COMPARATIVE REVIEW

WINDOWS SERVER 2003

Matt Ham

Windows 2003 Server is now an environment which can be considered mature. Furthermore, there were no major problems encountered during the last comparative review to be carried out on this platform (see *VB*, November 2003, p.13). With these factors in mind I had my hopes set on what might be a more relaxing review period than usual. Sadly, however, my hopes were dashed by the arrival of the test sets.

THE TEST SETS

The test sets were based on the most recent version of the (RealTime) WildList available on 6 October 2004, the deadline for product submission having been 8 October. However, three months had passed since the last comparative review (and the last maintenance of the test set), and that was sufficient time for close to 90 new worms to have been added to the In the Wild (ItW) category. The preponderance of all-but-identical worms in, for example, the W32/Sdbot, W32/Rbot, W32/Agobot and W32/Korgo families made replication a particularly mind-numbing process.

These additions are sufficiently irritating to name that the WildList Organization has taken to using checksum values to describe versions. They also add very little, if anything, to the difficulty of their detection. Although many are packaged in layer upon layer of obfuscating archive, the files themselves are easily recognisable. With this in mind, a bumper crop of VB 100% awards was expected.

Alwil avast! 4.5.286

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

Nov 2004
100%
VIRUS BULLETIN
www.virusbtn.com

The review of *avast!* began with a sinking feeling, since the on-access scanner refused to load. This turned out to be a result of it starting as a service under the local administrator account. *Windows* refused to allow this to happen since the default image used for *Windows 2003* testing has no password. This was easily remedied by changing to the system account. The problem can be discounted as an issue in the real world – except for administrators who have no passwords on their servers. Such folk, however, are likely to

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	112	93.58%	18	99.17%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	5	99.58%
BLC Win Cleaner	0	100.00%	0	100.00%	100.00%	87	97.92%	1087	92.85%	506	71.49%
CA eTrust Antivirus (InoculateIT)	0	100.00%	0	100.00%	100.00%	3	99.93%	2	99.78%	3	99.69%
CA eTrust Antivirus (Vet)	1	99.73%	0	100.00%	99.73%	12	99.82%	2	99.87%	5	99.60%
CA Vet Anti-Virus	1	99.73%	0	100.00%	99.73%	0	100.00%	2	99.87%	5	99.60%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	87	97.92%	1087	92.85%	506	71.49%
DrWeb DrWeb	2	99.45%	0	100.00%	99.46%	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%	1	99.82%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	201	95.52%	5658	61.51%	86	97.58%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	4	99.60%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	7	99.49%
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%	6	99.84%	271	98.74%	24	98.93%
Hauri ViRobot	0	100.00%	0	100.00%	100.00%	8	99.80%	8	99.69%	10	99.54%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	14	99.51%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	181	91.03%	11	99.63%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	9	99.78%	6	99.73%	23	99.05%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	15	99.30%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend ServerProtect	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.66%
UNA UNA	69	89.10%	4	0.00%	88.14%	1993	52.72%	14267	20.14%	584	72.98%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.45%	16	99.17%

find this the least of their problems. A more concerning issue was observed when the on-access scanner claimed to have crashed while scanning the test sets. However, the failure appeared to have been non-critical since the remainder of the test set was scanned with no problems. With minor glitches as the only moments of note, it will come as no surprise that *avast!* receives a VB 100 % award on this occasion.

Authentium Command AntiVirus 4.92.1

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

There is far less to comment upon where *Command AntiVirus* is concerned. All misses are those which will be

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	112	93.58%	15	99.36%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	2	99.72%
BLC Win Cleaner	0	100.00%	0	100.00%	100.00%	80	98.05%	1087	92.85%	169	92.91%
CA eTrust Antivirus (InoculateIT)	0	100.00%	0	100.00%	100.00%	3	99.93%	0	100.00%	1	99.82%
CA eTrust Antivirus (Vet)	1	99.73%	0	100.00%	99.73%	13	99.78%	2	99.87%	3	99.72%
CA Vet Anti-Virus	1	99.73%	0	100.00%	99.73%	0	100.00%	2	99.87%	3	99.72%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	80	98.05%	1087	92.85%	506	71.49%
DrWeb DrWeb	1	99.73%	0	100.00%	99.73%	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%	1	99.82%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	201	95.52%	5658	61.51%	86	97.58%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	2	99.72%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
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%	26	98.74%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	6	99.84%	271	98.74%	24	98.87%
Hauri ViRobot	0	100.00%	0	100.00%	100.00%	8	99.80%	4	99.78%	14	99.17%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	1	99.73%	0	100.00%	99.73%	2	99.95%	180	91.24%	5	99.69%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	9	99.78%	6	99.73%	22	99.23%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	15	99.30%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend ServerProtect	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	9	99.72%
UNA UNA	64	89.62%	4	0.00%	88.65%	1712	58.90%	14246	21.08%	537	75.21%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	102	91.45%	13	99.31%

painfully familiar to regular readers of the *VB* comparatives – a selection of samples missed entirely as a result of choices made by the developer based on product efficiency, rather than the product being unable to detect them. One problem that did occur here, however, was in the production of logs, since the original rtf log was mysteriously truncated. Results were therefore obtained by deletion. The award of a VB 100% duly followed.

BLC Win Cleaner 7.02

ItW Overall	100.00%	**Macro**	98.05%
ItW Overall (o/a)	100.00%	**Standard**	92.91%
ItW File	100.00%	**Polymorphic**	92.85%

Business Logic Corporation is a name that is new to the VB 100% testing roll call, though its pedigree is instantly recognisable when installed. The product is both functionally and, in all but a few strategically placed logos, visually identical to the *CAT* product from which *Win Cleaner* (*WC*) is derived. Despite its rather unfortunate acronym, *WC* denied any opportunity for jokes at its expense by detecting all viruses in the ItW test set. With no false positives, *Win Cleaner* earns a VB 100% award on its first appearance.

CA eTrust Antivirus 7.1.192

ItW Overall	99.73%	**Macro**	99.78%
ItW Overall (o/a)	99.73%	**Standard**	99.72%
ItW File	99.73%	**Polymorphic**	99.87%

It has been noted on several occasions that *eTrust* can operate with either the *InoculateIt* or *Vet* engines, both being supplied in a standard installation. On this occasion both engines were tested, with the intention of comparing their performance (see box). Currently the default installation is the *Vet* engine, which missed one of the W32/Agobot samples in the ItW test set. This was enough to deny *eTrust* a VB 100% award when used with the *Vet* engine. The logging facility of the product in either incarnation remains an affront to sanity, there being no real means to obtain logs which are readable to either machine or human.

CA Vet Anti-Virus 10.64.0

ItW Overall	99.73%	**Macro**	100.00%
ItW Overall (o/a)	99.73%	**Standard**	99.72%
ItW File	99.73%	**Polymorphic**	99.87%

This offering from *CA* contains the same engine as the previous offering, yet has a very different interface. Scanning here was in most cases slightly slower than the product's *eTrust* counterpart – except on the zipped OLE files, where the *Vet* product was considerably speedier. With the same engine inside the product, it should come as no surprise that the scanning results were the same for both *Vet*-based products and, of course, the miss of the W32/Agobot sample in the ItW test set denies *Vet* a VB 100% on this occasion.

CAT Quick Heal 7.02

ItW Overall	100.00%	**Macro**	98.05%
ItW Overall (o/a)	100.00%	**Standard**	71.49%
ItW File	100.00%	**Polymorphic**	92.85%

CA eTrust Antivirus 7.1.192 (InoculateIT engine)

ItW Overall	100.00%	**Macro**	99.93%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	100.00%

As noted in the text, the *eTrust* product can operate with either the *InoculateIt* or *Vet* engines, and on this occasion both engines were tested, with the intention of comparing their performance.

The *InoculateIT* engine, which is not currently the standard installation, performed much as expected. This included missing samples of W97M/Pain.A (a strange miss considering the otherwise full detection of macro viruses). Despite this, detection was, in general, very good and a VB 100% award would be obtained easily with the product using the *InoculateIT* engine.

As far as scanning speed is concerned, *eTrust* is marginally faster when using the *Vet* engine than when using the *InoculateIT* engine.

One other item of note was observed while testing: it seems to be possible to operate *eTrust* with one engine operating on demand and the other operating on access.

With a derived product (*Win Cleaner*) having already obtained a VB 100% in this comparative, it will come as no shock to learn that *Quick Heal* also earns a VB 100% award this month. Strangely, despite an otherwise identical performance, the *CAT* product was slightly slower than the *Business Logic* version.

Doctor Web Dr.Web 4.32a

ItW Overall	99.73%	**Macro**	100.00%
ItW Overall (o/a)	99.46%	**Standard**	100.00%
ItW File	99.73%	**Polymorphic**	100.00%

Dr.Web is now produced by Russian company *Doctor Web* rather than *DialogueScience*. Uncharacteristically, *Dr.Web* missed a sample of W32/Flopcopy, a sample located in the ItW test set, and was thus prevented from earning a VB 100% award. The slightly better news was that the product generated no false suspicious files, which has not been the case for a while.

Eset NOD32 1.889

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**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)
Alwil avast!	99	5524.6		12	6611.1		21	7591.3	9	8289.7
Authentium Command	114	4797.7		5	15866.8		50	3188.3	5	14921.5
BLC Win Cleaner	62	8821.5		15	5288.9		48	3321.2	18	4144.9
CA eTrust Antivirus (InoculateiT)	132	4143.4		4	19833.4		58	2748.6	9	8289.7
CA eTrust Antivirus (Vet)	141	3879.0		4	19833.4		66	2415.4	11	6782.5
CA Vet Anti-Virus	144	3798.1		6	13222.3		68	2344.4	3	24869.2
CAT Quick Heal	72	7596.3		15	5288.9		50	3188.3	25	2984.3
DrWeb DrWeb	194	2819.2		15	5288.9		63	2530.4	12	6217.3
Eset NOD32	49	11161.9		7	11333.4		29	5497.1	8	9325.9
Fortinet FortiClient	77	7103.0	1	12	6611.1		21	7591.3	13	5739.0
FRISK F-Prot Antivirus	139	3934.8		5	15866.8		55	2898.5	4	18651.9
F-Secure Anti-Virus	129	4239.8		15	5288.9		86	1853.7	23	3243.8
GDATA AntiVirusKit	672	813.9	[1]	18	4407.4		305	522.7	20	3730.4
Grisoft AVG	145	3771.9		8	9916.7		59	2702.0	9	8289.7
H+BEDV AntiVir	420	1302.2		14	5666.7		210	759.1	17	4388.7
Hauri ViRobot	536	1020.4	20 [2]	14	5666.7		-	-	28	2664.6
Kaspersky KAV	164	3335.0		15	5288.9		77	2070.3	18	4144.9
McAfee VirusScan	93	5881.0		8	9916.7		64	2490.9	15	4973.8
MicroWorld eScan	286	1912.4		23	3449.3		115	1386.2	46	1621.9
Norman Virus Control	345	1585.3		5	15866.8		144	1107.1	6	12434.6
SOFTWIN BitDefender	591	925.4	[1]	8	9916.7		242	658.7	8	9325.9
Sophos Anti-Virus	56	9766.6		10	7933.4		42	3795.6	11	6782.5
Symantec SAV	149	3670.7		21	3777.8		69	2310.4	21	3552.7
Trend ServerProtect	74	7391.0		8	9916.7		32	4981.8	10	7460.7
UNA UNA	80	6836.7	2 [1]	19	4175.5		110	1449.2	34	2194.3
VirusBuster VirusBuster	185	2956.4		7	11333.4		120	1328.5	14	5329.1

Coming very close to full detection of all samples in all test sets, *NOD32* continues to be entitled to quote its unblemished record of ItW detection on its marketing materials. If a failure in this area does ever occur, I am sure that the printers of *Eset*'s marketing materials will be as happy as *Eset* will be sad. With no incidents of note during testing, I can only congratulate Eset on another VB 100% award.

Nov 2004 100% VIRUS BULLETIN www.virusbtn.com

Fortinet FortiClient 1.2.130

ItW Overall	100.00%	**Macro**	95.52%
ItW Overall (o/a)	100.00%	**Standard**	97.58%
ItW File	100.00%	**Polymorphic**	61.51%

This product's detection has improved in leaps and bounds since first being submitted for *VB* testing a few months ago.

On this occasion all samples from the ItW test set were detected, the only real weaknesses in detection lying in the polymorphic test set. However, the improvement in detection has not come without a further false positive, which is sufficient grounds to deny *FortiClient* a VB 100% by the narrowest of margins. One suspects that it is merely a matter of when, rather than if, this situation will change for the better.

FRISK F-Prot Antivirus 3.15 b

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

A product with a far longer history behind it, logical readers will have already been able to guess much about *F-Prot*'s performance from the performance of *Command* earlier in the testing. Indeed, like *Command*, *FRISK*'s product is eligible for another VB 100% award.

F-Secure Anti-Virus 5.50

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

Since this product also makes use of *FRISK*-derived detection, the fate of *F-Secure Anti-Virus* is also fairly easy to predict – full detection and no false positives mean that the product earns a VB 100% award.

GDATA AntiVirusKit 14.0.8

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

Another example of repackaged engines, *AVK* is one of the older players in this area. One concern about the use of two engines might be an increase in the likelihood of false positives. On this occasion the product did alert on a clean file, although it was identified only as suspicious, rather than being a full blown false positive. The combination of *BitDefender* and *Kaspersky* engines in *AVK* seems a good choice; on this occasion all samples in all test sets were detected and *AVK* receives a VB 100% award.

Grisoft AVG 7.0.275

ItW Overall	100.00%	**Macro**	99.51%
ItW Overall (o/a)	100.00%	**Standard**	98.74%
ItW File	100.00%	**Polymorphic**	85.97%

Returning to products which are tested in only one incarnation, *Grisoft*'s *AVG* is the next in line. Misses here were, as ever, in the more complex variety of polymorphic virus. These polymorphics do tend, however, to be restricted to zoo collections rather than breaking into the wild. This does not, therefore, make a dent in the product's ItW detection rate. False positives were the cause of a temporary glitch in *AVG*'s performance a few months ago, but this seems very much consigned to history now. As a result, a VB 100% award wings its way towards *Grisoft*.

H+BEDV AntiVir Windows Server 6.28.0.101

ItW Overall	100.00%	**Macro**	99.84%
ItW Overall (o/a)	100.00%	**Standard**	98.87%
ItW File	100.00%	**Polymorphic**	98.74%

AntiVir's GUI is distinctive, in that is seems to have been designed for server use at the expense, in certain aspects, of user-friendliness. Since scheduled scans are stressed, which can be run in the background, there is little in the way of immediate user feedback on scans, for example. When scanning the clean test set, several files were flagged as 'possibly destroyed by a virus' but not considered to be suspicious or infected in any way. Detection was full in the ItW test sets, thus earning a VB 100% award for *H+BEDV*.

Hauri ViRobot Advanced Server

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Standard**	99.17%
ItW File	100.00%	**Polymorphic**	99.78%

Hauri's detection has been improving over recent tests and this occasion was no different. On the other side of the equation, however, the new detection has come at a cost. A full 20 false positives were noted along with two suspicious files in the clean test set. Most of these were for HLLC.Fataller, a name I have heard far more often during false positive testing than on any other occasion. Given that one false positive is causing much of the problem, it seems likely that this issue will be resolved soon, but in the meantime *ViRobot* is denied a VB 100% award.

Kaspersky KAV 4.5.0.97

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

Kaspersky AntiVirus (*KAV*) is one of those products where different names for different components are the order of the day. The version number given above is that for the main scanner – other components all being in the 4.5.0.9x region. *KAV* continues to behave smoothly and without any other cause for major comment. With full detection In the Wild and no false positives a VB 100% is awarded to the *Kaspersky* product.

McAfee VirusScan Enterprise 8.0.0 4396

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

McAfee's product is another which has been reviewed a sufficient number of times for no surprises to be expected. Indeed, all requirements for a VB 100% award were reached without problems. However, strange matters arrived to pique the interest somewhat. In this case it was the log file which perplexed, since all viruses detected seemed to have been detected twice.

MicroWorld eScan 2003

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

This product is a rebadge of *AVK*, thus like *AVK* it is derived from *BitDefender* and *Kaspersky* engines. *eScan*'s results rarely differ extensively from those expected as a result of its ancestry. Scanning here was notably faster on executables than *AVK*'s scanning speed, though the difference was reversed on OLE files. It was also notable that *AVK*'s declaration of a suspicious file was not mirrored here, suggesting that tweaks have been made behind the scenes. The differences were not, however, continued into the area of detection.

With full detection of all files and no false positives a VB 100% is a sure result for *MicroWorld*.

Norman Virus Control 5.70

ItW Overall	99.73%	**Macro**	99.95%
ItW Overall (o/a)	100.00%	**Standard**	99.69%
ItW File	99.73%	**Polymorphic**	91.24%

Norman Virus Control is another of those products which usually presents no problems at all, though on this occasion it elicited at least one surprise. Unfortunately this was not a particularly pleasant one for the developers, since it was a miss of BAT/Mumu. This is a particularly surprising miss, considering its relative age and its location in the ItW test set. This, of course, prevents *Norman* from obtaining a VB 100% award.

SOFTWIN BitDefender 8 Professional Plus

ItW Overall	100.00%	**Macro**	99.78%
ItW Overall (o/a)	100.00%	**Standard**	99.23%
ItW File	100.00%	**Polymorphic**	99.73%

One of the components of *AVK*, it came as no surprise that *BitDefender* declared a suspicious file in exactly the same location as that product – though, again, this was not one serious enough to negate the possibility of a VB 100% award. *BitDefender* did miss slightly more samples than its hybrid offspring, but none of these were likely to become an issue In the Wild. Not unexpectedly, a VB 100% was earned for this combination of detection and lack of false detection.

Sophos Anti-Virus 3.83

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

There was much rejoicing when reviewing *Sophos Anti-Virus* on this occasion, since the perennially irritating log format seems at last to have been brought up to date – simplifying log parsing immensely.

Sophos's detection rate is approaching full in all categories too. With no problems with regard to detection or false positives, *SAV* obtains a VB 100% award – and I regard the product with somewhat less antipathy.

Symantec SAV 9.0/0.338

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

Nov 2004 100% VIRUS BULLETIN www.virusbtn.com

Symantec's *SAV* continues to be one of the slower scanners when faced with infected files, the volume of its log files potentially bearing some responsibility for this. With each virus report occupying an average of 230 bytes, test sets numbering several tens of thousands of samples tend to imply vast log files. Such logs were sufficient, in fact, to crash the client when scanning had completed. Despite this (admittedly lab-specific) behaviour, the rates of detection and lack of false positives for *SAV* remained at their usual high levels such that a VB 100% award is appropriate.

Trend ServerProtect 5.58(1060)

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.72%
ItW File	100.00%	Polymorphic	95.77%

Nov 2004 100% VIRUS BULLETIN www.virusbtn.com

Trend Micro's product is among the more complex to install, since it is inextricable from its management software. A certain degree of fiddling is required to install update files and it tends to lose, among administrative options, the simple commands required during comparative testing. However, these complaints would be irrelevant to a real-world administrator who might be expected to concentrate on the grand scale as well as detection and false positives. Detection remained slightly under par on polymorphic samples, though full in the ItW test set, justifying the award of a VB 100% to *Trend*.

UNA UNA 1.83 Kernel 255

ItW Overall	88.65%	Macro	58.90%
ItW Overall (o/a)	88.14%	Standard	75.21%
ItW File	89.62%	Polymorphic	21.08%

Still a relative newcomer to the *VB* tests, the *UNA* product seems to have improved markedly in its ease of testing – though this may simply be a function of extra practice. False positive rates have certainly become less of a problem and new detections have been added in the test sets. Though there is still a considerable way to go until the product will achieve a VB 100% award, *UNA*'s developers have shown that this might be possible in time.

VirusBuster VirusBuster 4.7 build 18

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.31%
ItW File	100.00%	Polymorphic	91.45%

Nov 2004 100% VIRUS BULLETIN www.virusbtn.com

Last, but in the way of time-honoured cliches, by no means least, *VirusBuster*'s product leaves me scraping the barrel for worthwhile comments once more. At times such as these it pays to be called Aardvark Antivirus for sure. *VirusBuster* easily qualifies for a VB 100% award, with no false positives generated and misses being noticeable only among the more complex polymorphic samples.

CONCLUSION

The theory that the new worm samples included in the test sets would cause few problems turned out, by and large, to be correct – though there were a few surprising exceptions for usually steadfast products. In many similar cases in the past this has turned out to be due to the developers having a sample which they believe to be In the Wild and which their product can detect, while in fact a different sample is generally considered to be In the Wild. Whether this is the case here remains to be seen.

The lack of stability issues in *Windows 2003* that was seen in last November's comparative followed through on this occasion. *Microsoft* has been working ever more closely with anti-virus developers over the last few years and this could well be the reason behind the added stability. Platform stability certainly simplifies the matter of testing and can hardly be a bad thing as far as the real world is concerned either. The optimist in me dares to hope that this will be the case ever more as new operating systems are created, though the pessimist still tells me that major unforeseen disasters will be in store.

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 Server 2003 Web Edition V5.2 Build 3790.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win2K/2004/test_sets.html.

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

ERRATA – WINDOWS SERVER 2003 COMPARATIVE REVIEW

VB regrets that three mistakes crept into the Comparative review published in the November issue:

- The version number for *Sophos Anti-Virus* should have read 3.86, not 3.83 as published.
- The values for *CAT Quickheal* in the standard on-demand test set should read 'Misses: 169, Detection 92.91%' in all occurrences (the on access results were erroneously duplicated).
- *Norman Virus Control* did not reproducibly miss detection of any samples in the In the Wild test set and thus is due a VB 100% award.

VB apologises for the errors.