COMPARATIVE REVIEW

Windows NT

Matt Ham

The line-up of products in this comparative included a number of newly packaged products, but no true newcomers. However, this gave me no cause to imagine that the path of testing would be a smooth one – past tests on *NT* have shown a host of oddities in behaviour which act as pitfalls and banana skins for the unwary scanner. Given 21 products to review, the time for prevaricating is over – so on with the details.

Test Sets

VB2001 was deemed momentous enough that the September WildList was delayed to allow reporters to wend their way back from Prague. As a consequence, the test sets in this review are based on the somewhat antiquated August 2001 WildList. This should give the products every chance of doing well on In the Wild detections, and developers should be warned that any misses in the ItW test set will be particularly noteworthy, with a month's preparation time available to all. Making their debut in the WildList are the usual selection of macro viruses in addition to the combined VBS/EXE worm W95/Linong.A.

Most noteworthy (in terms of press interest at least) is W32/Bady.C, better known as Code Red II. This leads to the question 'what about Code Red?' The original Code Red had no file-based portion and, while the later derivatives contained some code, this can more accurately be considered Trojan. The Trojan parts have not been included in the test set, since they are no more than dropped payload files of the worm and are not part of the infective process. Technically, the fileless nature of the worm portion of these specimens is rather problematic as far as testing detection is concerned.

Two possibilities were considered: testing on a real infected machine or using files which contain an image of the infected memory. The latter was dismissed quickly since experiments with floppies and file images of disks have shown there to be major differences in behaviour between these two forms of the same data – the same could be expected of file and memory representations of data, which would render meaningless any results gained in this way. The ideal solution would be the use of infected machines, but this also was forced into the reject bin by virtue of the additional manpower and hardware required. Active Code Red detection is thus not included in this test.

Additions to the other test sets included two of particular interest, W32/Zmist.D and W32/Nimda.A. W32/Zmist.D is of note simply because it is widely considered to be a

difficult virus to detect due to its use of advanced polymorphic techniques (see *VB* March 2001, p.6). Not a threat in the wild, Zmist can be considered indicative of the complexity of detection to be expected in new generations of the virus threat. W32/Nimda.A, on the other hand, needs no introduction and will be featuring in the ItW set in the next comparative review. Here, Nimda is notable for the additional extensions it uses: .TMP, .EML, .NWS and .ASP are all potentially testing additions for those products not scanning all files.

Test Procedures

Testing procedures remain unchanged from those performed recently. Tests were performed on a *Windows NT4* server with Service Pack 6 and *Internet Explorer 5* installed. Scans of the test set were performed on a local hard drive using the default settings for the scanner as far as files to be scanned and methods of scanning were concerned.

Results for on-demand scans were, by preference, logged using the log generation facilities of the program under test, with deletion of infected files being the method used if log files proved resistant to parsing for usable results. On access testing was, by default, performed by attempting to open files and testing for blocking of this process. If not blocked by default, copying the files was attempted, checking for denial of attempts and logging the results.

Aladdin eSafe Desktop 3.0.33

ItW Overall	100.00%	Macro	99.31%
ItW Overall (o/a)	99.92%	Standard	98.17%
ItW File	100.00%	Polymorphic	92.47%

The greatest mystery concerning this product was its version number – invisible to the naked eye and only apparent while the product was being installed. Happily, viruses were much more easily detected, with lack of null extension scanning causing the only misses in the ItW test set. This lack of scanning applied only on-access and was expected by the developer as a result of a design decision.

The files are detected as viral when run but *Aladdin* is of the opinion that adding no-extension to the list of files which should be scanned is an unnecessary overhead. Unfortunately for *Aladdin* running each and every missed file to check for such behaviour is not really feasible.

Elsewhere there were problems in the clean test sets where the scan process repeatedly hung on the clean executable files set. The OLE set was scanned in a very respectable time with both compressed and raw data, but the zipped clean executables were somewhat sluggish. The problems encountered on executables are probably due to a high percentage of dynamically compressed files in the test sets. The product scans such files more slowly than might be hoped and as a result of the same underlying issues there may possibly be instability.

Alwil AVAST32 3.0

ItW Overall	100.00%	Macro	99.45%
ItW Overall (o/a)	99.07%	Standard	98.87%
ItW File	100.00%	Polymorphic	93.10%

Like the previous product, *AVAST32* showed misses due to extension issues, here only on demand, these being the .MDB files of the never-threatening ItW A97M/Accessiv.A and B viruses. However, these files were picked up as infected by the on-access scanner. Misses ItW were relegated to the single sample of W32/Badtrans.A, which was missed on access. This was something of an anomaly, since most differences between on-access and on-demand scanning were in the more recent and complex additions to the polymorphic sets.

An additional similarity was that *AVAST32* suffered from a frozen scan on the clean set – though on this occasion on the clean OLE file set. This was a disappointment as other clean set scanning times were respectable. On several occasions this timing would have been even more impressive if the internal timer was to be believed – this had a habit of claiming an elapsed time of zero seconds. A few additional niggles included the selection process for these scans which still does not offer browsing for the selection of targets.

Computer Associates eTrust Antivirus 6.0.96

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.98%
ItW File	100.00%	Polymorphic	97.50%

Although sporting an all-new box, fashionable 'e-name' and lurid splash screen graphics, *eTrust* is not perceptibly different from the *InoculateIT* it replaces. Stability and ease of use have been preserved, together with the usual high rates of detection. Misses were confined to two viruses: W32/Zmist.D was missed in all 43 samples in the polymorphic set, while a .HTM sample of W32/Nimda.A was missed in the standard set.

eTrust performed well in the clean test sets, with no false positives and reasonable speed of scanning and is thus given a VB100% award. Testing was performed using the default product engine, derived from the *iRiS* product of yesteryear, but it can also use the *Vet* engine.

CA Vet Anti-Virus 10.3.8

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.35%

Vet, like *InoculateIT*, shows signs of a slight migration in designation, with the *eTrust* logo being visible on the box (though in a very much less obtrusive manner than its sister

product). As far as speed of scanning the clean test sets is concerned, there was little to choose between the two products, with *Vet* slightly faster on the non-archived sets while losing out on the archives.

Traditionally, these two products have been distinguished in the polymorphic test sets, and this test was no different. *Vet* detected 32 of the 43 W32/Zmist.D samples in the test set and a lone sample of ACG.A was its only miss in the remaining viral samples. A good result for the team at *Vet* who, once more, help *Computer Associates* gain a pair of VB100% awards in the same comparative.

Command Antivirus 4.62.4

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.95%
ItW File	100.00%	Polymorphic	97.50%

In terms of detection, *Command Antivirus* missed two of the eight W32/Nimda.A samples (the .ASP and .TMP samples), while all of the W32/Zmist.D samples evaded detection. From the remaining test sets there were no misses.

In terms of speed, *Command* was at the faster end of the pack when scanning of clean files was performed and, with no false positives to its name, a VB100% is awarded. It should be noted that scanning of archives is off by default, which is quickly becoming an anomaly in these tests.

The fact that this product gained a VB100% award is not to say that there were no niggling problems; the floppy scanning tests proved somewhat awkward. In fact, general awkwardness in the scan process, and the alert boxes being hidden beneath other windows, almost gave rise to misses being reported where there were none.

DialogueScience DrWeb 4.26

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.78%
ItW File	100.00%	Polymorphic	97.50%

DrWeb detected 15 suspicious files in the clean executable test set but was denied the title of 'most paranoid' for this review. It also was denied the past glories of its full detection of all files in the test set, W32/Zmist.D and W32/Nimda.A being primarily but not the sole cause of this. There were also misses in the newly-added W32/Vote.B and .C samples in the standard set – though only the executable portions were missed. Other than these there were full detections of all files in the test sets and thus another VB100% award is winging its way towards St. Petersburg.

The slight problems encountered in past reviews recurred in the changing of on-access scan parameters – even changing the location of the log file required a reboot. Also there was a crash during the on-demand boot scan test – though other than this momentary instability the boot scanning process was one of the more user-friendly encountered.

Eset NOD32 1.114

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.53%

Eset have begun mentioning *VB* not only in their splash screen but also in the CD wallet information – referring to their past record of no misses, ever, in the ItW test set (failures to gain VB100% awards have been due to false positive issues). Their claim record remains unbroken, with only eight of the W32/Zmist.D samples being missed in the on-access or on-demand testing procedures.

Additionally, *NOD32* remains one of the fastest products on review, a speed which it combines with a recent record of no false positives or suspicious files. It will come as no surprise, therefore, that *NOD32* is the recipient of the fifth VB100% of this comparative.

FRISK F-Prot Antivirus 3.11

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.89%
ItW File	100.00%	Polymorphic	97.50%

F-Prot managed to throw a single exception early in the scanning process which, thankfully, was not reproduced later in the tests. There was also a degree of poor change detection apparent in the on-access floppy scanning procedure, with many disks having to be scanned four times with intervening clean disks before detection could be triggered.

After these complaints there was full detection in the on-access scanning, together with ItW and macro test sets. Considering that there were numerous new samples added to the macro set, this is somewhat more impressive for all products gaining clean sweeps in that set than might otherwise be assumed. Misses were W32/Nimda.A and all the W32/Zmist.D samples, with the addition of partial detection of W32/Vote.C and W95/SK.8044. Once more a VB100% award is gained.

F-Secure Anti-Virus 5.30

ItW Overall	99.83%	Macro	100.00%
ItW Overall (o/a)	99.73%	Standard	99.69%
ItW File	99.82%	Polymorphic	97.50%

Derived directly from the previous product, *FSAV* might be expected to have a similar detection rate – until, that is, it is

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Aladdin eSafe Desktop	0	100.00%	0	100.00%	100.00%	31	99.31%	74	92.47%	35	98.17%
Alwil AVAST32	0	100.00%	0	100.00%	100.00%	22	99.45%	71	93.10%	23	98.87%
CA eTrust	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	1	99.98%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	12	99.35%	0	100.00%
Command Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	2	99.95%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	6	99.78%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	8	99.53%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	3	99.89%
F-Secure Anti-Virus	0	100.00%	3	99.82%	99.83%	0	100.00%	43	97.50%	22	99.69%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	2	99.95%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	51	97.57%	13	99.67%
Grisoft AVG	0	100.00%	1	99.97%	99.97%	20	99.50%	167	89.91%	66	96.92%
HAURI ViRobot	0	100.00%	75	91.34%	91.82%	363	90.42%	10836	35.38%	656	65.18%
IKARUS virus utilities	0	100.00%	14	98.83%	98.90%	143	96.67%	426	90.73%	89	95.14%
Kaspersky Lab KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	2	99.95%
NAI NetShield	0	100.00%	7	99.57%	99.60%	3	99.97%	2	99.88%	19	99.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	61	95.47%	0	100.00%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	234	92.98%	20	99.36%
Symantec Norton AntiVirus	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%	3	99.94%	255	92.87%	9	99.78%
VirusBuster VirusBuster	1	91.67%	0	100.00%	99.53%	4	99.90%	71	92.97%	10	99.72%

noted that the extension list for *F-Secure*'s offering has been kept deliberately restricted. Detection of the .BAT and .LNK samples of W32/SirCam.A and the .DLL sample of W32/MTX.B ItW is thus effectively off by default.

In the standard set the BAT/911.A and B samples were missed for the same reason, along with the .TMP file associated with W32/Nimda.A. Other than purely extension-based misses, only samples of W32/Zmist.D went undetected.The reasoning behind the decision to restrict the number of extensions scanned is the customary one of reducing scanning times – which, admittedly, are already rather slower than might be considered ideal. Quite whether this is the best method of dealing with such a speed issue is, however, open to debate.

GDATA AntiVirusKit Generation 10

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	94.42%	Standard	99.95%
ItW File	100.00%	Polymorphic	97.50%

A product derived from *Kaspersky Anti-Virus*, the similarity in speed for the clean test sets tends to suggest that no huge inefficiencies have been introduced. A major difference does exist, however, that on-access boot sector scanning is absent from the *GDATA* product – or at least not triggerable by any deducible means. From the point of view of detection in files the news was better, with the predictable pair of W32/Nimda.A and all the W32/Zmist.D samples causing the only misses throughout the entire test set.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Aladdin eSafe Desktop	0	100.00%	2	99.92%	99.92%	34	99.29%	74	92.47%	38	98.07%
Alwil AVAST32	1	91.67%	1	99.51%	99.07%	0	100.00%	43	97.50%	11	99.62%
CA eTrust	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	1	99.98%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	12	99.35%	0	100.00%
Command Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	2	99.95%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	5	99.80%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	8	99.53%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	3	99.89%
F-Secure Anti-Virus	0	100.00%	4	99.72%	99.73%	0	100.00%	43	97.50%	23	99.66%
GDATA AntiVirusKit	12	0.00%	0	100.00%	94.42%	0	100.00%	43	97.50%	2	99.95%
GeCAD RAV	1	91.67%	0	100.00%	99.53%	0	100.00%	51	97.57%	13	99.67%
Grisoft AVG	12	0.00%	0	100.00%	94.42%	0	100.00%	43	97.50%	7	99.67%
HAURI ViRobot	12	0.00%	77	91.25%	86.16%	368	90.37%	10836	35.38%	659	65.11%
IKARUS virus utilities	1	91.67%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Kaspersky Lab KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	2	99.95%
NAI NetShield	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.88%	11	99.02%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	61	95.47%	10	99.65%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	234	92.98%	20	99.36%
Symantec Norton AntiVirus	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%	3	99.94%	255	92.87%	9	99.78%
VirusBuster VirusBuster	1	91.67%	0	100.00%	99.53%	4	99.90%	71	92.97%	11	99.70%

GeCAD RAV 8.2.1.12

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	99.53%	Standard	99.67%
ItW File	100.00%	Polymorphic	97.57%

The testing of *RAV* did not start well since installation did not complete due to errors with Visual C runtime libraries which are required to be particular versions. Some manual fiddling got the process back on track, but the lack of these files in the installation package is a weakness. The process of updating was also somewhat more convoluted than might be expected – doing so from a file was explained poorly in the help files. Matters improved when detection was considered, with 65 missed files out of the whole test set – once more exclusively from the standard and polymorphic sets and including four of the W32/Nimda.A and all but two of the W32/Zmist.D samples. Unfortunately for *GeCAD*, Michelangelo was missed in the on-access boot tests and a grand total of 21 false positives and one suspicious file were present in the clean test set. Although not the most paranoid of this review, this was a sufficient harvest to deny *RAV* a VB100% award.

Grisoft AVG 6.0 285

ItW Overall	99.97%	Macro	99.50%
ItW Overall (o/a)	94.42%	Standard	96.92%
ItW File	99.97%	Polymorphic	89.91%

AVG certainly wins prizes on the on-access boot mystery front – although claiming to have such a feature, this proved to be untriggered in numerous attempts. On demand this did not prove to be a problem, so the capability is in the product somewhere. It managed to produce a smattering of false positives in the clean test set which, akin to the previous product, scuppered *AVG*'s attempt at gaining a VB100% award. *AVG* was also notable in this test for missing files in all of the test sets rather than the more limited selection which characterised detection rates over all products. Particularly surprising was the repeated missing of the .HTA sample of JS/Kak.A which has been in the wild for a number of years.

HAURI ViRobot Professional 3.0

ItW Overall	91.82%	Macro	90.42%
ItW Overall (o/a)	86.16%	Standard	65.18%
ItW File	91.34%	Polymorphic	35.38%

ViRobot distinguished itself by performing very quickly on the clean executable test sets, though some might suggest that this is because it is not really looking for much. Overall detection rates were roughly 50 percent of files, with more misses ItW than can be considered by any means comfortable. On floppy scanning the detection rate was exactly half of all samples since, despite there being full detection on demand, there was no detection on access.

The interface was pleasant enough, but the much-needed improvements have not been made since the last time *ViRobot* was reviewed. The reasoning that there are differing anti-virus needs in Korea from the rest of the world may be applicable here, but will be no great comfort to a western user of this product.

IKARUS virus utilities 5.03

ItW Overall	98.90%	Macro	96.67%
ItW Overall (o/a)	N/A	Standard	95.14%
ItW File	98.83%	Polymorphic	90.73%

This rates as the most over-paranoid of the products on test, with a grand total of 29 suspicious files and five false positives in the combined clean test sets. Its powers of looking for what was not there were not only very efficient but also somewhat time-consuming, making the scan times decidedly slow. Heuristics did prove to be of use in the on-demand boot sector tests, this being the reason for AntiExe's detection, but this did not carry over to the detection of the same virus on access.

Indeed, on-access scanning was something of a nightmare, with no automatic treatment available and those which were available not seeming to perform consistently in the manner they suggested would work. Log files contained large amounts of useless information and were size-limited which, after ten hours of testing, led me to abandon on-access file scan testing for this product. The fragments of data retrieved from logs suggest slightly worse detection on access than on demand, on demand showing large numbers of misses in both standard and polymorphic test sets.

Kaspersky Labs Kaspersky Anti-Virus (AVP) 3.5

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.95%
ItW File	100.00%	Polymorphic	97.50%

Clearly, product recognition is something that the *Kaspersky* folks are concerned about, hence the inclusion of the parenthesised *AVP* in the splash screens of this product. However, naming matters proved the most complex of the issues on hand here, with all tests going smoothly and as expected.

It was mentioned earlier that *GDATA*'s *AVK* and *KAV* share the same engine. Indeed, with only one exception, the detection rates were identical. However, this exception was rather major in that *KAV* showed perfect detection for on-access boot sector viruses. This is the difference that wins a VB100% award.

NAI NetShield 4.5

ItW Overall	99.60%	Macro	99.97%
ItW Overall (o/a)	100.00%	Standard	99.00%
ItW File	99.57%	Polymorphic	99.88%

The *VB* comparative test is often a frenzy of patching of products when testing is about to begin – this time, both a Service Pack and a SuperDat file had to be added before *NetShield* was ready for operation. However, the line was drawn at the inclusion of a suggested scan-all-files patch, since this was hidden away on a section of the *NAI* Web site reserved for patches which should not be applied under normal circumstances.

The result was fairly predictable, in that *NAI* missed out on a VB100% award due to extension-related misses ItW which would have been solved by the patch. The good news is that on-access, where contents rather than extensions are considered, these files were scanned and detected correctly, and all W32/Zmist.D samples were detected. There were also a number of new misses in the standard set of ancient viruses – possibly removed from the datafiles for reasons of space saving.

Norman Virus Control 5.20

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	95.47%

Norman Virus Control is one of those products looking for a bizarre niche role – in this case to have no method of

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time(s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	Time(s)	Throughput (MB/s)
Aladdin eSafe Desktop	N/A	N/A		26.0	3051.3		484.0	329.4	38.0	1963.4
Alwil AVAST32	290.0	1886.0		N/A	N/A		140.0	1138.7	6.0	12434.6
CA eTrust	293.0	1866.7		21.0	3777.8		101.0	1578.4	22.0	3391.2
CA Vet Anti-Virus	227.0	2409.4		16.0	4958.4		113.0	1410.8	26.0	2869.5
Command Antivirus	204.0	2681.0		24.0	3305.6		97.0	1643.5	14.0	5329.1
DialogueScience DrWeb	310.0	1764.3	[15]	28.0	2833.3		133.0	1198.6	23.0	3243.8
Eset NOD32	95.0	5757.2		15.0	5288.9		21.0	7591.3	4.0	18651.9
FRISK F-Prot	239.0	2288.4		24.0	3305.6		102.0	1562.9	16.0	4663.0
F-Secure Anti-Virus	594.0	920.8		32.0	2479.2		308.0	517.6	102.0	731.4
GDATA AntiVirusKit	270.0	2025.7		39.0	2034.2		136.0	1172.2	42.0	1776.4
GeCAD RAV	612.0	893.7	21 [1]	42.0	1888.9		124.0	1285.6	52.0	1434.8
Grisoft AVG	327.0	1672.6	4 [2]	21.0	3777.8		113.0	1410.8	21.0	3552.7
HAURI ViRobot	100.0	5469.3	[1]	40.0	1983.3		82.0	1944.1	44.0	1695.6
IKARUS virus utilities	2667.0	205.1	5 [17]	51.0	1555.6	[12]	2142.0	74.4	42.0	1776.4
Kaspersky Lab KAV	281.0	1946.4		33.0	2404.1		148.0	1077.1	43.0	1735.1
NAI NetShield	201.0	2721.1		22.0	3606.1		88.0	1811.6	23.0	3243.8
Norman Virus Control	2498.0	218.9		14.0	5666.7		304.0	524.4	25.0	2984.3
Sophos Anti-Virus	132.0	4143.4		20.0	3966.7		78.0	2043.8	21.0	3552.7
Symantec Norton AntiVirus	310.0	1764.3		37.0	2144.2		157.0	1015.4	43.0	1735.1
Trend ServerProtect	211.0	2592.1		19.0	4175.5		102.0	1562.9	30.0	2486.9
VirusBuster VirusBuster	272.0	2010.8		33.0	2404.1		143.0	1114.8	32.0	2331.5

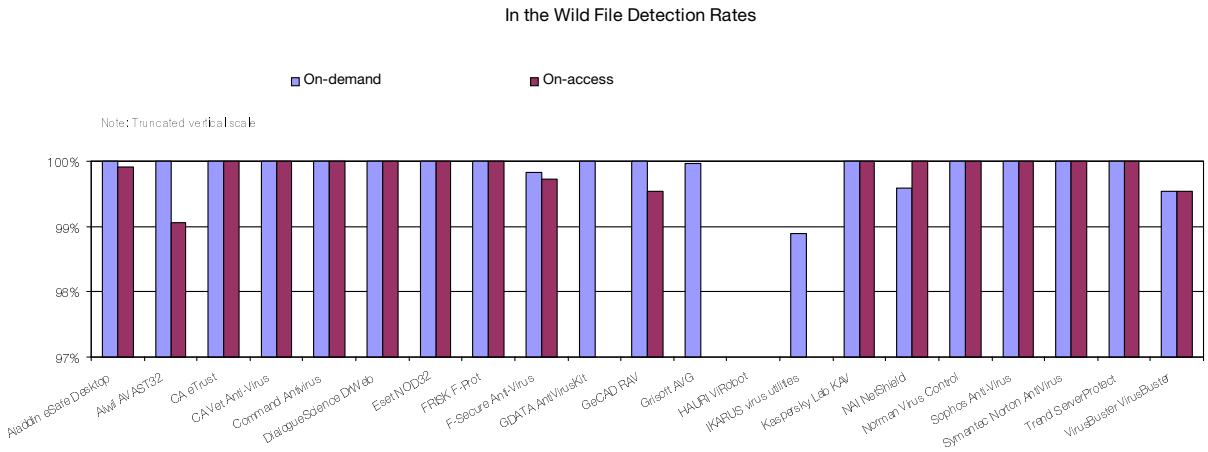
reporting without resorting to undocumented switches in the program. Once the initial disbelief at this 'feature' was over, the testing process was considerably more pleasant. Misses were W32/Nimda.A and W32/Zmist.D with a small selection of extra standard files for good measure. This, coupled with a lack of false positives on the clean test sets, sends *NVC* away with another VB100% award.

There were some problems and, as in the September 2001 *NetWare* review, these were in the length of time taken for the clean executable test set. For the *NetWare* test this has been tracked down to a design decision – gaps in scanning were introduced since server scanning could otherwise be too much of a constant load on a machine which can be expected to have many other duties. The same reason may apply here.

Sophos Anti-Virus 3.50

ItW Overall	100.00%	Macro	99.66%
ItW Overall (o/a)	100.00%	Standard	99.36%
ItW File	100.00%	Polymorphic	92.98%

Putting behind them the matter of extension-related problems, *Sophos* came forward with full detection of all files ItW and receives a VB100% award. Detection rates remained slightly lowered by the choice of extensions that are not scanned by default, and a new addition to the scanning engine is still forthcoming, leaving rather more misses in the polymorphic set than might be the case in a few months' time. The exclusion of extensions from scanning, and the fact that archive scanning is off by default, are for speed reasons, and speed of scanning was indeed good. Reports



proved to be a quirky part of the product, causing problems in parsing until it was realised that long filenames within them are always compressed to 8+3 format. This is at odds with the designated operating system and presumably is retained for backwards-compatibility with older and other-platform products.

Symantec Norton AntiVirus 7.51.847

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

Since *Symantec*'s Péter Ször is notorious for bringing with him tidings of W32/Zmist.D and its effects upon the future of scanners, it was interesting to see how his company's product bears up when faced with the virus itself. *NAV* detected all the samples of W32/Zmist.D thrown at it. In fact, all samples in all test sets were detected, which left activity in the clean test sets as the deciding factor as to whether a VB100% was awarded. Although on the slow side, the clean tests proved completely lacking in false positives, so *Symantec* add a VB100% to their collection.

Trend ServerProtect 5.21

ItW Overall	100.00%	Macro	99.94%
ItW Overall (o/a)	100.00%	Standard	99.78%
ItW File	100.00%	Polymorphic	92.87%

The installation of *ServerProtect* proved to be slightly odd since there were such lengthy delays that crashes were suspected. Once installed, the logging was slightly problematic too – of a massive log file of some 60 MB, only 1000 lines were actively viewable. These problems were overcome and the results proved no great surprise. The usual combination of standard and polymorphic misses was noted, although with more misses in the polymorphic set than many products. In addition were misses of the polymorphic macro XM/Soldier.A and X97M/Soldier.A, but no ItW misses. On-access testing showed poor change detection for boot sector viruses and it was often difficult to tell when an infection was present. Despite this, the combination of complete ItW detection and no false positives gained *Trend* a VB100% award.

VirusBuster VirusBuster 3.06

ItW Overall	99.53%	Macro	99.90%
ItW Overall (o/a)	99.53%	Standard	99.72%
ItW File	100.00%	Polymorphic	92.97%

The testing of *VirusBuster* threw up a few problems, which were almost exclusively related to how logs could be produced. The results were good however, with standard and polymorphic test sets being the source of all but one of the misses, and a solitary macro miss in addition. There were no misses in the ItW test set, and fast clean set results with no false positives left this contender in a good position to claim a VB100% award. This was not to be, however, since both on demand and on access there were misses of the ancient Stoned.NoInt.A. A disappointing result for the developers, but one which should be easy to remedy.

Conclusion

As expected, a high harvest of VB100% awards resulted from the use of a dated WildList in the testing process. The future looks set to be interesting, however, since extension issues associated with W32/Nimda.A, in the current WildList, tripped up a few here – and there are some companies with a history of problems in the extension field.

Technical Details

Test Environment: Three 750 MHz AMD Duron workstations with 128 MB RAM, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, all running *Windows NT4 Server SP6*. The workstations were rebuilt from image back-ups and the test sets restored from CD after each test.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NT/2001/08test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.