COMPARATIVE REVIEW

It's ME Again!

Matt Ham

The last *Windows ME* comparative review – in the February 2001 issue of *Virus Bulletin* – saw VB 100% awards earned by six products from a field of 17. One year on, 18 products are in the line-up. The newcomers to the roster are *Command AntiVirus*, *F-Secure Anti-Virus* and *Trend PC-cillin*, while a product from *Network Associates* is the most noteworthy of the absentees from this test. (On this occasion *NAI* failed to supply a product by the cut-off date for submissions, though we are assured that *NAI*'s offerings will continue to grace the pages of future comparative reviews.)

Windows ME is the closest any *Virus Bulletin* product review comes to the home-user market, and certainly a couple of the products submitted for testing were more consumer- than business-oriented. Possibly more surprising is the number of products which were submitted not just for the *ME* review but which have been seen in an identical form on other *Windows* platforms – '*Product-Scan for Windows 95/98/ME/NT/2K/XP*' is hardly a name that trips off the tongue, but it is not too dissimilar to some of the actual product titles.

In terms of new features, both *Kaspersky Anti-Virus* and *GeCAD*'s *RAV* presented new GUIs in these tests, with the *Kaspersky* product having a new scanning engine in addition. As for the problems that beset products in the previous *ME* review, these were twofold – problems with boot-sector detection and instability due to the production of massive log files in memory.

Test Procedures

Since there are still some questions as to exactly what earns a product a VB 100% award, there follows a short explanation. This is mostly unchanged from a year ago, with some slight modifications and clarifications.

In order to achieve a VB 100% award a product must detect in its default settings all viruses on the top half of the WildList of the month prior to its testing. 'Default settings' refers to such selectable items as sensitivity of detection, scanned extensions and the use of heuristics. Settings not related to detection may be changed to facilitate the production of realistic results. Full detection must be demonstrated in both on-access and on-demand scanning.

For on-demand testing, results are as first choice taken by parsing of log files, with the setting of 'report only' selected. Network and CD scanning has been noted to introduce sporadic errors into the test results and thus this is done on a copy of the test sets on a local hard drive.

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	99.83%	99.84%	34	99.13%	71	92.50%	31	98.73%
Alwil AVAST32	0	100.00%	2	99.87%	99.88%	21	99.53%	52	95.59%	49	97.46%
CA InoculateIT	0	100.00%	7	98.21%	98.30%	0	100.00%	1	99.94%	8	99.31%
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%	2	99.40%	99.43%	0	100.00%	43	97.50%	2	99.95%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.94%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	8	99.81%
F-Secure Anti-Virus	0	100.00%	4	99.71%	99.72%	0	100.00%	43	97.50%	23	99.66%
GDATA AntiVirusKit	0	100.00%	4	99.79%	99.80%	19	99.60%	43	97.50%	1	99.98%
GeCAD RAV	0	100.00%	1	99.91%	99.92%	0	100.00%	52	97.56%	23	99.15%
Grisoft AVG	0	100.00%	1	99.96%	99.96%	26	99.40%	181	87.85%	56	98.00%
Kaspersky Lab KAV	0	100.00%	4	99.79%	99.80%	19	99.60%	0	100.00%	1	99.98%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	29	98.65%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	60	95.48%	13	99.50%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.81%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	1	99.99%	234	93.86%	7	99.83%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	69	93.33%	8	99.81%

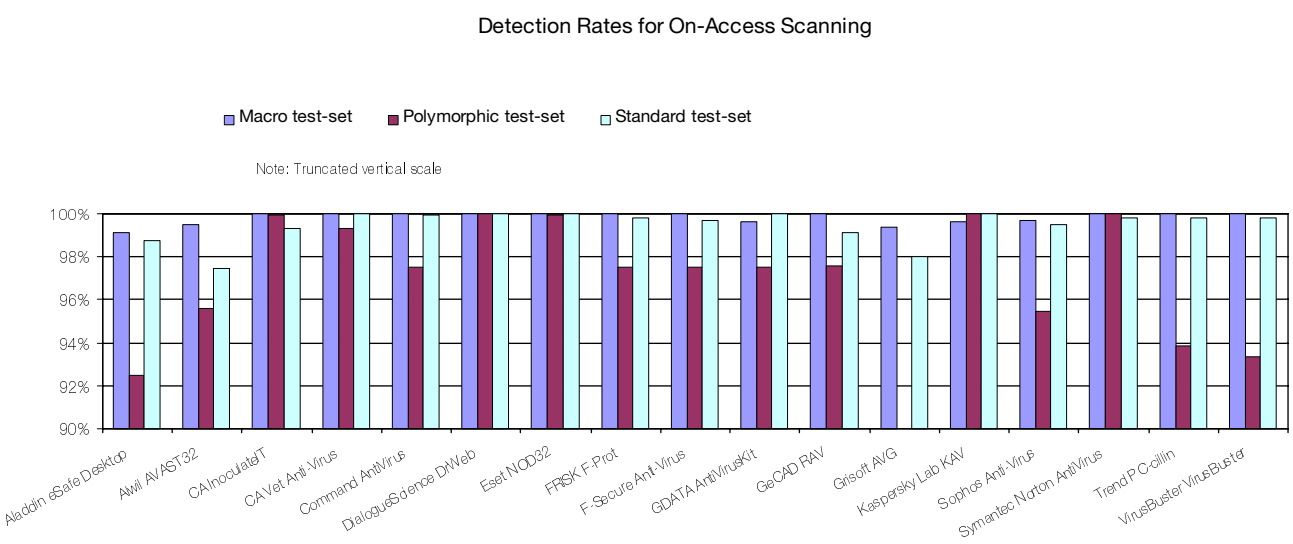
However, it has been the case in many products of late that log files are either useless for *VB* results or that the taking of log files causes the scanner to crash after a certain size is reached. In such cases the preferred method is to run a scan selecting delete as the option, followed by another choosing quarantine and another scan to check that no further files are being detected as viral. Those files remaining are regarded as misses.

For on-access testing, a selection of tools is used which seek recursively through the test sets, opening each file in turn. Scanners are set to block access on opening an infected file and a tool generates a log of those files opened.

For products which scan on file write rather than open a different method is used. Under operating systems where such a function is available natively, the test set is copied using a command which allows the blocking of individual copy operations. In this test the XCOPY command was used for this purpose. *Aladdin eSafe Desktop* uses a slightly different method of decision-making to determine when a file should be scanned. In order to simulate this activity a custom tool is used for this product.

Some products show unrepeatable misses during on-access testing which are attributable to the massive flow of infected files through the scanning engine. For these products on-access testing may be performed with deletion in the same manner as described for the on-demand tests.

For false positive detection the scanners are required to produce no false positives on the OLE and clean test sets. Many products declare files to be 'suspicious'. This is not considered to be a false positive but is registered in the table of results by the numbers enclosed in square brackets. A test of archive scanning speed is performed for purposes of testing the rate of scanning only. In this test most products scanned inside archives by default. Those products where it was necessary to activate archive scanning manually were tested with archive scanning off for the non-archived test sets. These products were *Sophos Anti-Virus, Alwil AVAST32, GeCAD RAV* and *F-Prot Antivirus*.



The Test Sets

The test sets were aligned to the December WildList, giving a sizeable gap between this update and the August WildList used in the November 2001 test of *Windows NT* products. The nature of these changes is a good reflection of the way the virus threat is progressing at the moment.

Changes to the set consisted of 39 leaving and 31 entering the list, but the proportions of virus type showed a greater difference. Leaving the test set were 28 macro viruses with a scattering of script, boot, DOS and 32-bit *Windows* viruses making up the remaining 11. Of those viruses entering the list for the first time the figures were almost reversed, with four new macro viruses and the catch-all group of 'the rest' accounting for 27 new samples. Of these, 21 were 32-bit *Windows* files which certainly seem to be the current fad among virus writers.

Looking at these figures, what might be expected as a result? With the majority of the new 32-bit viruses being more exactly defined as worms, and of these mostly non-polymorphic, it might be anticipated that these samples would be easy to detect. On the other hand, the new extensions used by some of these samples are a guaranteed way of inspiring otherwise competent scanners to miss detection.

Aladdin eSafe Desktop 3.0.33

ItW Overall	99.84%	Macro	99.16%
ItW Overall (o/a)	99.84%	Standard	98.81%
ItW File	99.83%	Polymorphic	92.47%

The behaviour of *eSafe Desktop* is, at first glance, an example of the problems associated with the new extensions used by ItW viruses. The offending samples here were W32/Nimda.A with .ASP and .HTM extensions. However, since all files in the test set were scanned on demand, this does not seem to be an extension-related pair of missed samples. Other than this, detection on demand was good, with polymorphic detection being an area in which *eSafe Desktop* is still showing improvement in detection rates.

The boot-sector testing was perfect both on demand and on access, which brings us back to the problems with boot-sector detection in the last *ME* test. On that occasion several products had major problems with this area of detection – on this occasion, all products were able to detect all samples both on access and on demand. Not only this, but the user-friendliness has also improved in many cases, resulting in a great sigh of thanks from the reviewer.

On-access tests of *eSafe Desktop* showed almost identical results to the on-demand tests and thus speed tests are the next area of interest. Here there was one oddity, standing out in the scanning of the clean test set, which showed a propensity to slow down and appeared to halt on several of the files in the test set. At first it was assumed to have crashed, but eventually the test concluded. Unfortunately this test produced three false positives – the same number as produced a year ago. The remaining speed tests showed a similarity with past results: the scanning of executable files is not very fast, but OLE files are performed at the faster edge of average for this test.

Alwil AVAST32 3.0.419.0

ItW Overall	99.86%	Macro	99.55%
ItW Overall (o/a)	99.88%	Standard	98.46%
ItW File	99.85%	Polymorphic	95.59%

AVAST32 was another product to suffer at the hands of a false positive – though in this case a single one. Scanning speeds were particularly fast on the OLE clean set, and pretty good on the executable portion of this test too.

The feeling of 'almost but not quite' continued in the detection tests. Once more W32/Nimda.A was missed in the ItW set – here it was missed in the .EML form both on

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%	2	99.83%	99.84%	37	99.16%	74	92.47%	29	98.81%
Alwil AVAST32	0	100.00%	2	99.85%	99.86%	18	99.55%	52	95.59%	29	98.46%
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.94%	0	100.00%
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%	2	99.85%	99.86%	0	100.00%	43	97.50%	2	99.95%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.94%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	43	97.50%	8	99.81%
F-Secure Anti-Virus	0	100.00%	3	99.81%	99.82%	8	99.80%	43	97.50%	22	99.69%
GDATA AntiVirusKit	0	100.00%	1	99.91%	99.92%	0	100.00%	43	97.50%	1	99.98%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	13	99.83%	21	99.20%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	23	99.42%	181	87.85%	56	98.00%
Kaspersky Lab KAV	0	100.00%	1	99.91%	99.92%	0	100.00%	43	97.50%	1	99.98%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	561	92.97%	29	98.65%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	60	95.48%	13	99.50%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.81%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	1	99.99%	234	93.86%	7	99.83%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	69	93.33%	8	99.81%

access and on demand. Other samples missed in the ItW set were a single sample each of O97M/Tristate.C on access and a sample of W32/SirCam.A on demand. The missing of W32/SirCam.A is the most concerning, since the others are likely due to extension- or format-related problems, while the missing of W32/SirCam.A is more likely to be due to a defective identity in the virus database.

Other misses were by and large confined to the polymorphics, whether in the polymorphic test set or in the macro or standard test sets. An apology must be made concerning a comment about *AVAST32* in the last *Windows NT* test – contrary to a statement in that review, the product *does* allow browsing for scan targets.

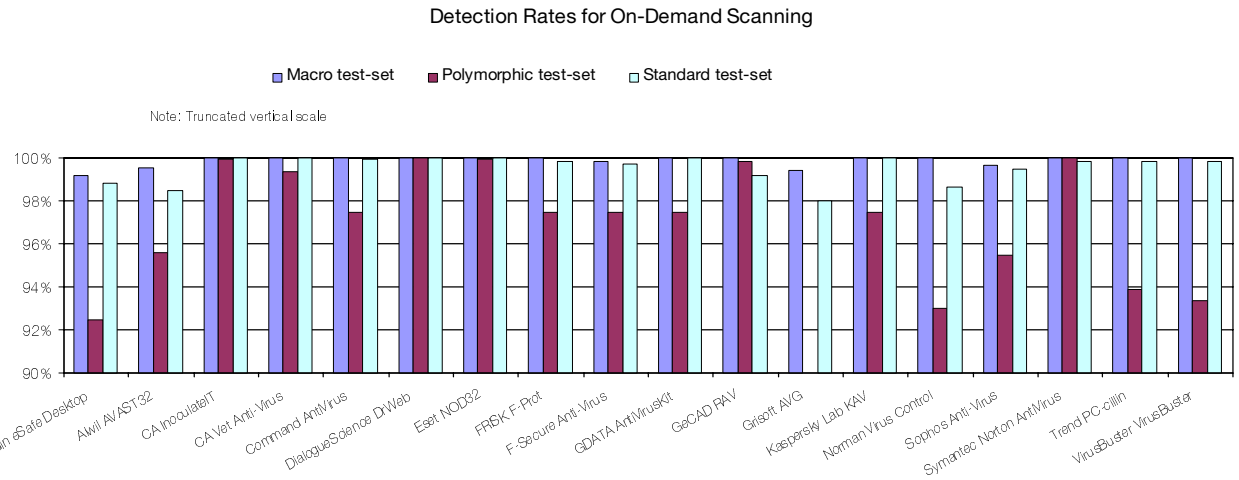
CA InoculateIT 6.0.85

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	98.30%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.94%

The greatest surprise on receiving *InoculateIT* on this occasion was that it was not accompanied by a lengthy patch list – reducing the number of downloads and installation procedures required quite considerably. Though this is good from a reviewer's point of view, this lack of patching may be an irritation to the developers.

The results of on-demand scanning were the usual excellent level demonstrated by *InoculateIT* in recent tests – just one sample of W32/Zmist.D was missed from the entire test set. The matter of on-access scanning was different, however, with a further 16 misses occurring, all of them in .HTM and .HTA extensioned samples.

Such a sudden change is almost certainly related to a configuration issue rather than an inability to detect. This notwithstanding since some of these files were within the ItW set *InoculateIT* misses out on a VB 100% award. On the other hand, false positives remained absent and speed tests showed there to be no worries for *CA* on that front either.



CA Vet Anti-Virus 10.4.4.1.1740

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

Remaining with *Computer Associates*, *CA Vet* is the next to be scrutinized. *Vet* managed once more to produce consistent results over the on-access and on-demand tests and missed only one sample of ACG.A and 11 of W32/Zmist.D. When it first appeared, W32/Zmist.A was heralded as a major challenge to detect – and changes in the variants from A to D were implemented mainly to increase this difficulty. That so many products are offering partial or full detection of this virus is a good sign.

Returning to *Vet* and with no false-positives the first VB 100% award of this comparative can be forwarded to *CA*. A single worry from a reviewer's point of view is that *Computer Associates* now seem to be marketing their products under three rather than two badges – the *CA Vet*, *InoculateIT* and *eTrust* lines of product. If this expansion continues it will not be long before a comparative review is populated by a majority of *CA* products.

Command AntiVirus 4.64.0

ItW Overall	99.86%	Macro	100.00%
ItW Overall (o/a)	99.43%	Standard	99.95%
ItW File	99.85%	Polymorphic	97.50%

After the *Computer Associates* run of products it is time to start on those powered by the *F-Prot* engine, starting with the offering from *Command*. The first area of note comes with the speed of scanning, which is certainly fast and came with no false positives to detract from the performance.

Detection was equivalent for the on-access and on-demand tests, with the majority of misses coming from the samples of W32/Zmist.D once more. However, it is the remaining misses which are more of concern. The .ASP form of W32/Nimda.A remained undetected, as did the sample of W32/Redesi.C. As these are both In the Wild for the test sets used this is sufficient to deny *Command* a VB 100% award on this occasion. As far as mitigating circumstances are concerned there is one comment to be made, in that this product was submitted considerably earlier than any others reviewed at this time.

DialogueScience DrWeb 4.27

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

To deal with the bad matters first, in its traditional manner *DrWeb* gave rise to 15 suspicious files but no false-positives. The speed at which this scanning is performed is good, however, and thus all is well (if not perfect) on this front.

Detection rates to be happy with are also becoming a tradition for *DrWeb* and this was no exception. Once more all files in both the on-access and on-demand test sets were detected correctly and this gains *DrWeb* another VB 100% award for the efforts of *DialogueScience*.

Eset NOD32 1.144

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

The testing of *NOD32* started with some odd glitches during the on-access tests – which suffered from the intermittent and non-reproducible misses on access as described in the test procedures information. Performing several scans resulted in different misses each time, usually within or just after the polymorphic test sets. The speed at which these files were processed, by far the fastest of the products

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	1305.0	419.1	3	26.0	3051.3		471.0	338.5	36.0	2072.4
Alwil AVAST32	394.0	1388.2	1	16.0	4958.4		69.0	2310.4	37.0	2016.4
CA InoculateIT	367.0	1490.3		18.0	4407.4		107.0	1489.9	21.0	3552.7
CA Vet Anti-Virus	217.0	2520.4		12.0	6611.1		108.0	5064.2	21.0	3777.8
Command AntiVirus	132.0	4143.4		11.0	7212.2		94.0	1695.9	14.0	5329.1
DialogueScience DrWeb	353.0	1549.4	[15]	13.0	6102.6		145.0	1099.4	25.0	2984.3
Eset NOD32	77.0	7103.0		15.0	5288.9		16.0	9963.5	2.0	37303.7
FRISK F-Prot	236.0	2317.5		21.0	3777.8		109.0	1462.5	14.0	5329.1
F-Secure Anti-Virus	2406.0	227.3		56.0	1416.7		1502.0	106.1	458.0	162.9
GDATA AntiVirusKit	249.0	2196.5		36.0	2203.7		135.0	1180.9	47.0	1587.4
GeCAD RAV	663.0	824.9	[1]	37.0	2144.2		278.0	573.4	18.0	4144.9
Grisoft AVG	350.0	1562.7	4 [2]	22.0	3606.1		122.0	1306.7	20.0	3730.4
Kaspersky Lab KAV	254.0	2153.3		33.0	2404.1		159.0	1002.6	47.0	1587.4
Norman Virus Control	2782.0	196.6		16.0	4958.4		294.0	542.2	20.0	3730.4
Sophos Anti-Virus	199.0	2748.4		29.0	2735.6		148.0	1077.1	21.0	3552.7
Symantec Norton AntiVirus	236.0	2317.5		31.0	2559.2		100.0	1594.2	21.0	3552.7
Trend PC-cillin	245.0	2232.4		23.0	3449.3		116.0	1374.3	32.0	2331.5
VirusBuster VirusBuster	324.0	1688.1		31.0	2559.2	[1]	199.0	801.1	31.0	2406.7

on test, seemed a possible cause for these misses (files were, presumably, not being scanned since *NOD32* had built up a large backlog of files waiting to be scanned). Sure enough, by introducing a delay between the file accesses used to trigger detection, the phenomenon was markedly reduced.

With this problem possibly explained, the matter of detection rates could be examined more thoroughly and in the end only one sample of W32/Zmist.D was missed on access and on demand.

No false positives in addition to this performance results in another VB 100% award for *Eset* –which is lucky indeed, for the company states on its CD packaging that *NOD32* has never yet missed a file In the Wild in *VB* tests.

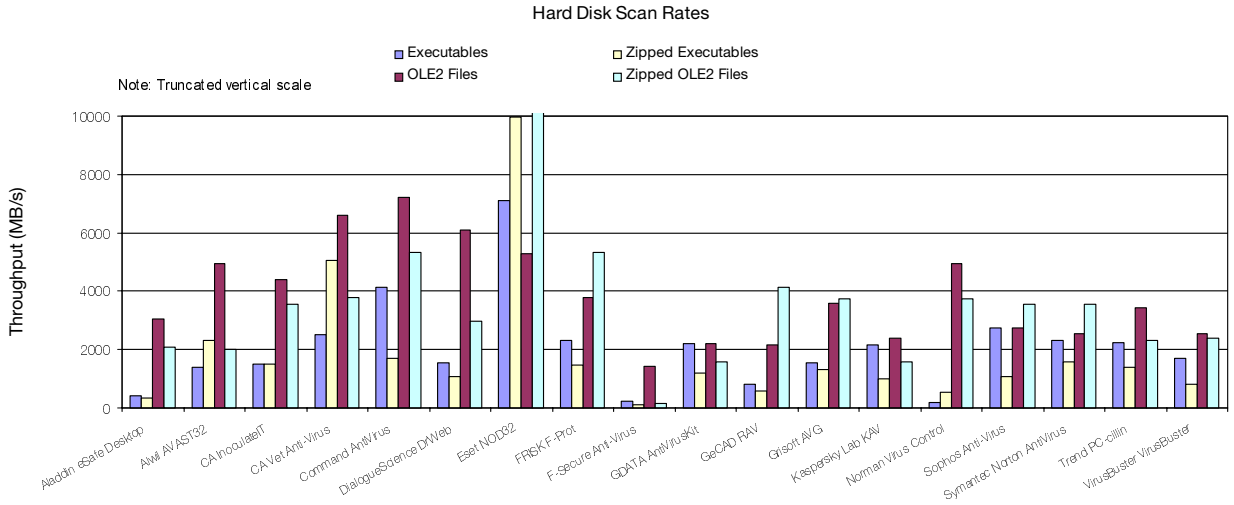
FRISK F-Prot 3.11b

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.81%
ItW File	100.00%	Polymorphic	97.50%

With the same engine as *Command AntiVirus*, but a more recent set of virus information, would the *FRISK* engine fare better in its originator's product than in a third-party product? Oddly enough, in terms of raw speed, it seems that the *Command* product has the edge, leaving detection as the other possible point of differentiation between the products.

F-Prot's detection was indeed different, though not in the way which might be expected. Sure enough, both W32/Nimda.A and W32/Redesi.C were fully detected by *F-Prot*, which is sufficient to entitle the product to a VB 100% award. More mysteriously, though, the samples of W32/Tuareg.B detected by *Command*'s product were missed by *F-Prot*.

The only explanation that springs to mind is that this is related to different time-out or heuristic settings between the two implementations, which might lead to differences when faced with complex polymorphics such as W32/Tuareg.B. Without insider knowledge however, this all remains speculation.



F-Secure Anti-Virus 5.30.7262

ItW Overall	99.82%	Macro	99.80%
ItW Overall (o/a)	99.72%	Standard	99.69%
ItW File	99.81%	Polymorphic	97.50%

With such intriguing differences between the other two *F-Prot*-based products, the third was approached with interest. Results here did little to clarify matters. First, *F-Secure*'s detection rate was lower than either of the others, due mainly to the default non-scanning of a variety of extensions both on access and on demand. The ItW samples of W32/Nimda.A and W32/Redesi.C were all detected, as were the W32/Tuareg.B samples. With such a combination of results, little in the way of a conclusion springs to mind.

Of more relevance, the selection of unscanned extensions included the .BAT and .LNK extensions used by W32/SirCam.A, and as this is in the Wild, no VB 100% award goes to *F-Secure*. Also unhappily for *F-Secure*, their product is vastly slower than the other two *F-Prot*-based products, especially on polymorphic viruses and notably so in the clean test sets.

GDATA AntiVirusKit 10.1.0.0

ItW Overall	99.92%	Macro	100.00%
ItW Overall (o/a)	99.80%	Standard	99.98%
ItW File	99.91%	Polymorphic	97.50%

AntiVirusKit (*AVK*) is another product which shares an engine, this time with the *Kaspersky* products. With a new engine installed by *Kaspersky* in their own product, it remained to be seen how *AVK* would fare. The answer was that no problems related to the engine could be noted, with both speed and detection looking good. Good, however, was not enough to gain a VB 100% award for *AVK*, since the .ASP form of W32/Nimda.A remained undetected. Other misses were entirely relegated to the samples of W32/Zmist.D.

One rather odd feature relates to the on-access scanning of boot sectors. This testing was not available in the last *ME* comparative in which *AVK* was inspected and the solution offered is somewhat imperfect aesthetically. The on-access boot-sector scanner operates by launching the on-demand scanner when boot sectors are accessed and found infected. This works, but seems rather more clumsy than the usual dedicated messaging system.

GeCAD RAV 8.5.80

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	99.92%	Standard	99.20%
ItW File	100.00%	Polymorphic	99.83%

The first of a pair of products to have benefited from a facelift, the new-look *RAV* is both aesthetically and from an ease-of-use point of view, superior to the old. The engine remains the same, but with such major interface changes obvious will there be changes in functionality? The last review saw problems which had all vanished on this occasion, so no lack of improvement can be cited on either detection or usability.

For *RAV*, only one small problem remained – the .EML form of W32/Nimda.A which was undetected on access. There were other misses in the polymorphic sets for a small number of Cryptor and all W32/Zmist.D and a number of standard files, but overall detection has significantly improved since the test this time last year. More impressive still is the change in false positives, down from two false positives and 47 suspicious files to a mere one suspicious file on this occasion. All in all a good result, with just one disheartening miss for the developers to curse.

Grisoft AVG 6.0.313.174

ItW Overall	100.00%	Macro	99.42%
ItW Overall (o/a)	99.96%	Standard	98.00%
ItW File	100.00%	Polymorphic	87.85%

From a new-looking product to one which has seen no outward change for over two years now. Even more impressive is that *AVG* can still be installed using the same CD that shipped all that time ago. The updates, of course, are more than just virus information and contain a replacement for probably most of the internal parts of the applications, yet this is still an impressive longevity for an anti-virus product CD.

To start with the bad, *AVG* managed to throw up four false positives and two suspicious files on the clean test set, thus denying the product any chance of a VB 100% award. This was done in a very respectable time, however. Detection was marred on access only for the In the Wild set – where the extensionless sample of O97M/Tristate.C was missed. This and the misses of all .MDB files in the test set are likely to be extension- rather than content-based lapses in detection. With regard to detection in the other test sets, *AVG* is somewhat weak with regards to the various polymorphic *Win32* viruses in the test set, though shows no serious weaknesses elsewhere.

Kaspersky Lab KAV 4.0.1.54

ItW Overall	99.92%	Macro	100.00%
ItW Overall (o/a)	99.80%	Standard	99.98%
ItW File	99.91%	Polymorphic	97.50%

Kaspersky Anti-Virus is the second product to have undergone a great change in appearance recently – and in this case too, the change is all for the better. It may lie purely in the realms of aesthetic subjectivism, but the product did feel nice to use. The comparative test is not about such affairs, though, so we move on to the more objective ratings.

The *Kaspersky* product performed well, though with a slightly lower rate of data throughput than the *AVK* product which also houses a *Kaspersky* engine. On matters of detection, all W32/Zmist.D samples were missed both on access and on demand, though the other missed samples were of more interest if fewer in number. On demand, the .ASP sample of W32/Nimda.A was missed as the sole remaining file. On access this was also missed but in addition the .PPT and .POT samples of O97M/Tristate.C were undetected. It is clear that this is an extension scanning decision, nevertheless these misses deny *Kaspersky Anti-Virus* a VB 100% award.

Norman Virus Control 5.2

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	98.65%
ItW File	100.00%	Polymorphic	92.97%

Norman Virus Control continues to frustrate with its lack of any log-producing facility. Quite why this should be the case is a mystery, though this is easy to circumvent by undocumented means. Also perplexing is the continued matter of the slow scan rates on the executable portion of the clean test set, a problem which does not occur if the same files are archived and then scanned. On the scanning of compressed executables and on raw and compressed OLE files the throughput is at much more respectable levels.

Despite these troubles there were no false positives – leaving the detection rates as the arbiter of the VB 100% award. Oddly enough, detection rates for some areas seem to have plummeted since the last reviews of *Norman Virus Control*, with the polymorphics Uruguay.4 and Sepultura:MtE-Small being missed where before they were detected. Thankfully for *Norman*, however, these misses were not present in the ItW test sets, where full detection merits another VB 100% award.

Sophos Anti-Virus 3.53

ItW Overall	100.00%	Macro	99.66%
ItW Overall (o/a)	100.00%	Standard	99.50%
ItW File	100.00%	Polymorphic	95.48%

On this occasion, *Sophos AntiVirus* proved quite an entertaining product to test. To deal with the dull but worthy matters first, the clean test sets were scanned and produced no false positives in the process while producing good throughput rates. On-demand testing was also much as expected. *SAV* missed those files it usually misses (files where detection is only supported under a full mode of scanning), but did detect some files which it was hitherto incapable of.

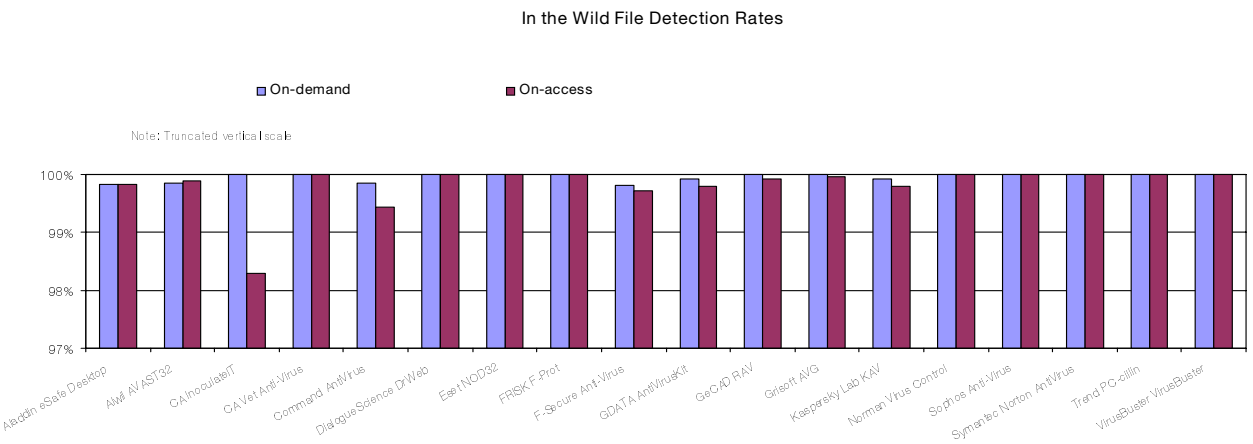
Momentary problems lay in the on-access test, where the samples of W32/Maldal.C and the .HTM sample of W32/Haptime.D were undetected in addition to those files undetected on demand, but further testing showed this problem to be non-reproducible. Due to the transient nature of the problem it was not enough to deny *SAV* a VB 100% award on this occasion.

Symantec Norton AntiVirus 2002 8.00.58

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.81%
ItW File	100.00%	Polymorphic	100.00%

Norton AntiVirus 2002 is the *Norton* home-user offering, and thus was a novel experience in terms of testing when compared with the usual corporate fare. Unfortunately, the freshness of the experience was marred by a lack of features which are expected in the corporate environment.

Lack of logging required that on-demand testing was performed by the deletion of infected files, while the testing of the on-access scanner required some undocumented



tweaks. However, detection was such that *NAV* is eligible for a VB 100% award.

To its credit it should be stated that *NAV* detected all of the files in the test set but Goldbug, had no false positives and was quite speedy on the clean set tests. It was also very easy to use – though this was at the expense of flexibility and configuration.

Trend PC-cillin 2000 7.61.0.1437.195

ItW Overall	100.00%	Macro	99.99%
ItW Overall (o/a)	100.00%	Standard	99.83%
ItW File	100.00%	Polymorphic	93.86%

As a potential home-user product, *PC-cillin* represents the other side of the coin – having most of the features seen in its server-based counterparts, but being more daunting to behold than some home users might be able to accept.

Starting with the clean set tests, these were all completed without false positives and in a speed slightly better than the average. (It is notable that, with a few exceptions which stand out suitably, the scanning speeds seen in the comparatives are becoming more and more clustered about a central point, thus the preponderance of 'about average' comments made when referring to scanning speeds.)

Moving on to detection rates, *PC-cillin* performed much as it has done recently on other platforms. The misses consisted of a single *Excel* polymorphic sample, with the remainder being spread amongst the executable polymorphics.

The polymorphics are thus an area where *Trend*'s scanner does have room for improvement. Those polymorphics which are In the Wild, however, were perfectly detected, suggesting that this is an area where research is applied to threats rather than in a blanket manner. This detection is also quite sufficient for *PC-cillin* to gain a VB 100% award.

VirusBuster VirusBuster 3.08

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.81%
ItW File	100.00%	Polymorphic	93.33%

Last in the line-up comes *VirusBuster*. One point that springs to mind to rant about is the small default size of the log which, at 50 KB, is barely enough for the general information passed to it. However, the performance of *VirusBuster* was good.

Clean set scanning rates were in that popular 'average' position, with only one suspicious file found. This did have some claim to originality since it was in the OLE set, while almost all other false-positives occur in the executable portion of the test sets. Not so uncommon are those viruses where *VirusBuster* missed detection. W32/Zmist.D, ACG.B, W95/SK8044 and W95/SK7972 have all been missed by a number of products. Despite these polymorphic misses however, there were no misses in the macro and ItW test sets and thus *VirusBuster* brings the review to a close with a VB 100% award.

Conclusion

In conclusion this review was almost too simple – nearly all problems encountered were overcome easily and the products themselves were universally friendly. I hope the same is true for *VB*'s first *Linux* Comparative, which is due in two months.

Technical Details

Test environment: Two 750 MHz AMD Duron workstations with 64 MB RAM, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, all running *Windows ME*. The workstations and test sets were rebuilt from image back-ups after each test.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/WinME/2001/12test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.