# COMPARATIVE REVIEW

## In it to Win 98 it!

*Matt Ham*

This month's review is something of an oddity in recent years, being the first where two reviewers have worked together on a Comparative since the FitzGeraldian era. It is also the first time that this writer has reported upon a Comparative Review since those long gone days, and thus the slow trickle of changes observed by the outgoing writer have become a great avalanche for the returning one. Whether these changes are for better or for worse, or in some cases have occurred at all, varies with the product, and of course there are some new faces available for the delight and delectation of our avid readers.

The number of products submitted for review has increased since the last *Windows 98* Comparative (see *VB*, November 1999, p.16) – sixteen were submitted then, eighteen now, two extra sheep having wandered hopefully into the *VB* fold. Delayed by the lack of a March 2000 WildList, and the subsequent late announcement of the April list, this Comparative sees the resumption of scheduled *VB* testing. So, are there any wolves in sheep's clothing, or is it all mutton dressed as lamb this month?

### Test Procedures

The customary *VB* test-sets were used for testing, the ItW set aligned to the April 2000 WildList, which was announced on 25 April. Accordingly, products were submitted by a 26 April deadline. A variety of viruses were added to the test-sets, the most notable new entries being a selection of JS/Kak variants, the .A and .B variants of BAT/911, and samples infected with the polymorphic W97M/Service.A. Relevant to the ItW and Standard sets, was the (somewhat unexpected) addition of JS/Unicle, which proved to be something of a nemesis to all but the luckiest.

As ever, performance tests included the measuring of on-demand scan rates and on-access scanning overheads. The means by which such properties have been assessed have been described in previous Comparatives.

### Alwil AVAST32 v3.0.247 (25/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 97.1% |
| ItW Overall (o/d) | 99.7% | Standard | 97.8% |
| ItW Overall (o/a) | 98.9% | Polymorphic | 90.1% |

Starting with no surprises, *AVAST32* still required an altered version of the on-access test procedure – with deletes being applied to created/modified files for a copy run of the test-set. The product was noticeably sluggish but this was forgiveable when combined with good detection rates.

The bulkiest misses for *Alwil* occurred with the polymorphic macro viruses – W97M/Service.A and the .E and .F variants of W97M/AntiSocial accounting for over half of all the product's misses on-demand. There also seems to be something of a blindspot at the other end of the complexity scale with 32 misses on members of the W97M/Minimal family newly introduced to the Macro set.

Other than macro woes, the newcomers of JS/Unicle.A and BAT/911.A and .B were also undetected. Concerning both BAT/911 and JS/Unicle a brief discussion can be found in the conclusion, since both bring up interesting points. Missing JS/Unicle cost *AVAST32* a VB 100% award from an on-demand viewpoint, though a smattering of wild non-macros missed on-access provided something of a contrast. *Alwil* is seemingly concentrating its efforts in macro viruses into those which are in the wild, while their non-macro problems are mainly due to differences between the on-access and on-demand components of the product.

### CA InoculateIT v4.53.524 (25/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 100.0% |
| ItW Overall (o/d) | 99.7% | Standard | 99.9% |
| ItW Overall (o/a) | 99.7% | Polymorphic | 97.8% |

*InoculateIT* showed a defiance of the usual status quo in this latest test by being relatively superior on-access. The results were, however, none too shoddy in either department. JS/Unicle was again a sticking point in both varieties of test, along with macro list entry W97M/Story.F.

Another WildList miss at first appeared for the *PowerPoint* incarnations of O97M/Tristate.C, this being one of those spotted on-demand but not on-access. The simplest explanation of this, that the on-access product is not checking all extensions scanned by the on-demand component, is clearly incorrect since similarly infected *PowerPoint* samples were detected successfully in the Macro test-set. Odd indeed, but not unexpected since the *InoculateIT* on-access scanner is, as traditionally has been the case, particularly unstable and, as here, not always totally effective.

### CA Vet Anti-Virus v10.1.8.6 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 99.6% |
| ItW Overall (o/d) | 99.7% | Standard | 99.2% |
| ItW Overall (o/a) | 99.7% | Polymorphic | 92.3% |

From vague memories of the past *InoculateIT* was generally a less likeable creature than *Vet Anti-Virus*. This led to some commentators being rather scathing about *CA's* choice of the *Vet* line to be the basis of their free offering to the world. On the basis of the detection rates shown in this

| On-demand tests | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | % | Missed | % | Missed | % | Missed | % |
| Alwil AVAST32 | 0 | 100.0% | 1 | 99.7% | 99.7% | 104 | 97.1% | 178 | 90.1% | 32 | 97.8% |
| CA InoculateIT | 0 | 100.0% | 1 | 99.7% | 99.7% | 0 | 100.0% | 17 | 97.8% | 1 | 99.9% |
| CA Vet Anti-Virus | 0 | 100.0% | 1 | 99.7% | 99.7% | 18 | 99.6% | 340 | 92.3% | 8 | 99.2% |
| Command AntiVirus | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | 1 | 99.9% | 9 | 99.1% |
| DialogueScience DrWeb | 0 | 100.0% | 2 | 99.4% | 99.4% | 8 | 99.7% | 100 | 97.3% | 9 | 99.2% |
| Eset NOD32 | 0 | 100.0% | 0 | 100.0% | 100.0% | 8 | 99.7% | 100 | 97.3% | 7 | 99.1% |
| F-Secure Anti-Virus | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | n/t | n/t | 21 | 99.7% |
| FRISK F-PROT | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | 1 | 99.9% | 9 | 99.1% |
| GeCAD RAV | 0 | 100.0% | 1 | 99.7% | 99.7% | 40 | 98.9% | 17 | 97.8% | 21 | 98.1% |
| Grisoft AVG | 0 | 100.0% | 5 | 98.8% | 98.9% | 20 | 99.4% | 124 | 92.0% | 34 | 98.2% |
| Kaspersky Lab AVP | 0 | 100.0% | 1 | 99.7% | 99.7% | 8 | 99.7% | 0 | 100.0% | 5 | 99.8% |
| NAI VirusScan | 0 | 100.0% | 1 | 99.9% | 99.9% | 7 | 99.8% | 6 | 99.2% | 4 | 99.9% |
| Norman Virus Control | 0 | 100.0% | 1 | 99.7% | 99.7% | 4 | 99.8% | 286 | 91.2% | 1 | 99.9% |
| Panda AntiVirus | 0 | 100.0% | 24 | 97.1% | 97.2% | 44 | 98.9% | 1336 | 86.0% | 59 | 97.1% |
| Softwin AVX | 1 | 96.5% | 23 | 98.2% | 98.1% | 8 | 99.7% | 376 | 90.5% | 101 | 95.1% |
| Sophos Anti-Virus | 0 | 100.0% | 1 | 99.7% | 99.7% | 21 | 99.4% | 191 | 95.2% | 45 | 98.2% |
| Symantec Norton AntiVirus | 0 | 100.0% | 0 | 100.0% | 100.0% | 21 | 99.4% | 264 | 94.7% | 17 | 99.2% |
| VirusBuster | 1 | 96.5% | 122 | 85.9% | 86.3% | 264 | 93.9% | 2042 | 79.3% | 166 | 91.6% |

review, however, *CA* at first glance seemed to have made the correct choice as far as detection rates are concerned.

Admittedly, for in-the-wild scanning the usual suspect of JS/Unicle was the preventor of a VB 100% award for *Vet Anti-Virus*, and this was consistent, as in fact were all results, between the on-access and on-demand tests. Of the rest of the files, however, *Vet* missed a larger total number, which makes *InoculateIT* clearly better. Or not, since *Vet's* misses are almost all due to two polymorphic viruses, so actual viruses detected are comparable despite samples detected being fewer. This definitely shows the perils of using straight numbers as a guide to performance, and leaves the 'which is better' debate beween these two products as up in the air as ever. It also leaves a sense of relief that *VB* is not constrained to put a ranking on every product as is so common in general industry magazines.

One area where *Vet* has slipped is, however, scan rates. Once the speed merchant to beat in the throughput tests, *Vet Anti-Virus* now sits in the middle of the pack.

## Command AntiVirus v4.58.3 (23/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 100.0% |
| ItW Overall (o/d) | 100.0% | Standard | 99.1% |
| ItW Overall (o/a) | 100.0% | Polymorphic | 99.9% |

With a new nifty trick supplied to *Virus Bulletin* for disabling on-access messaging (via the Registry), the ease of testing of *Command's* offering was markedly up from past tribulations. Detection-wise too, all was sweetness and light, with *Command* being able to claim the first VB 100% award of this month's products. Of the small number of samples missed BAT/911 was one – though only in its .PIF portions. The slight vagaries of on-access versus on-demand were again apparent, with VBS/First.C showing as infected on-demand and not on-access.

As always with those products where detection is high and problems few, there is little to write but the pleasant and so we move quickly on in hope of features to criticise.

| On-access tests | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | % | Number | % | Number | % | Number | % |
| Alwil AVAST32 | 0 | 100.0% | 4 | 98.9% | 98.9% | 104 | 97.1% | 178 | 90.1% | 55 | 96.4% |
| CA InoculateIT | 0 | 100.0% | 1 | 99.7% | 99.7% | 0 | 100.0% | 0 | 100.0% | 1 | 99.9% |
| CA Vet Anti-Virus | 0 | 100.0% | 1 | 99.7% | 99.7% | 18 | 99.6% | 340 | 92.3% | 8 | 99.2% |
| Command AntiVirus | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | 1 | 99.9% | 10 | 99.0% |
| DialogueScience DrWeb | 0 | 100.0% | 2 | 99.4% | 99.4% | 8 | 99.7% | 100 | 97.3% | 11 | 99.1% |
| Eset NOD32 | 0 | 100.0% | 0 | 100.0% | 100.0% | 8 | 99.7% | 100 | 97.3% | 7 | 99.1% |
| F-Secure Anti-Virus | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | n/t | n/t | 21 | 99.7% |
| FRISK F-PROT | 1 | 96.5% | 0 | 100.0% | 99.8% | 0 | 100.0% | 1 | 99.9% | 31 | 97.8% |
| GeCAD RAV | n/t | n/t | 1 | 99.7% | n/a | 37 | 98.9% | 18 | 97.8% | 21 | 98.1% |
| Grisoft AVG | 1 | 96.5% | 6 | 98.7% | 98.6% | 23 | 99.3% | 292 | 89.4% | 51 | 96.6% |
| Kaspersky Lab AVP | 0 | 100.0% | 1 | 99.7% | 99.7% | 8 | 99.7% | 0 | 100.0% | 5 | 99.8% |
| NAI VirusScan | 0 | 100.0% | 1 | 99.9% | 99.9% | 7 | 99.8% | 698 | 95.6% | 6 | 99.7% |
| Norman Virus Control | 0 | 100.0% | 1 | 99.7% | 99.7% | 8 | 99.7% | 292 | 90.9% | 1 | 99.9% |
| Panda AntiVirus | 0 | 100.0% | 28 | 96.5% | 96.7% | 84 | 97.8% | 1336 | 86.0% | 87 | 95.9% |
| Softwin AVX | n/t | n/t | 23 | 98.2% | n/a | 8 | 99.7% | 374 | 90.6% | 101 | 95.1% |
| Sophos Anti-Virus | 0 | 100.0% | 1 | 99.7% | 99.7% | 25 | 99.2% | 191 | 95.2% | 45 | 98.2% |
| Symantec Norton AntiVirus | 0 | 100.0% | 0 | 100.0% | 100.0% | 21 | 99.4% | 264 | 94.7% | 17 | 99.2% |
| VirusBuster | 3 | 89.6% | 125 | 85.6% | 85.7% | 267 | 93.9% | 2042 | 79.3% | 167 | 91.4% |

## DialogueScience DrWeb v4.17 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.4% | Macro | 99.7% |
| ItW Overall (o/d) | 99.4% | Standard | 99.2% |
| ItW Overall (o/a) | 99.4% | Polymorphic | 97.3% |

Thankfully, *DrWeb* does not disappoint on the niggles front, though not through a lack of detection capability. As might be expected from previous entries JS/Unicle.A was not detected, which  was enough to deny *DialogueScience* a VB 100% award this month. Elsewhere, misses included BAT/911 in its .PIF forms and W97M/Service.A. As far as differences between on-access and on-demand were concerned, a couple of extra file viruses slipped through on-access, with no readily discernable rhyme or reason.

Where *DialogueScience* can be heartily upbraided, however, is the matter of its glorious retro interface, which although no doubt fashionable in nightclubs is most unpopular with this reviewer. The on-access boot scans in particular were hampered by lack of configurability and a distinctly 16-bit ambience. This is likely the case behind the scenes too, as *DrWeb* is resource-hungry when performing on-access scans and dawdles in the scanning race.

## Eset NOD32 v1.35 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.7% |
| ItW Overall (o/d) | 100.0% | Standard | 99.1% |
| ItW Overall (o/a) | 100.0% | Polymorphic | 97.3% |

After that slight diversion into the land of the unusual back into the predictable, and another VB 100% award for *Eset*. *NOD32* does, to its credit, remain one of the more interestingly styled products on offer, as well one of the least amenable for witty comments at its expense. It has an excellent rate of scanning combined with accuracy, an enviable position to be in. W97M/Service.A proved a sticking point for detection, as did a smattering of assorted JS/Kak worm variants though none of those encountered in the WildList as used.

This leaves space to comment that one of the related files to JS/Unicle did slip through *Eset's* scanning, probably for the very good reason that *Eset* had not received it. Part of JS/Unicle's payload involved downloading this missed file from an ftp site (now closed). *VB* did not include this EXE as part of the WildList set since such downloads are open to change at the whim of the site owner.

Quite what anti-virus companies should do about such malware, where, in a twist of the usual Trojan behaviour, the name cannot change but the contents can, is left for the moment as an exercise for the enthusiastic reader.

## F-Secure Anti-Virus v5.10.6152 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 100.0% |
| ItW Overall (o/d) | 100.0% | Standard | 99.7% |
| ItW Overall (o/a) | 100.0% | Polymorphic | n/t |

Slightly more serious complaints may be levelled at *F-Secure Anti-Virus* (*FSAV*), though once more this is not primarily through a lack of detection ability. Detection was sufficient to find all in the wild specimens, with only a bunch of the usual suspects remaining undetected in the Standard test set. There may well have been some misses in the Polymorphic set too, but an executive decision was made not to bother doing these tests.

Before cries of anguish, wailing, gnashing of teeth and stern emails erupt, this was not simply a case of the tester deciding to skip a few days of work. In the long established tradition of log files proving to be the curse of Comparative testing, *FSAV* have added yet another unpleasantness, by providing log files in HTML format. These are vast, epic and sprawling affairs, sufficient to slow first to a crawl and next crash the test machines when scanning any decent sized collection, thus the Polymorphic sets were not testable in any convenient way.

Admittedly, the Polymorphic test-sets are a somewhat harsh test for any application where the log is constantly open, but whole new vistas of possible problems are unveiled with an HTML log. In the past, unique formats and .TXT files have been the norm, the files thus being uninfectable by any virus. Now the *F-Secure* team have introduced an infectable log. Infect this with script virus and lo and behold you could have infected log files. Does *FSAV* scan its own log files? Well, whether or not it does, the situation could be distinctly messy.

*FSAV* missed a VB 100% award due to a false positive, an act which might well be considered divine justice in response to the HTML logs.

## FRISK F-PROT v3.07b (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 100.0% |
| ItW Overall (o/d) | 100.0% | Standard | 99.1% |
| ItW Overall (o/a) | 99.8% | Polymorphic | 99.9% |

Back into the rant-free world and to earlier halcyon days. Unfortunately for *FRISK*, though, these days are so far in the past that they include the odd spectacle of missed in-the-wild boot viruses, in this case the decrepit Michelangelo (see *VB*, November 1999, p.20). Other misses were no surprise, though the ability to scan (on-access) the test-sets turned out to be another challenge by the software rather than the samples.

In parallel with the ability to miss boot viruses this product has also harked back to the days before networks and the real-time component had major problems with this new fangled connectivity. These problems resulted in blue-screen crashes until the scanning was performed locally, a 'feature' to bring pleasure to only the most masochistic. The version-specific bug (associated with mapped drives) proved an exception to the rule for the traditionally reliable Icelandic product.

## GeCAD RAV v7.6.360 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 98.9% |
| ItW Overall (o/d) | 99.7% | Standard | 98.1% |
| ItW Overall (o/a) | n/a | Polymorphic | 97.8% |

*GeCAD* continues in its attempts to gain the *VB* whimsy crown (*Eset* and *Alwil's* selection of beetles and geigeresque illustrations being the main competition) with a move away from their traditional shock tactics. The original operating theatre graphics have been replaced by those of a more relaxing domestic pet, though the setup has been altered in a most original way.

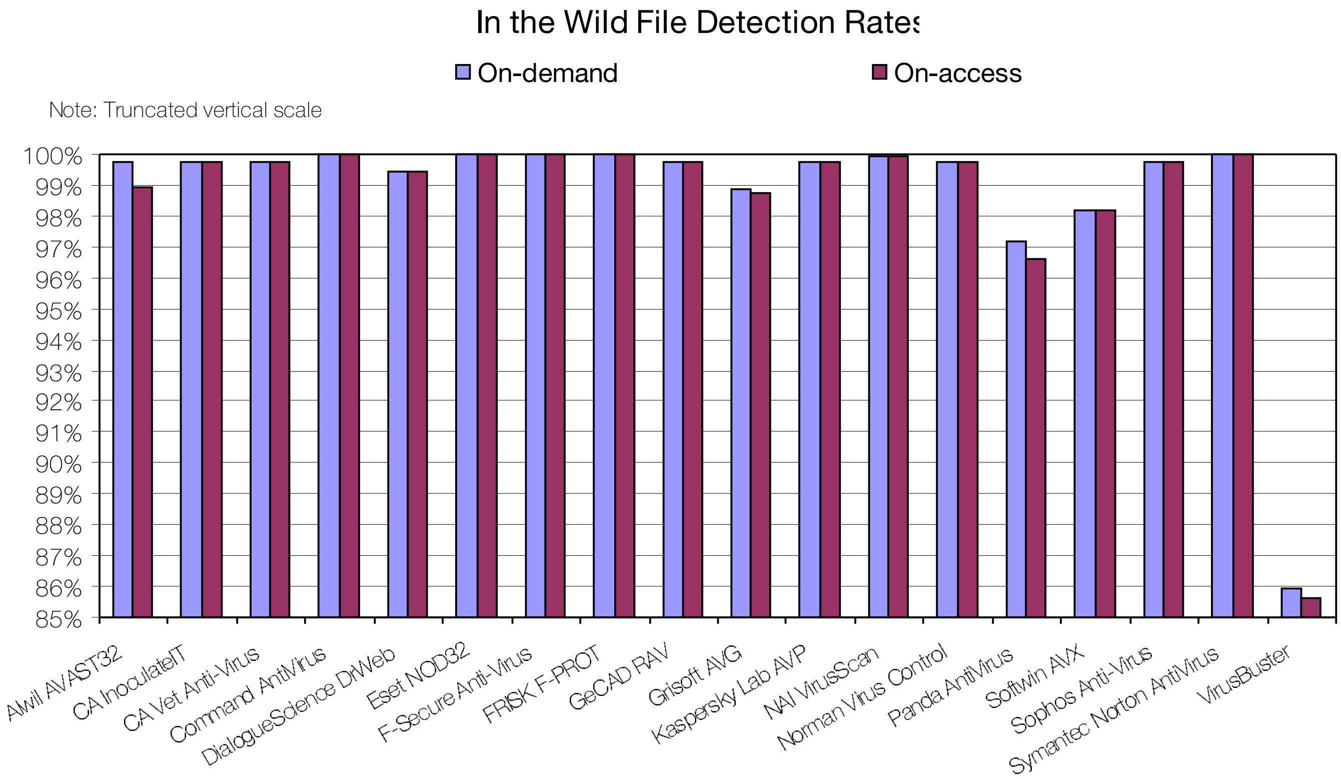
Upon first loading *RAV*, options are given for customisation. Colour scheme is selected first, then the rather more *outré* 'voice'. This gives a choice between graceful or macho, which brought visions of the computer declaring loudly 'I spit on your feeble infection attempt!'

As far as performance is concerned *RAV* missed the VB 100% award on the basis of the no doubt guessable JS/Unicle, though there were some scares since the 'files scanned' counter bore no resemblance to the number in fact processed. File scanning was otherwise not fraught with any great perils, boot sectors were another matter.

Rather than performing the trick of blue screens and floppy problems, *RAV* opts for a more refined approach to these glitches, namely by combining the two in one neat package. On-access boot scanning has never been a strong point of *RAV*, at least from the ease-of-use perspective, though until now it could at least be performed without blue screens – another victory for retro problems.

## Grisoft AVG v6.0.116 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 98.8% | Macro | 99.4% |
| ItW Overall (o/d) | 98.9% | Standard | 98.2% |
| ItW Overall (o/a) | 98.6% | Polymorphic | 92.0% |



Having taken over the mantle of mighty speed king, at least in the area of OLE files, *AVG* has changed much since its first arrival on the scene. ItW misses yet again included JS/Unicle, with Win32/Kriz providing the rest of on-demand misses. The less commonly encountered .OCX extension sample of Win32/Funlove added to the undetectables on-access. On-access boot scanning was once again a problem, though at least completed with no crashes. Michelangelo was again the culprit, which would no doubt leave its author amused if he were aware of this and if indeed he has not died due to advanced age.

The speediness of a product is often directly related to false positives and lack of detection, so these are areas of interest with *AVG*. Sure enough, both the main Clean set and the zipped executable set showed false positives. Detection, on the other hand, was not particularly bad, though undetected samples were something more of a mixed bag than with other products – only a distinct weakness with dedicated Win32 viruses being particularly notable.

## Kaspersky Lab AVP v3.0.132 (23/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 99.7% |
| ItW Overall (o/d) | 99.7% | Standard | 99.8% |
| ItW Overall (o/a) | 99.7% | Polymorphic | 100.0% |

The inevitable JS/Unicle miss again prevented a VB 100% award for *AVP*, which does not exactly make for fascinating reading. Other misses were also nothing to write home about – the .PIF parts of BAT/911 and a triad of sundry macro viruses. Most notable for *VB* testers, though possibly less so for the rest of the known world, there is now an option to disable on-screen alerts during on-access scanning, which improved reviewers' quality of life greatly.

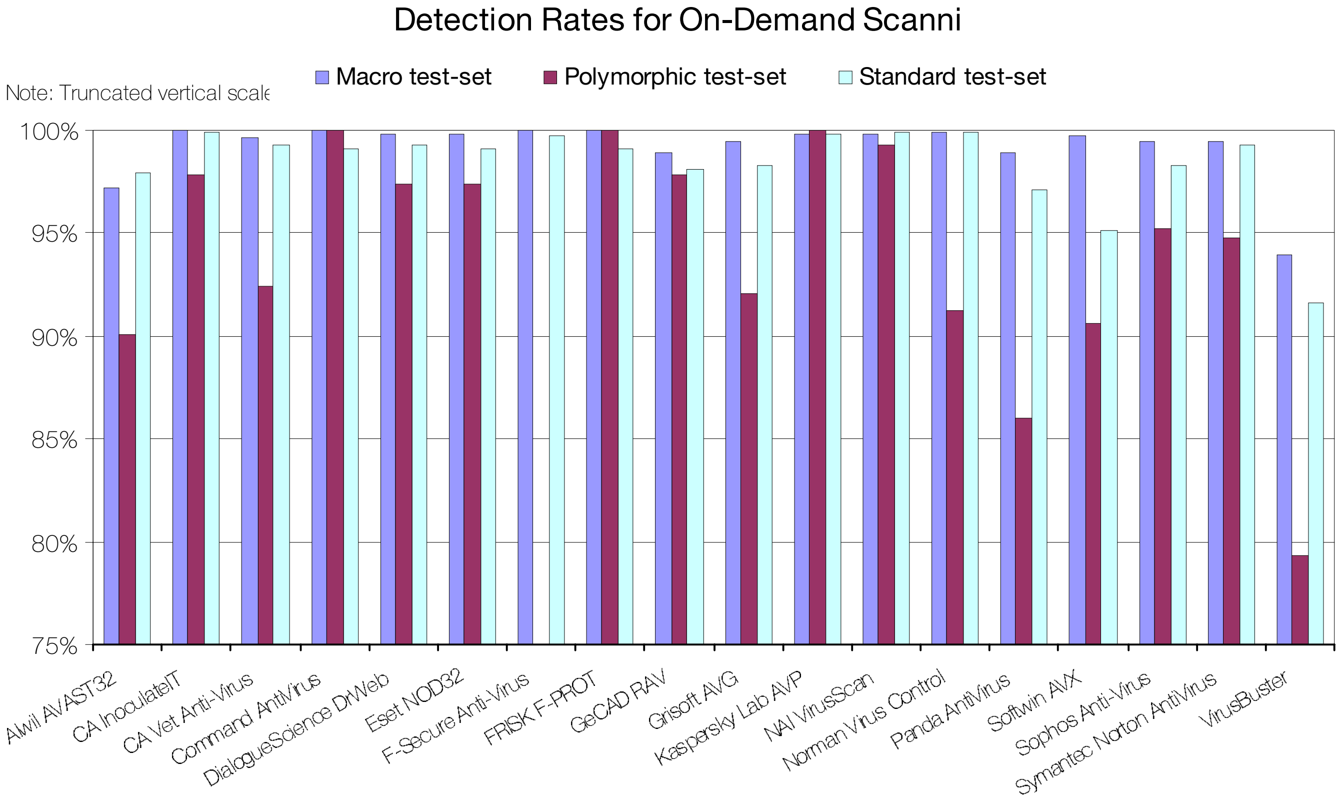
*AVP* now rests towards the slower end of the pack, but other than this there is little of evil repute to malign it with, and so on to the next victim.

## NAI VirusScan v4.5.0.4075 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.9% | Macro | 99.8% |
| ItW Overall (o/d) | 99.9% | Standard | 99.9% |
| ItW Overall (o/a) | 99.9% | Polymorphic | 99.2% |

Where you may be forgiven for guessing that only JS/Unicle prevented a VB 100% award, for once this would be erroneous. An extensionless O97M/Tristate.C sample was the bugbear for *VirusScan* on this occasion, a welcome breath of novelty in the testing procedure. Also of note was the wide disparity in polymorphic detection when operating on-demand and on-access. Russel.3072.A and SatanBug.5000.A proved easily, if slowly, detected by the on-demand scans, though patchily detected on-access. With such antiques, this is something of a surprise.

A new installation routine, in 50s style and demonstrating the less than purely corporate leanings of the *NAI Windows* product, led on to a not particularly revolutionary front end. Thus, no great new problems were to be expected and none were encountered.



## Norman Virus Control v4.80 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 99.8% |
| ItW Overall (o/d) | 99.7% | Standard | 99.9% |
| ItW Overall (o/a) | 99.7% | Polymorphic | 91.2% |

It has always been tricky to find exciting faults with *Norman's* scanners, and with JS/Unicle around to provide a topical reason this situation seems destined to continue. On this occasion, however, a small amount of excitement can be added in the form of two false positives in the Clean set. Not being a particularly fast or slow product there is, however, no great deal of discussion possible on the subject of this small failing.

As far as misses in the other test sets go ACG.A and .B plus Win95/Sk.8044 made up the majority, mostly by dint of being polymorphics and thus being scanned in large numbers. As far as other executables went, however, initial tests revealed a single executable infected with Vcomm.637 to be the only undetected non-polymorphic. Due to the suspicious nature of this observation, a subsequent retest was performed, which revealed the observation to indeed be bogus. Quite why this sample was missed initially remains a Comparative mystery.

## Panda AntiVirus v6.17.20 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 97.1% | Macro | 98.9% |
| ItW Overall (o/d) | 97.2% | Standard | 97.1% |
| ItW Overall (o/a) | 96.7% | Polymorphic | 86.0% |

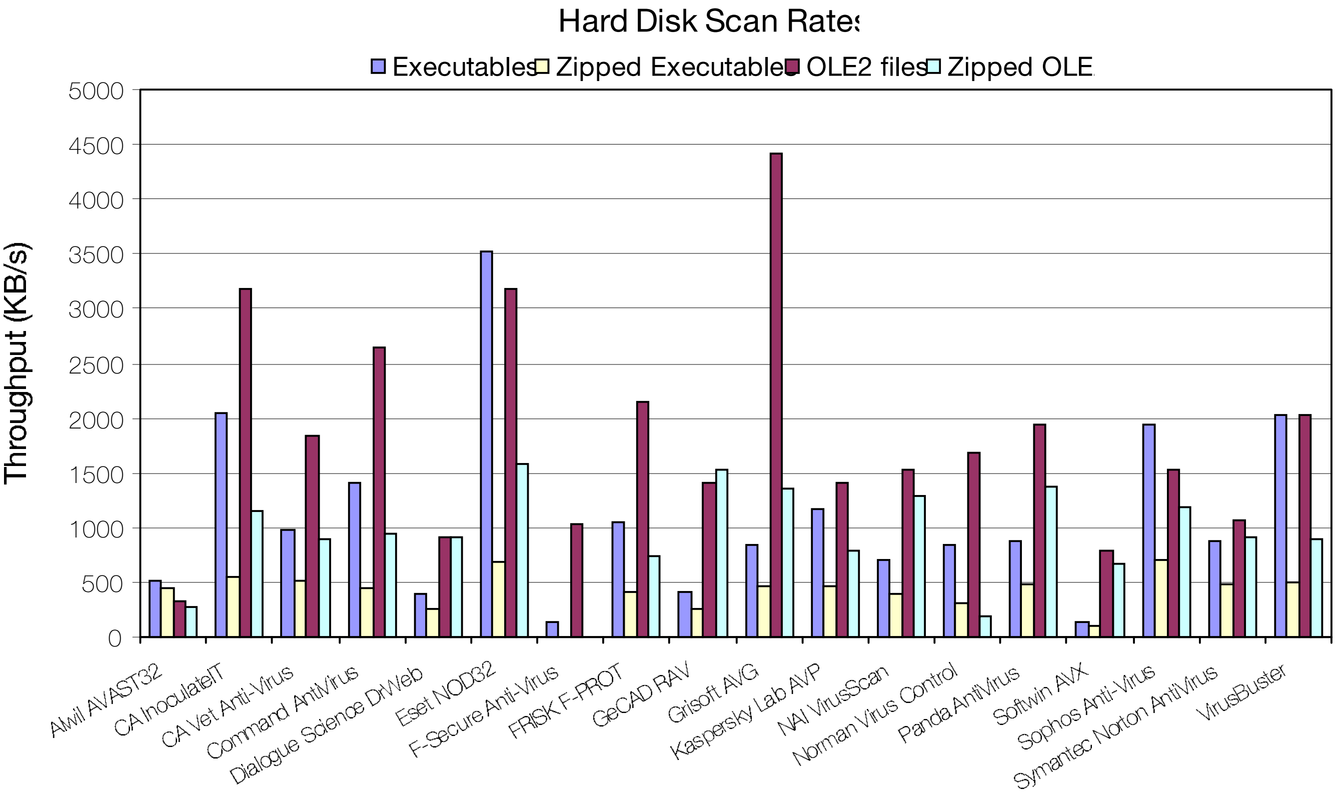
A product where niggles fight with good points in a deadlocked struggle, *Panda AntiVirus* (*PAV*) suffered a number of stability issues, and oddities in its reports. On-access scanning tests proved impossible without failure over a network, thus scanning was performed locally after several different configurations failed to fix the problem.

In common with the other product developers, *Panda* is keen to earn itself a VB 100% award. The feat was not achieved in this review due, quite simply, to a wholly inadequate default extension list. Sadly, a series of omissions from this list (somewhat unbelievably including the .SCR extension) caused *PAV* to miss a variety of files from the ItW set. No doubt the developers will be looking forward to the next Comparative, by which time the extension list will hopefully have been updated.

## Softwin AntiVirus eXpert v2000 (25/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 98.2% | Macro | 99.7% |
| ItW Overall (o/d) | 98.1% | Standard | 95.1% |
| ItW Overall (o/a) | n/a | Polymorphic | 90.5% |

The first of the two newer products, as far as *VB* is concerned at least, *Softwin* shared with its fellow newcomer a miss in the on-demand boot sector tests. On-access boot tests were another blast from the past since they were not present – a feature which will, we hope, be added as soon as possible. Results elsewhere, however, were promising, with only speed of processing being a particularly weak point. Presumably this will be slowed even further as extra



definitions are added, and it could be tricky to keep it within manageable margins. This is a point to follow in future appearances of *AntiVirus eXpert* (*AVX*) in *VB* Comparative reviews.

As well as the by now *passé* missing of JS/Unicle.A, TMC_Level-69 was also missed from the In the Wild set. Elsewhere a mixed selection of viral files passed through the detection net. Certainly a product which looks set to be among the top performers with a little improvement.

## Sophos Anti-Virus v3.33 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 99.7% | Macro | 99.4% |
| ItW Overall (o/d) | 99.7% | Standard | 98.2% |
| ItW Overall (o/a) | 99.7% | Polymorphic | 95.2% |

A not particularly happy outing for *Sophos Anti-Virus* (*SAV*) this time around, with numerous misses in areas where detection could have been simply obtained. The failure to detect all the JS/Unicle samples was added to by a lack of HTM scanning in this release which led to JS/Kak samples passing undetected through the test. In the Standard set, BAT/911's .PIF and .BAT components were also passed wholesale as non-viral. The HTM scanning has since been added as standard, but the lack in the intervening time can be considered rather inopportune.

This particular problem was perhaps less worrying than the missing of a selection of a few polymorphic virus samples within ACG.A and Win95/Sk.8044, since *SAV* has traditionally encountered few problems in the Polymorphic sets. One suspects that *Sophos* will be relieved that such a performance came at a time when few other VB 100% awards were received, and will be looking for a major improvement in the next *VB* Comparative.

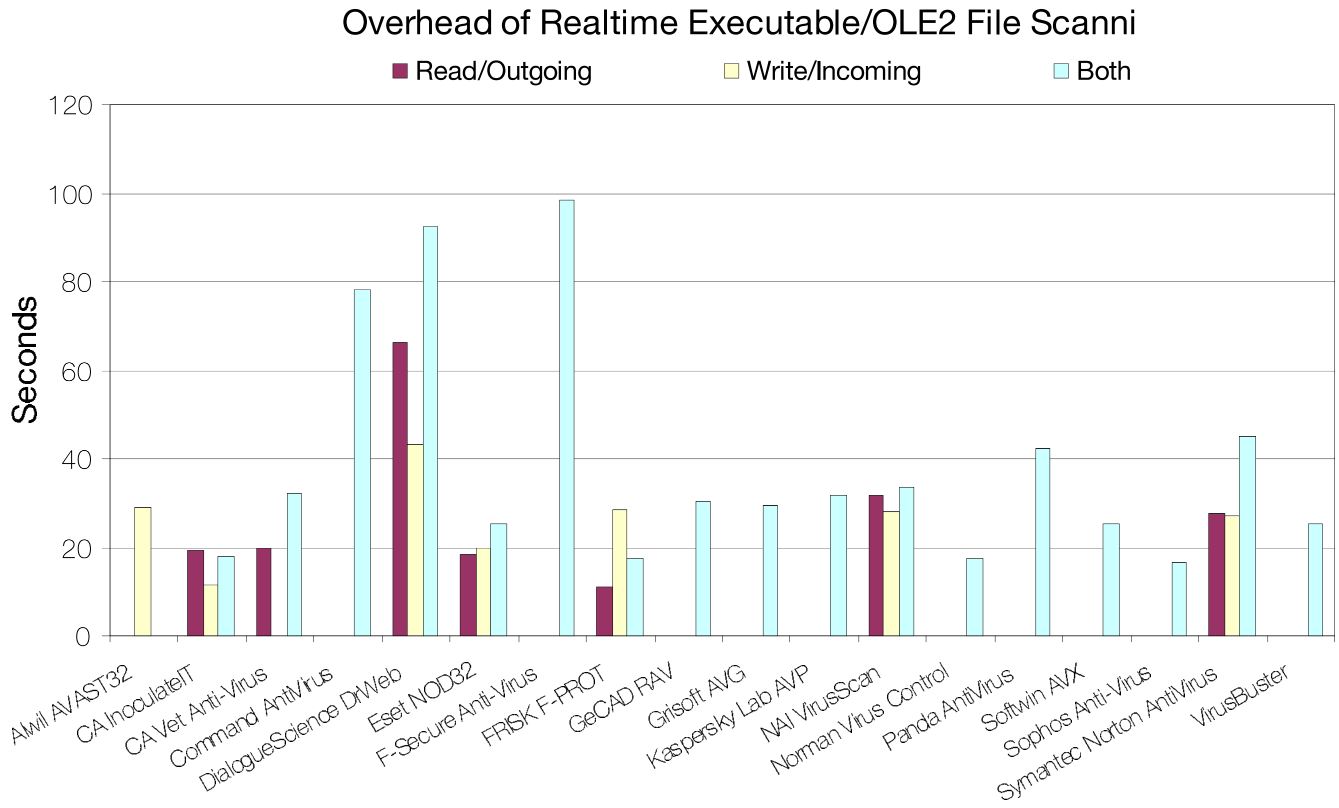
## Symantec Norton AntiVirus v5.02.04 (24/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.4% |
| ItW Overall (o/d) | 100.0% | Standard | 99.2% |
| ItW Overall (o/a) | 100.0% | Polymorphic | 94.7% |

The last of the three VB 100% awards this month, *Symantec* will no doubt make marketing capital of this slightly hollow victory. Polymorphic detection remains the *Norton AntiVirus* (*NAV*) weakpoint outside the WildList arena, though the misses here are not particularly damning given that they all fell within the samples of ACG.A and ACG.B. With results constant on-access and on-demand *NAV* definitely has cause to feel pleased with itself, but not perhaps to the same degree as some products which nevertheless failed to gain a VB 100% award this month.

## VirusBuster v3.0 (26/04/2000)

| | | | |
|---|---|---|---|
| ItW File | 85.9% | Macro | 93.9% |
| ItW Overall (o/d) | 86.3% | Standard | 91.6% |
| ItW Overall (o/a) | 85.7% | Polymorphic | 79.3% |



A second newcomer to *VB Win9x* Comparatives, *VirusBuster* had much the same baptism of fire as a number of the now well-respected products already reviewed. When reviewing a product for the first time there is always a niggling fear that there will be equal numbers of hits and misses, leading to maximum possible work, though in this case the detections were respectable if not particularly watertight. *VirusBuster* had slightly less detection ability on-access than on-demand, though this can be seen to be a common problem even with more mature products.

ItW and macro detection could in both cases be taken into the realms of good rather than OK detection by an improved implementation of *Word 97* scanning, whether by virus data or engine tweaking, since the vast majority of these misses fell into this category. More tricky to deal with might be the distinct weakness on the Polymorphic sets, though a slighly better than average scan rate should alleviate extra overhead on this front.

## Summary and Conclusions

A degree of comment concerning a couple of the samples included this month would seem to be in order. Firstly, the VB 100% awards are totally altered if JS/Unicle.A is omitted from calculations.

JS/Unicle was declared in the wild just after having been sparsely spotted (by two WildList reporters – the minimum required for a virus to make it to the list) and is a low threat (if at all) to the majority of AV users. It only operates correctly in a unicode environment, thus cutting out its threat in most of the more important market areas of those products submitted. This led to its not being a priority and not being available for some companies, thus the sparse detection in this test. However, JS/Unicle.A is on the WildList, and thus affects the allocation of *VB* scores in this, and future, Comparative Reviews. This provides yet another another opportunity to point out that VB 100% awards in one Comparative should not be used as some variety of ‘buyer’s guide’, for it is in the short term an award where luck plays its part.

Aside from the three products earning themselves the VB 100% award this month – *Command AntiVirus*, *Eset NOD32* and *Symantec Norton AntiVirus* – some other products performed admirably against the test-sets as a whole. Readers are encouraged to view the entirety of the results therefore, and not simply flick through the VB 100% awards. The next Comparative Review (*NetWare*) will feature in the September issue.

**Technical Details**

**Test Environment:** Server: *Compaq Prolinea 590*, 90 MHz Pentium with 80 MB of RAM, 2 GB hard disk, running *NetWare* 4.10. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, CD-ROM and 3.5-inch floppy, all running *Windows 98*. The workstations were rebuilt from image back-ups, and the test-sets were stored in a read-only directory on the server.

**Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/200007/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.