COMPARATIVE REVIEW

WINDOWS NT 4.0

Matt Ham

With the number of *Windows* platforms that are officially supported by *Microsoft* on the decrease, it is sometimes a knotty problem deciding which platforms should be included in *Virus Bulletin* comparative testing. DOS testing is now a thing of the past, and *Windows Me* looks very much as if it too has reached the graveyard of antiquated operating systems. Personally, I had expected to see *Windows 98* being administered the last rites this year – however, it seems that *Windows NT* will officially be killed off first. This raises the question as to why *VB* has decided to test AV products on *Windows NT*, when *Windows 98* is apparently a more thriving platform.

The answer is twofold. First, the schedules for testing are planned well in advance, and the demise of *NT* as a *Microsoft*-supported system was not made clear until after the schedule had been set. The second, and more significant reason, is the fact that the decision by *Microsoft* to remove support from an OS is not necessarily an indication of that OS becoming extinct in the wild. From a marketing point of view, *NT* users are likely to upgrade to *XP* if *NT* is no longer supported. *NT* was always much stronger among corporates than in the home-user environment and, in a large company, expense is not always as significant a consideration as continuity and the ability to make long term plans. On balance, although doomed to lack of support in the near future, *NT* is still a rather more relevant platform for business users.

TEST SETS

The test sets used in this review were the first to be aligned to the real-time WildList and as such were expected to provide rather more of a challenge for the products than the test sets used in past reviews. Unfortunately, both the *VB2003* conference and the Christmas period conspired to cause delays in the updating of the real-time WildList and, on the date when the test set was finalised, the ‘real-time’ WildList was updated only as far as late October 2003. In future reviews the test set will be derived from the real-time WildList two days prior to the test deadline, with the hope that it will pose greater challenges for the products under test.

AhnLab V3VirusBlock

ItW Overall	100.00%	**Macro**	98.08%
ItW Overall (o/a)	100.00%	**Standard**	85.57%
ItW File	100.00%	**Polymorphic**	43.19%

Over the year since its debut in the *VB* comparative review line-up, the detection rates of *V3* in its various incarnations have improved in all test sets. Admittedly this improvement is only by a few percentage points in each category, but with the most significant improvement in the ItW set, *V3VirusBlock* gains a VB 100% award.

Alwil Avast! 4.1.319

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	N/A	**Standard**	99.10%
ItW File	100.00	**Polymorphic**	93.54%

Changes to *Alwil*'s on-access scanner caused problems during the last review of the product (see *VB*, November 2003, p.13) and it proved troublesome again this time. With the configuration options available it is impossible to activate on-access scanning for many file types unless the files are executed. Clearly, this is infeasible when dealing with tens of thousands (or even merely dozens) of samples in a test environment. Therefore, the on-access file capabilities of *Avast!* were untestable. Where on-demand scanning was concerned the results were good – unfortunately without on-access results the product does not qualify for a VB 100% award.

Authentium Command AntiVirus 4.90.2

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

A familiar product from a new company, *Command AntiVirus* performed much the same as it ever has, earning a VB 100% award in the process. Casting back to the results of the February 2003 comparative review (see *VB*, February 2003, p.16), this product (along with many others) missed the polymorphics W32/Tuareg.B, W32/Zmist.D and W32/Etap.A. Of these previously problematic viruses only a single Zmist sample was missed this time. This is a good sign that progress is being made in the more complex areas of virus detection technology.

CA eTrust Antivirus 7.0.142

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

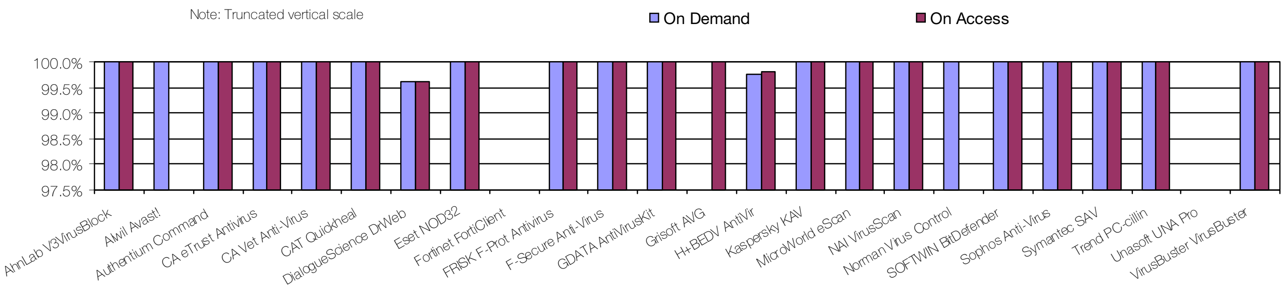
The samples missed by *eTrust Antivirus* on this occasion were very much the same as those missed last year, and with no misses in the ItW test set, another VB 100% is on its way to *Computer Associates*. Still disappointing, however, is the new log file functionality, which renders production of parseable result files an impossibility. In a very low-tech workaround the software was set up to log missed samples (which were few in number), and the results were stored in a screen shot for later reference.

CA Vet Anti-Virus Protection 10.59.2.1

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.90%
ItW File	100.00%	**Polymorphic**	99.87%

Vet's results were sufficient to warrant a further VB 100% award for *CA*. Although there is little perceptible change in *Vet*'s detection performance since this time last year, there has been a notable slowing of scanning speed over that period.

In the Wild File Detection Rates



CAT Quickheal X Gen 7.00

ItW Overall	100.00%	**Macro**	97.49%
ItW Overall (o/a)	100.00%	**Standard**	83.33%
ItW File	100.00%	**Polymorphic**	95.12%

In the last *NT* comparative, *CAT*'s detection was skewed very much in favour of ItW viruses, with a distinctly second-rate level of detection in other areas. This skew seems to have been ironed out over the course of the year, although the one remaining weak area is the polymorphic set, especially where on-access scanning is concerned. However, the detection rate of ItW files has improved, rendering *Quickheal* eligible for another VB 100% award.

DialogueScience Dr.Web 4.30a

ItW Overall	99.60%	**Macro**	100.00%
ItW Overall (o/a)	99.60%	**Standard**	100.00%
ItW File	99.59%	**Polymorphic**	100.00%

Dr.Web continues to surprise with the number of suspicious files it notes. Not because the number is excessively large but because the number of such files seems to vary from virtually zero to the mid-teens. A more disturbing surprise was that the product missed BAT/Mumu.A in the ItW test set. This missed detection was checked several times, both on access and on demand, and proved to be reproducible. *Dr.Web* is thus denied a VB 100% award on this occasion.

Eset NOD32 1.595

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

This month sees another addition to *Eset*'s growing collection of VB 100% awards. With 100 per cent detection in all categories and no false positives, *NOD32* fails to pull any surprises out of the bag.

Fortinet FortiClient 1.0.048

ItW Overall	95.55%	**Macro**	43.10%
ItW Overall (o/a)	95.39%	**Standard**	27.40%
ItW File	99.10%	**Polymorphic**	23.44%

Fortinet's *FortiClient* is not designed primarily as an AV product, although this functionality is prominent in its GUI. Unfortunately, the degree to which it detects viruses is not very impressive. Admittedly, the product's detection rates for ItW viruses are close to acceptable, and this, presumably, is the area in which the developers have decided to concentrate their efforts. Among polymorphic and standard viruses, the detection rate is so poor it is barely worth mentioning. In addition to poor detection rates the product announced an exception when scanning the clean OLE file test set. To its credit, though, this was cleanly trapped and dealt with, without a blue screen being triggered.

FRISK F-Prot Antivirus 3.14 b

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.74%
ItW File	100.00%	**Polymorphic**	99.91%

It is generally the case that rebadged products detect either identically to, or slightly less well than their parent products. Since *FRISK* supplies the engine for *Command AV* – already the recipient of a VB 100% – this should be a good omen for *F-Prot*. Indeed this proved to be the case, since *F-Prot* achieved full detection in the wild and leaves the test with a new VB 100%.

F-Secure Anti-Virus Client Security 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 *Command AV*, *F-Secure* also uses the *FRISK* engine, along with that of *Kaspersky* – and it would be quite an embarrassment were this product to fail to earn a VB 100% where the others succeeded. Happily, the *F-Secure* product met all the requirements for a VB 100% award.

GDATA AntiVirusKit 14.0.2

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

A chimera of the *SOFTWIN* and *Kaspersky* engines, *AVK*'s scanning results are no cause for concern for either company, since all files in every test set were detected without problem. A momentary panic on the clean test sets was

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3VirusBlock	0	100.00%	0	100.00%	100.00%	82	98.08%	9139	43.19%	313	85.57%
Alwil Avast!	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	4	99.76%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	2	99.88%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	4	99.78%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	107	97.45%	1086	92.85%	647	61.99%
DialogueScience Dr.Web	1	99.59%	0	100.00%	99.60%	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	9	98.94%	9	0.00%	95.39%	2328	43.10%	12524	23.44%	1226	27.40%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	3	99.79%
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%	30	98.50%
H+BEDV AntiVir	1	99.79%	0	100.00%	99.80%	56	99.26%	1004	84.94%	52	97.91%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.88%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	13	99.69%	11	97.46%	60	97.79%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	1	99.95%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.82%
Unasoft UNA Pro	157	76.03%	9	0.00%	73.30%	3048	26.88%	14446	11.67%	904	57.30%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.78%	8	99.82%

averted since the single false positive was a warning rather than a full blown erroneous detection, thus leaving *AVK* with a VB 100% award and its component engine developers with high hopes.

Grisoft AVG Anti-Virus 7.0

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

ItW File	N/A	Polymorphic	N/A

AVG has undergone a major version change recently, bringing with it numerous changes in the look and feel of the product. The majority of these changes are positive in nature, having made the product more intuitive. There is, however, an area in which the changes have been less desirable. Currently it is only possible to automatically disinfect or log files detected as being infected. Where disinfection is impossible – for example in the case of all worms – the files will remain on the machine and at this point they must be removed manually, one by one. This, when combined with no provision for exportable logs of any great size, was sufficient to make on-demand detection testing (and consequently the chance to earn a VB 100% award) impossible. A VB 100% would have been ruled out in any case due to several false positives.

H+BEDV AntiVir 6.22.00.09

ItW Overall	99.77%	Macro	99.53%
ItW Overall (o/a)	99.80%	Standard	98.03%
ItW File	99.76%	Polymorphic	84.94%

Not having taken part in last year's review, *AntiVir* can also be considered as something of a newcomer, though it has been tested in the distant past and as part of the *Linux* review process. Detection rates for the product were good overall, only polymorphics showing signs of weakness. Unfortunately, however, there were several misses in the ItW test set. These were the DLL portion of VBS/Redlof.A and the extensionless samples of O97M/Tristate.C. Since the latter was detected on access this was clearly an issue of extensions.

Kaspersky Anti-Virus 4.5.0.94

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

After disabling its soul-wrenching sound effects *KAV* is always a pleasant product to deal with. Since the last review even the most pesky of the remaining polymorphics have been rendered detectable by the *KAV* engine, leaving only the zipped samples of W32/Heidi.A as undetected on access. Since this is a result of not scanning ZIP archives on access (which is entirely understandable), detection rates can be considered all but perfect. With no false positives, *KAV* has gained a VB 100%.

Feb 2004 100% VIRUS BULLETIN www.virusbtn.com

MicroWorld eScanWin 1.3

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

Consisting of a rebadge of the *GDATA* product, it might be expected that the results obtained by *eScan* would be similar to those of its parent product. Happily for *MicroWorld* this did indeed prove to be the case. The outcome of this review is a far cry from that of a year ago, when *eScan* suffered from a bizarre loss of detection and demonstrates that any teething troubles are now well behind the product. Little more remains, therefore, other than to pass a VB 100% in *eScan*'s direction.

Feb 2004 100% VIRUS BULLETIN www.virusbtn.com

NAI VirusScan Enterprise 7.1.0 4.3.20 4113

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

Causing confusion with ever-mutating name, *NAI*'s product makes up for this foible by maintaining a consistent interface over all of its incarnations. This is not the only area where consistency has been achieved, with the detection rate also remaining uniformly high. Since false positives have never been a problem for *NAI* during my experience of testing, this results in a VB 100% for *Network Associates*.

Feb 2004 100% VIRUS BULLETIN www.virusbtn.com

Norman Virus Control 5.7

ItW Overall	100.00%	Macro	99.95%
ItW Overall (o/a)	N/A	Standard	99.89%
ItW File	100.00%	Polymorphic	91.72%

The *Norman* team seems to be somewhat cursed with strange bugs when it comes to *VB* testing. This time the problem lay in the on-access portion of the tests. When running the on-access scanner over the infected test sets, the number of files detected was at variance each time with the previous occasion.

Having run the tests some ten times without any form of pattern having emerged, on-access testing was abandoned. Unfortunately this means that a VB 100% award is beyond the reach of the product on this occasion, despite all other results being good.

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3VirusBlock	0	100.00%	0	100.00%	100.00%	82	98.08%	9139	43.19%	313	85.57%
Alwil Avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	124	93.54%	23	99.10%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	1	99.91%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	2	99.90%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	103	97.49%	1044	95.12%	310	83.33%
DialogueScience DrWeb	1	99.59%	0	100.00%	99.60%	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	9	99.10%	9	0.00%	95.55%	2328	43.10%	12524	23.44%	1226	27.40%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	5	99.74%
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	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
H+BEDV AntiVir	2	99.76%	0	100.00%	99.77%	31	99.53%	1004	84.94%	50	98.03%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI 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%	174	91.72%	3	99.89%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	13	99.69%	10	97.51%	60	97.79%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	1	99.95%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.82%
Unasoft UNA Pro	126	80.03%	4	55.56%	79.15%	1783	57.92%	14379	12.85%	773	64.31%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.78%	8	99.82%

SOFTWIN BitDefender Standard 7.2

ItW Overall	100.00%	**Macro**	99.69%
ItW Overall (o/a)	100.00%	**Standard**	97.79%
ItW File	100.00%	**Polymorphic**	97.51%

Having already appeared in this test as a part of both *AVK* and *eScan*, *BitDefender* now arrives for testing on its own.

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 V3VirusBlock	143	3824.7		26	3051.3		175	911.0	49	1522.6
Alwil Avast!	268	2040.8		31	2559.2		96	1660.6	36	2072.4
Authentium Command	253	2161.8		19	4175.5		85	1875.5	13	5739.0
CA eTrust Antivirus	293	1866.7		18	4407.4		107	1489.9	22	3391.2
CA Vet Anti-Virus	237	2307.7		20	3966.7		98	1626.7	27	2763.2
CAT Quickheal	149	3670.7		24	3305.6		102	1562.9	31	2406.7
DialogueScience Dr.Web	297	1841.5	[12]	31	2559.2		100	1594.2	19	3926.7
Eset NOD32	204	2681.0		21	3777.8		46	3465.6	8	9325.9
Fortinet FortiClient	258	2119.9		N/A	-		62	2571.2	20	3730.4
FRISK F-Prot Antivirus	238	2298.0		19	4175.5		106	1503.9	15	4973.8
F-Secure Anti-Virus	304	1799.1		36	2203.7		118	1351.0	30	2486.9
GDATA AntiVirusKit	824	663.8	[1]	40	1983.3		373	427.4	43	1735.1
Grisoft AVG	320	1709.2	4 [2]	24	3305.6		156	1021.9	36	2072.4
H+BEDV AntiVir	286	1912.4		19	4175.5		111	1436.2	23	3243.8
Kaspersky KAV	290	1886.0		32	2479.2		118	1351.0	27	2763.2
MicroWorld eScan	389	1406.0		38	2087.7		161	990.2	35	2131.6
NAI VirusScan	213	2567.8		26	3051.3		98	1626.7	17	4388.7
Norman Virus Control	445	1229.1		25	3173.4		216	738.0	22	3391.2
SOFTWIN BitDefender	770	710.3	[1]	21	3777.8		315	506.1	22	3391.2
Sophos Anti-Virus	182	3005.1		24	3305.6		88	1811.6	20	3730.4
Symantec SAV	299	1829.2		34	2333.3		114	1398.4	32	2331.5
Trend PC-cillin	197	2776.3		14	5666.7		71	2245.3	16	4663.0
Unasoft UNA Pro	252	2170.4	6 [8]	32	2479.2	[2]	207	770.1	39	1913.0
VirusBuster VirusBuster	313	1747.4		26	3051.3		162	984.1	29	2572.7

Despite having a scattering of misses across the test sets, none of these were in the ItW set, thus *BitDefender* earns a VB 100% award. The last year has seen small increases in detection rates overall for *SOFTWIN*, though there were only small numbers of misses to start with.

Sophos Anti-Virus 3.77

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Standard**	99.49%
ItW File	100.00%	**Polymorphic**	99.95%

Sophos continues to improve its detection rates in the polymorphic test sets, with only a single miss in that area. The remaining misses all fell into the category of samples deliberately chosen not to be detected on performance grounds, so the developers will no doubt be happy with their work on the underlying engine. With its usual lack of false positives the *Sophos* product is well deserving of a VB 100% award.

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%

Symantec's product detected all files in all test sets, leaving little room for discussion. What's more, the product managed exactly the same feat this time last year. As a result a VB 100% is awarded to *Symantec*.

Trend PC-cillin 10.04-1114

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	95.77%

With historical trends in mind, *PC-cillin* is another product whose performance has changed very little in the last year. Virtually identical results on the two occasions are slightly less impressive where misses are concerned, although the ItW and macro test sets showed perfect detection. Despite the lack of improvement during the year, *PC-cillin* is due a VB 100% award.

Unasoft UNA Pro 1.82

ItW Overall	79.15%	**Macro**	57.92%
ItW Overall (o/a)	73.30%	**Standard**	64.31%
ItW File	80.03%	**Polymorphic**	12.85%

Hailing from the Ukraine, this was another new product on offer this month – and was possibly the most disappointing product I have yet reviewed in terms of detection rate. The missed files were scattered without any distinguishable pattern throughout all the test sets, dispelling the view that perhaps detection had been concentrated in any one key area. To compound these woes, the product detected a considerable number of viruses where they did not exist.

Needless to say a VB 100% for *UNA* looks a far off prospect. However, *UNA* did excel in one area: the security measures designed to prevent unauthorised use of the program. This is a four-layer process, involving a key file, a personal serial number, an approved name and an allocated password. With this level of security it seems unlikely that any unauthorised users will be operating *UNA* – which can only be a good thing as far as protecting the world from viruses is concerned.

VirusBuster VirusBuster 4.5-12

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	91.78%

Back to more normal rates of detection, *VirusBuster* continues to whittle away at the few samples which it misses. This slow progress starts from a point at which improvement is hard, since detection rates are already very good. As a result of this detection quality *VirusBuster* is due another VB 100% award.

CONCLUSION

As can be seen from the results of this test, newcomers can have quite a harsh time as far as detection results are concerned, though old-timers do also suffer the odd indignity. Many of the reasons for this are external factors relating to the product's niche. For example, a product from the Far East will not necessarily aim to detect the same set of samples as a product from South America. Similarly, some products may focus on macro viruses or worms by dint of their perceived market. In many ways, the ItW test set is the most valid way of judging a new product, since detection rates in other test sets depend so much on the product's origin. Of course, we would expect to see improvements in detection rates in subsequent submissions, as has historically been the case, but for the products in this review only time will tell.

Technical details:

Test environment: Three 1.6 GHz Intel Pentium 4 workstations with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, all running *Windows NT 4 Workstation Service Pack 6*.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/WinNT/2004/test_sets.html.

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

ERRATA: WINDOWS NT COMPARATIVE FEBRUARY 2004

The results were reviewed for two other products in the *Windows NT* comparative (*VB* February 2004, p.12), with the following outcome:

Alwil AVAST!

After consultation with the developers a method was discovered by which the on-access function of *AVAST!* could be tested fully. The results of this re-testing were such that *Alwil*'s product gains a VB 100% award.

Feb 2004
100%
VIRUS BULLETIN
www.virusbtn.com

Sophos Anti-Virus

Sophos Anti-Virus was noted in the *Windows NT* comparative as having missed one sample in the polymorphic test set. Further investigation determined that although this file was triply infected with W32/Zmist.D, the multiple infection had rendered the sample unable to replicate. Consequently this file has been removed from the test set. Although this does not affect percentages for other products, this does mean that *Sophos Anti-Virus* achieved 100% detection in the polymorphic test set, and indeed across all test sets.