00%	73	98.23%	602	87.07%	98	96.51%
Command Authentium AntiVirus for Windows 4.93.8	0	100.00%	0	100.00%	2	99.93%	1	99.98%
Doctor Web Dr.Web v.4.33.2	0	100.00%	0	100.00%	9	98.08%	0	100.00%
Eset NOD32 2.5	0	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus for Windows Servers v.5.52	0	100.00%	0	100.00%	0	100.00%	3	99.85%
Fortinet FortiClient 3.0.001	0	100.00%	0	100.00%	277	84.47%	0	100.00%
FRISK F-Prot v.3.16f	0	100.00%	0	100.00%	2	99.93%	3	99.69%
GDATA AntiVirusKit 16.0.7	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Greatsoft Virusclean v.2.0.3286.3	1	99.85%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG Anti-Virus 7.1	0	100.00%	3	99.93%	414	82.59%	27	98.56%
Kaspersky Anti-Virus 5.0 for Windows File Servers v. 5.0.77.0	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kingsoft AntiVirus 2006 v.7.1	2	99.78%	358	78.31%	14043	14.70%	871	54.70%
McAfee VirusScan Enterprise 8.0	0	100.00%	0	100.00%	46	99.01%	0	100.00%
MicroWorld eScan Internet Security for Windows 8.0.673.1	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control v.5.82	0	100.00%	0	100.00%	309	92.76%	4	99.71%
NWI Virus Chaser v.5.0a	0	100.00%	4	99.90%	14	98.06%	13	98.96%
Sophos Anti-Virus v.6.03	0	100.00%	8	99.80%	1	99.86%	15	99.30%
Symantec AntiVirus 10.0.0.359	0	100.00%	0	100.00%	4	99.91%	0	100.00%
Trend Micro OfficeScan Corporate Edition v.7.3	0	100.00%	13	99.68%	851	94.42%	30	98.76%
TrustPort Antivirus 2.01.855	0	100.00%	0	100.00%	25	98.88%	0	100.00%
VirusBuster VirusBuster 2006 for Windows Servers v.5.2	0	100.00%	0	100.00%	628	92.00%	27	99.27%

Grisoft AVG Anti-Virus 7.1

ItW	100.00%	**Macro**	99.93%
ItW (o/a)	100.00%	**Macro (o/a)**	99.93%
Standard	98.56%	**Polymorphic**	82.59%

Installation of *AVG* was slowed down not only by the marathon licence code (totalling 31 characters, plus seven hyphens), but also by the absence of a necessary DLL in the default *Windows 2000* setup – MSVCP60.DLL, also required by many variants of W32/Mytob. With these hurdles overcome, and a restart suggested but not initiated by the

product, I was offered a tall, skinny GUI, with the option to switch to a more friendly 'Basic Interface'. Both of these were fairly straightforward to operate, and on-demand scanning surprised me only by the numbers of 'could be' lines in the log.

With good speeds and solid detection, only let down seriously by several misses in the polymorphic set, along with a miraculous lack of false positives, *Grisoft* earns itself a VB 100%.

Kaspersky Anti-Virus 5.0 for Windows File Servers v.5.0.77.0

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

Kaspersky's product came as a basic command-line operated system, with a GUI available for those who require it. With time pressing and many more products to come, I opted to skip this extra step, and ran through the tests using the simple and well documented command-line controls. After an initial test during which the product seemed consistently to ignore a single Mytob sample in the Wild set, a reinstall on a fresh machine soon smoothed out this odd quirk, and I was not surprised (given *GDATA*'s performance), to find another product capable of taking the entire test set in its stride. Only two files were missed across all collections, both zips in a zoo set not scanned by default on-access, and with no false positives *Kaspersky* racks up another VB 100% award.

Kingsoft AntiVirus 2006 v.7.1

ItW	99.78%	**Macro**	78.31%
ItW (o/a)	99.78%	**Macro (o/a)**	78.31%
Standard	54.70%	**Polymorphic**	14.70%

The second of the VB 100% first-timers arriving this month from China, although the first to hit the test bench, was provided by *Kingsoft* – a company whose primary output is computer games and office software. The product offered a fairly standard experience however, with a straightforward installation process remarkable only for a few odd uses of language.

The GUI, once up, was simple to operate, and on-demand scans were admirably rapid. Once completed, the set of infections detected was presented, along with the option to 'clean' them. Once this was rejected, and after some processing, the same list returned, this time with a 'quarantine' option, and then a third time with the offer to delete. With all these rejected, a log was provided which when parsed revealed very large numbers of misses across the zoo test sets.

The WildList, however, was handled much more impressively, with only two samples missed: a W32/Mytob and a Kakworm in .HTA format. These misses, along with no fewer than five false positives in the clean set, denied *Kingsoft* the VB 100% this time, but leaves the product looking a good contender for qualification in the near future.

McAfee VirusScan Enterprise v.8.0.0

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	99.01%

McAfee's product installed cleanly, and once done informed me that some components would require a reboot to be fully operational. These did not, it seems, include the on-access virus scanner, which appeared operational from the off.

The main GUI was simple and pared-down, but opened numerous other windows during the process of configuring and running a scan.

Speeds were impressive, although the on-access scanner was noticeably slow, and only one of the new polymorphic set prevented *McAfee* from taking a clean sweep of the infected sets. With no false positives either, *McAfee* joins the other high achievers on this month's VB 100% platform.

MicroWorld eScan Internet Security for Windows 8.0.673.1

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

Another product using the *Kaspersky* engine, *MicroWorld eScan* provided its own interface and also added in a little slowness over the scans of infected areas, although it achieved decent throughput over the clean sets.

On first attempt, a single file was missed on access, but I could not get this bad behaviour to repeat itself, and another VB 100% award is the result.

Norman Virus Control v.5.82

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.71%	**Polymorphic**	92.76%

Norman's installation was fast and simple, with no reboot required, but the GUI seemed over complex, with numerous windows used in the process of configuring and running a scan 'task'.

Throughput in the speed tests was somewhat slow in some areas and remarkably fast in others, while detection in the infected sets was mostly very good, missing a handful of standard viruses and a few sets of polymorphic samples. The WildList and clean sets were dealt with without a flaw, earning *Norman* a VB 100% award.

NWI VirusChaser 5.0a

ItW	100.00%	**Macro**	99.90%
ItW (o/a)	100.00%	**Macro (o/a)**	99.90%
Standard	98.96%	**Polymorphic**	98.06%

VirusChaser offers a rebadged invocation of the *Dr.Web* scanning engine, and much attention has been paid to the rebadging. After a fast and easy installation, with language options leaning towards the Asian market, there were options to tweak the GUI into any of a variety of pastelly shades for my visual pleasure.

Graphics were also configurable, and a choice of system tray icons for the on-access scanner was prominent, with *VirusChaser*'s own available as an alternative to the SpIDer. A disk usage monitor was one of a few innovative ideas added to the interface.

Scanning was decent, once the logs were discovered, although on-access seemed to offer little configuration and some unpredictable behaviour, and the product fared slightly less well than the engine it is built upon has proved itself capable of. Despite this, few infections were missed, with the entire ItW set detected, without false positives, and *VirusChaser* earns itself a VB 100% award.

Sophos Anti-Virus v.6.03

ItW	100.00%	**Macro**	99.80%
ItW (o/a)	100.00%	**Macro (o/a)**	99.88%
Standard	99.30%	**Polymorphic**	99.86%

The AV component of *Sophos*'s recently-released enterprise suite is not visibly very different from the previous version, apart from offering to install a firewall during the browser-style installation process.

The GUI, which feels a little lopsided and lacking in symmetry, was easy to use and scans were initiated without difficulty. The progress bar provided was a little misleading, hinting that a scan was 80% complete when the figures showed that less than half the files had been processed, and a change in the logging method meant that many files were labelled as part of an infection rather than merely an infection in themselves.

Despite these minor issues, with speeds good and only a single sample from a large set of new polymorphic types added to its usual low rate of misses, *Sophos* easily earns another VB 100%.

Symantec AntiVirus 10.0.0.359

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

Symantec required me once again to update the browser on my test machine, the minimum it supports being *IE 5.5 SP2*. With *IE* upgraded, the installation was speedy and efficient, with no rebooting and an automated scan of important areas.

The browser seemed necessary only for viewing reports, which showed a file in the clean set flagged as a 'security risk' during the speed tests, which were a little on the slow side. During scanning of the infected sets, this slowness increased dramatically; presumably encountering an infection triggers some super-in-depth analysis of the file in question, as the scan dragged on for a spectacular 4,700 minutes. This may have had something to do with on-access reactivating itself without my noticing.

Once logs for the four days were gathered, rejoined and parsed, a tiny handful of polymorphic viruses were the only misses, and a VB 100% was earned without difficulty.

Trend Micro OfficeScan Corporate Edition 7.3

ItW	100.00%	**Macro**	99.68%
ItW (o/a)	100.00%	**Macro (o/a)**	99.68%
Standard	98.76%	**Polymorphic**	94.42%

Trend's installation process was by far the most complex of all the products, with numerous dialogs offering and requesting information on a huge array of components and functions. This product also required a browser upgrade, this time *IE 5.5 SP1* being the minimum.

The client side was adequate for many tests, its big fat buttons and chunky checkmarks making setting things up fairly foolproof, but the 'options' button was greyed out and the server console was needed for more advanced configuration.

Having zipped through the speed tests, the machine got a little bogged down towards the end of a hefty scan of infected collections, but soon recovered. Several alerts were issued for items found in the quarantine folder, rather confusingly, and detection in the polymorphic set was a little disappointing, but in the end the WildList viruses were all found and the clean set produced no surprises, resulting in a VB 100% award for *Trend Micro*.

Trustport AntiVirus 2.01.855

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	98.88%

Trustport is another product combining two engines from separate providers, along with some useful functionality of its own, and controls them from a useable GUI, marred only by the occasional bit of odd English and some strange logging behaviour – including reporting times for scans seemingly unrelated to the system time.

The combination of *BitDefender* and *Norman* engines worked well for *Trustport*, giving better detection rates across the zoo sets than either provider on its own, but of course it also suffered the same false positive as *BitDefender*, rendering its flawless detection of ItW viruses inadequate to earn it the VB 100%.

VirusBuster VirusBuster 2006 for Windows Servers v.5.2

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.27%	**Polymorphic**	92.00%

After a straightforward installation process, *VirusBuster* offers a selection of GUIs, including a Microsoft Management Console (MMC) based configuration system, opened from the desktop shortcut provided, and a more user-friendly scanner control, somewhat confusingly entitled the 'console' and opened from the system tray menu.

After a slightly complicated setup process, scanning speeds were decent, although a file in the clean set snagged the product rather nastily and another was reported 'suspicious'. These issues aside, detection rates were very good, and another VB 100% award is due to *VirusBuster*.

CONCLUSIONS

With such a huge raft of entries to test, time to analyse individual products in detail was a little short, but a few broad patterns seemed to emerge. There appeared to be a fairly distinct divide between the products that thought they knew best, and provided little chance to conform their behaviour to suit an individual's requirements, and those that seemed aimed more firmly at the expert or corporate user, and thus provided a wealth of detailed levels of configurability. On either side of this divide detection rates were generally strong, although the small handful of new samples introduced managed to sneak something past most of the entries.

Most noticeable was the large number of false positives, an effect not helped by many other products running one or other of the engines affected by them. All of these were in the older part of the clean set, and so should have been inspected many times before by most of these products. The exceptions to this, the two new entries, unsurprisingly suffered most heavily from false positives, but also missed out where it matters most, in the WildList. Hopefully all these issues will soon be resolved by the respective vendors. A select few can, of course, walk away with their heads held high.

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 2000 Server*, service pack 4.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win2K/2006/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

Any developers interested in submitting products for VB's comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.