COMPARATIVE REVIEW

Windows-shopping

Though it did not prove to be as problematic as first thought, various stability problems were encountered in the previous *Windows 98* Comparative Review some six months ago. It was with a degree of trepidation, therefore, that *VB* approached this review.

Eighteen products from across the globe were submitted for entry into the *Windows 98* arena, four of the offerings featured in the previous test being absent this time – *eSafe Protect*, *Intel LANDesk*, *Norman ThunderByte* and *Stiller Integrity Master*.

Test Procedures

Three identical machines were used for every aspect of the testing, and the hard disks of each were completely rewritten from the appropate image files prior to the installation of each of the products. Despite the three machines being nearly identical, all the timed tests (disk scanning rates and overhead tests) were performed on a single PC disconnected from the local network. The other two machines were simultaneously used to perform both the on-demand and on-access detection tests.

The test-sets were updated from those employed in the previous comparative, and, where appropriate, matched to the February 1999 WildList. Due to a delay in the publication of the WildList, the call for products deadline was extended from 26 February to 3 March 1999.

Following its spring clean the WildList is merely a shadow of its former self totalling just 145 viruses compared to the 266 that featured in the March NT comparative (based on the January 1999 WildList). New additions to the list include W97M/Class.B, W97M/Ethan.A, W97M/Brenda.A and W97M/Nono.A. Additionally, the polymorphic multipartite One_Half.3577 joins its 3544 byte comrade.

For products that provided a facility to scan network drives, all detection tests were performed with the test-set stored on a network drive as a read-only share. For products that either did not permit the scanning of network drives or were incapable of producing a workable log-file, the test-set was copied to a local hard drive, and the products were set to ‘Delete File if infected’.

In all cases the detection tests were initially performed with the default configuration settings – i.e. those selected after a fresh installation prior to any user intervention. Perhaps the use of a larger, bolder typeface for this previous statement may help some of the developers register this point, but then again perhaps not? Following the first test runs performed with such configurations, the tests were typically repeated with alternative, more thorough, options selected. Details, where appropriate, can be found within the report for each product.

The timed tests were performed in accordance with previous comparatives, such that the scanning rates can be directly compared to previous results. Hard disk scanning rates were determined by timing the scanning of 5,500 executables, a process which doubles up as a false positive test. Floppy disk scanning rates were measured for both clean and infected files, using two disks, identical except that the files on one were infected with Natas.4744.

A second Clean set consisting entirely of OLE2 files is currently being prepared for future comparatives. This will facilitate the measuring of scanning rates over OLE2 files.

To measure the overhead of the on-access scanners, 200 files were moved using XCOPY. In contrast to previous comparatives, these 200 files were composed of 100 executables and 100 OLE2 (.DOC and .XLS) files. The OLE2 files were included in order to make the overhead tests as realistic as possible. The overheads have been normalized with respect to an average baseline of 12 seconds and are presented in units of time.

Complete detection and timed test results are presented in the main tables. The overall In the Wild detection rates are corrected by weighting them to the number of samples of each virus. Thus, for cases where there are multiple virus samples in a particular test-set (especially relevant to the Polymorphic test-set), the results are not distorted. The results reported in the summaries are only for on-demand scanning unless otherwise indicated.

Alwil Avast32 v2.0-730

ItW Overall	99.8%	Macro	96.5%
ItW Overall (o/a)	n/a	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.8%

In the last *Windows 98* comparative *Avast32* went home with a VB 100% award for total In the Wild detection, but unfortunately this was not to be repeated this time. Failure to detect one of the EXE samples of Win95/Fono was all that stood in its path.

Performance elsewhere in the testing was maintained at the level expected from previous reviews of *Avast32*. The Czech product once again proved to be as stable as ever, and unlike several of its competitors detected floppy disk changes consistently during the on-access scanning tests. High detection rates were returned against all the test-sets, the area of most concern perhaps being *Avast32's* detection of macro viruses.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	44	100.0%	525	99.9%	99.8%	2671	96.5%	14435	99.9%	1260	99.8%
CA InnoculateIT	44	100.0%	526	100.0%	100.0%	2747	99.1%	14433	99.9%	1258	99.7%
Command AntiVirus	44	100.0%	525	99.9%	99.8%	2737	99.0%	14444	100.0%	1251	99.3%
Cybec Vet AntiVirus	44	100.0%	523	99.7%	99.4%	2643	96.0%	14430	99.3%	1261	99.8%
Data-Fellows FSAV	44	100.0%	525	99.9%	99.8%	2747	99.3%	14444	100.0%	1252	99.6%
Dialogue Science DrWeb32	44	100.0%	526	100.0%	100.0%	2640	94.9%	14444	100.0%	1263	99.9%
Eset NOD32	44	100.0%	526	100.0%	100.0%	2750	99.3%	14444	100.0%	1264	99.9%
Frisk F-Prot	44	100.0%	526	100.0%	100.0%	2741	99.1%	14444	100.0%	1260	99.6%
GeCAD RAV	44	100.0%	509	99.0%	97.0%	2729	98.6%	13668	95.7%	1206	96.3%
Grisoft AVG	44	100.0%	525	99.9%	99.8%	2618	94.5%	14440	99.9%	1233	98.4%
H+BEDV AntiVir	42	95.4%	449	92.5%	86.1%	2419	88.5%	12930	85.8%	1239	99.0%
iRiS AntiVirus	44	100.0%	526	100.0%	100.0%	2750	99.2%	14433	99.9%	1258	99.7%
Kaspersky Lab AVP	44	100.0%	526	100.0%	100.0%	2754	99.4%	14444	100.0%	1261	99.8%
NAI VirusScan	44	100.0%	514	99.3%	97.8%	2742	99.2%	14190	98.8%	1264	99.9%
Norman Virus Control	44	100.0%	526	100.0%	100.0%	2712	98.3%	14444	100.0%	1249	99.5%
Proland Protector Plus	36	81.8%	318	65.9%	62.1%	1284	46.9%	2275	14.5%	658	60.5%
Sophos Anti-Virus	44	100.0%	526	100.0%	100.0%	2703	98.4%	14444	100.0%	1249	99.3%
Symantec Norton AntiVirus	43	97.7%	525	99.9%	99.6%	2725	98.4%	14443	99.9%	1247	99.5%

CA InnoculateIT v4.53

ItW Overall	100.0%	Macro	99.1%
ItW Overall (o/a)	97.8%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.7%

The user-friendly and intuitive (if slightly outdated) layout of the user interface initially lulled the innocent reviewer into believing that the testing of *InnoculateIT* from *Computer Associates* would be a relatively painless process. How true it is that first impressions can be deceptive…

On-demand ItW file and boot virus detection was perfect, resulting in *InnoculateIT* retaining its VB 100% award. This impressive detection rate is not the end of the story however. After finishing each scan of the test-set, the program hung immediately upon choosing another scan. Exiting and restarting the program avoided this problem, but on reloading, *InnoculateIT* gave false warning messages about viruses being in memory. Annoyances such as these have been encountered and reported in previous reviews, but hopefully, will be fixed in the near future so as not to plague *VB* in the future.

Matters became worse when testing the on-access scanner, which exhibited extremely poor stability. When attempting to open and close the infected test-set files stored on a network drive, a dialog box saying that REALMON had performed an illegal operation appeared persistently.

In order to test the on-access scanner therefore, the test-set had to be copied to a local drive, and the scanner set to delete infected files. Even then, only clusters of 100 or so files could be opened and closed without the system hanging. Trawling through the Polymorphic test-set in such a manner was considered too depressing, not to say onerous, a task and as a result the on-access capabilities of *InnoculateIT* have not been tested against this particular *Virus Bulletin* test-set.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	44	100.0%		n/t	n/a		n/t		n/t		n/t
CA InnoculateIT	44	100.0%	514	99.3%	97.8%	2734	98.8%		n/t	1255	99.6%
Command AntiVirus	44	100.0%	525	99.9%	99.8%	2737	99.0%	14444	100.0%	1250	99.3%
Cybec Vet AntiVirus	44	100.0%	523	99.7%	99.4%	2640	95.9%	14430	99.3%	1261	99.8%
Data-Fellows FSAV	44	100.0%	525	99.9%	99.8%	2750	99.3%	14444	100.0%	1252	99.5%
Dialogue Science DrWeb32	44	100.0%	526	100.0%	100.0%	2626	94.7%	14444	100.0%	1263	99.9%
Eset NOD32	44	100.0%	526	100.0%	100.0%	2750	99.3%	14444	100.0%	1265	100.0%
Frisk F-Prot	44	100.0%	526	100.0%	100.0%	2700	98.5%	14444	100.0%	1260	99.5%
Grisoft AVG	33	75.0%	264	58.6%	52.1%	1500	55.5%	1651	13.5%	719	67.3%
H+BEDV AntiVir	42	95.4%	457	92.3%	87.5%	2381	87.6%	13176	86.9%	1238	98.9%
iRiS AntiVirus	44	100.0%	526	100.0%	100.0%	2747	99.1%	14432	99.9%	1258	99.7%
Kaspersky Lab AVP	44	100.0%	526	100.0%	100.0%	2754	99.4%	14428	99.8%	1258	99.5%
NAI VirusScan	44	100.0%	513	99.2%	97.7%	2742	99.2%	14190	98.8%	1250	99.3%
Norman Virus Control	44	100.0%	526	100.0%	100.0%	2715	98.3%	14442	99.9%	1249	99.4%
Sophos Anti-Virus	44	100.0%	525	99.9%	99.8%	2704	98.4%	14444	100.0%	1249	99.3%
Symantec Norton AntiVirus	43	97.7%	525	99.9%	99.6%	2725	98.4%	14443	99.9%	1247	99.5%

Command AntiVirus v4.54 (SP1)

ItW Overall	99.8%	Macro	99.0%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.3%

This was a fairly middle-of-the-road performance by *Command Antivirus* (*CSAV*), with detection rates too low for any accolades, yet too high for significant rebuke. The VxD sample of Win95/Fono proved to be a thorn in its side, remaining undetected in both on-demand and on-access tests, denying *CSAV* the VB 100% award. Simply changing the configuration settings to ‘All Files’ mode did not remedy the situation, the VxD sample proving too elusive a prey. Though disappointed with incomplete ItW detection, *CSAV’s* developers can at least take heart from the high level of detection across the remaining test-sets.

In terms of speed *CSAV* is once again the fence-sitter, its performance somewhere in the middle of the pack, the scanning rate slightly improved over that reported previously. The overhead of the on-access scanner remains high, however, at a little over 400%.

Cybec Vet AntiVirus Premium v9.9.4.0

ItW Overall	99.4%	Macro	96.0%
ItW Overall (o/a)	99.4%	Polymorphic	99.3%
ItW Boot	100.0%	Standard	99.8%

Despite *Cybec’s* acquisition by *Computer Associates*, *Vet AntiVirus* is still attributed to the Australian development team. Three XLA samples of XM/Compat.A remained undetected during on-demand scanning pulling the VB 100% award away from *Cybec Vet’s* grasp. Complete detection of the In the Wild test-set was achieved with the configuration settings set to scan ‘All Files’, once again raising the issue of which file types to scan and which not. Detection rates elsewhere were respectable, although the Macro test-set proved troublesome.

Speed tests revealed *Vet* to be as fast as ever, although it was pipped to the winning post by a Slovakian competitor. The slight blemish on its high scanning speed was the reporting of a suspected infection during scanning of the hard disk Clean set. A commendably low overhead was observed upon activation of its resident protection.

Data Fellows F-Secure Anti-Virus v4.03.1090

ItW Overall	99.8%	Macro	99.3%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.6%

Data Fellows FSAV is another product this month to miss out on the VB 100% award thanks to Win95/Fono. Using the default settings, the VxD sample was missed in both on-demand and on-access scanning. This is attributable to the omission of the VxD file extension from the extensions list, since the sample was detected when the configuration settings were changed so that 'All Files' were scanned.

Respectably high detection rates were achieved against the other test-sets. The performance of *FSAV* against the macro test-set is much improved following the last comparative, the product showing a detection rate second only to *Kaspersky Lab's AVP* for both on-demand and on-access scanning. Infected *PowerPoint* presentation and template files and the extension-less samples of the O97M/Tristate variants accounted for all the misses in the Macro test-set.

Results were not quite so favourable in the speed tests, however. *FSAV*, though not the slowest, was at the slower end of the scale for both floppy disk and hard disk scanning, with throughputs of approximately 20 and 600 KB/s respectively. The overhead of the on-access scanner was significantly higher than that of the other products, a feature which has not previously been associated with *FSAV*. This is presumably attributable to the inclusion of OLE2 files in the file-set copied during the tests.

Dialogue Science DrWeb32 v4.04b

ItW Overall	100.0%	Macro	94.9%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.9%

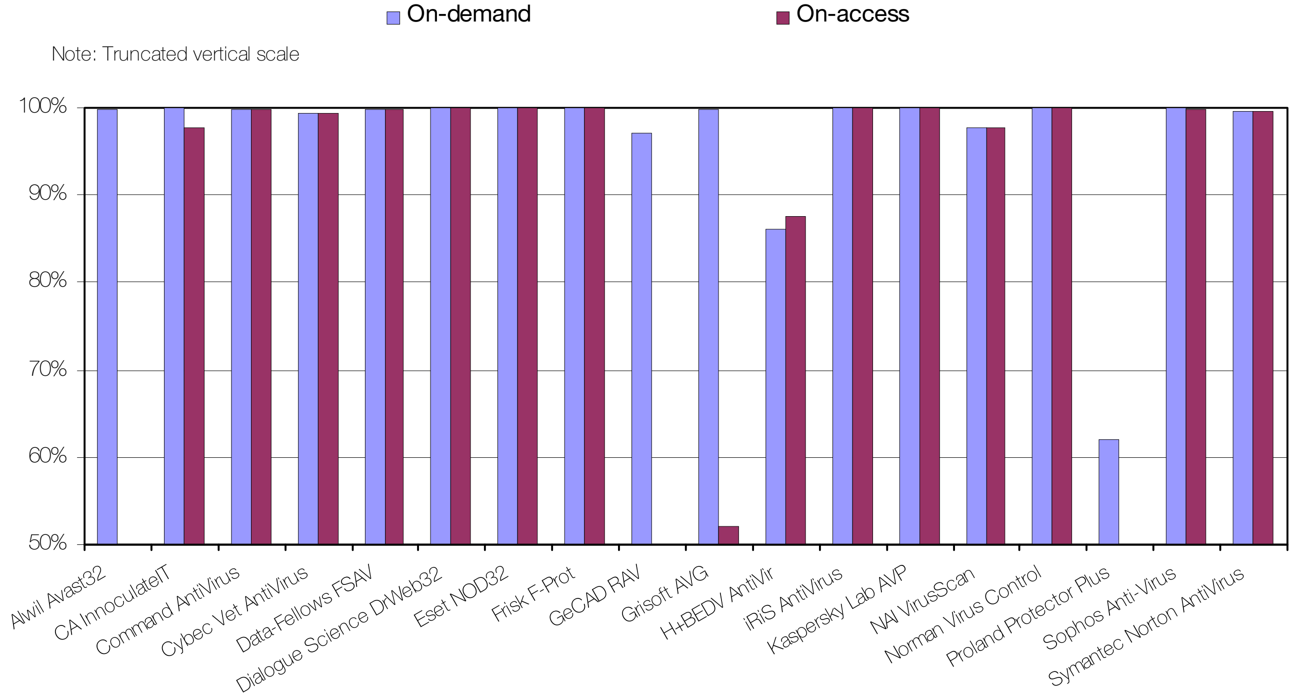
A beta product version was entered for this comparative by the Russian developers of *Dialogue Science's DrWeb32*. The interface is certainly outdated, but extremely straightforward and usable. Contrary to previously tested *DrWeb32* products, this version features an on-access component called *SpIDer Guard* for *Windows 98*.

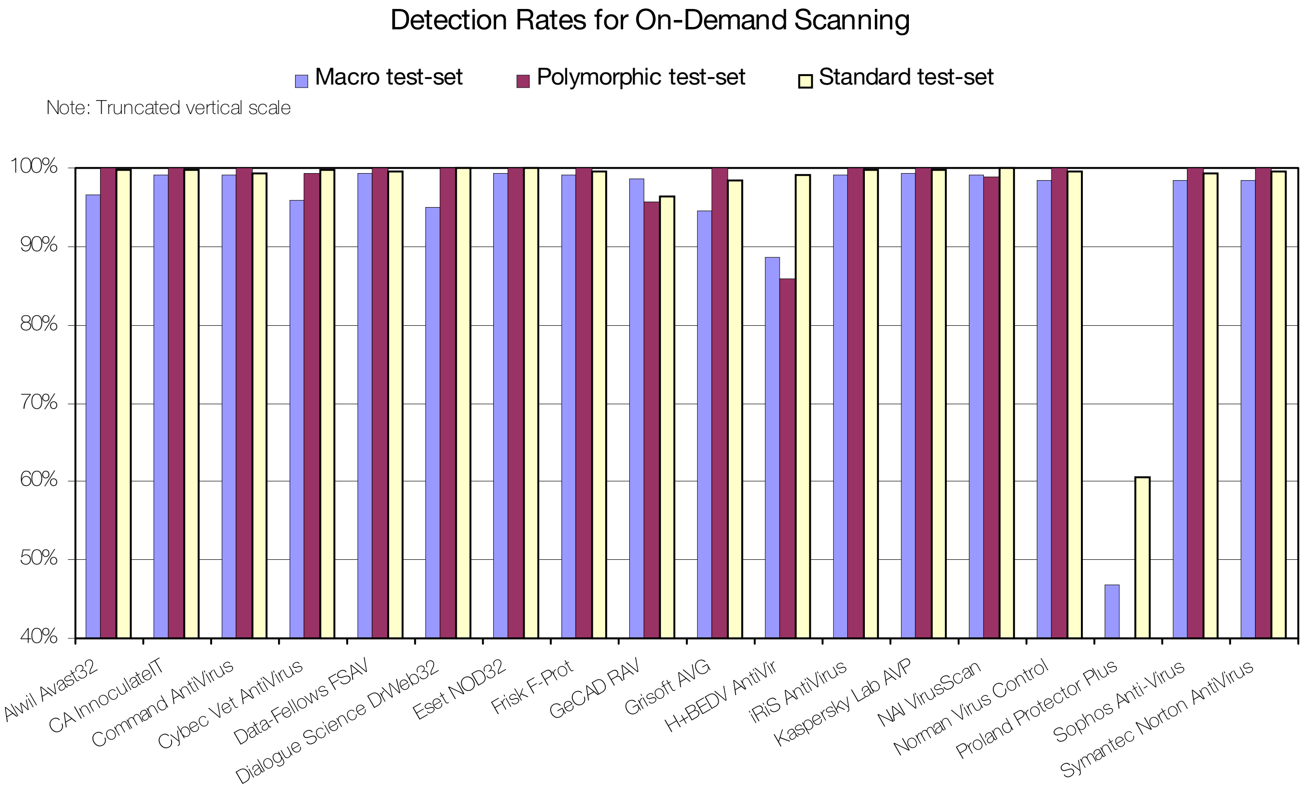
On-demand detection rates were admirable across all the test-sets, sufficient to earn *DrWeb32* the VB 100% award for detection of all the ItW viruses. The weakest area was detection of Macro viruses, where only a 94.9% detection rate was observed.

Extremely promising results were seen during testing of the new face of *DrWeb32*, the *SpIDer Guard* resident protection component. Detection rates mirrored those observed during on-demand scanning, the Macro test-set again proving more troublesome. Slight stability problems were encountered during testing of *SpIDer Guard*, mainly during on-access boot sector scanning.

Interestingly, the overhead of the on-access scanner when set to scan on File Open only, was much higher than that when scanning on File Close or File Open and Close. The hard disk scanning rate was at the slower end of the range

In the Wild Overall Detection Rates





for the products tested in this comparative but not significantly so. Perhaps more important were the false positives registered during scanning of the Clean test-set – one infection and 17 suspected infections were reported.

ESET NOD32 v1.15

ItW Overall	100.0%	Macro	99.3%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.9%

High detection rates on all platforms have been the norm for this Slovakian product in previous *Virus Bulletin* Comparative Reviews, and this month proved to be no exception. Aside from detecting all the In the Wild file and boot sector viruses, *NOD32* had the highest overall detection rates across all the other test-sets.

If this accolade was not enough, *NOD32* was also the leader of the pack in terms of both hard disk and floppy disk scanning rates. Only a slight overhead was observed when the on-access scanner was activated – impressive given the high detection rate.

Frisk F-Prot v3.04 (trial version)

ItW Overall	100.0%	Macro	99.1%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.6%

Better known as one of the engines behind the *DataFellows FSAV* product, this is the first showing of *F-Prot* as a standalone antivirus product in a *Virus Bulletin* review.

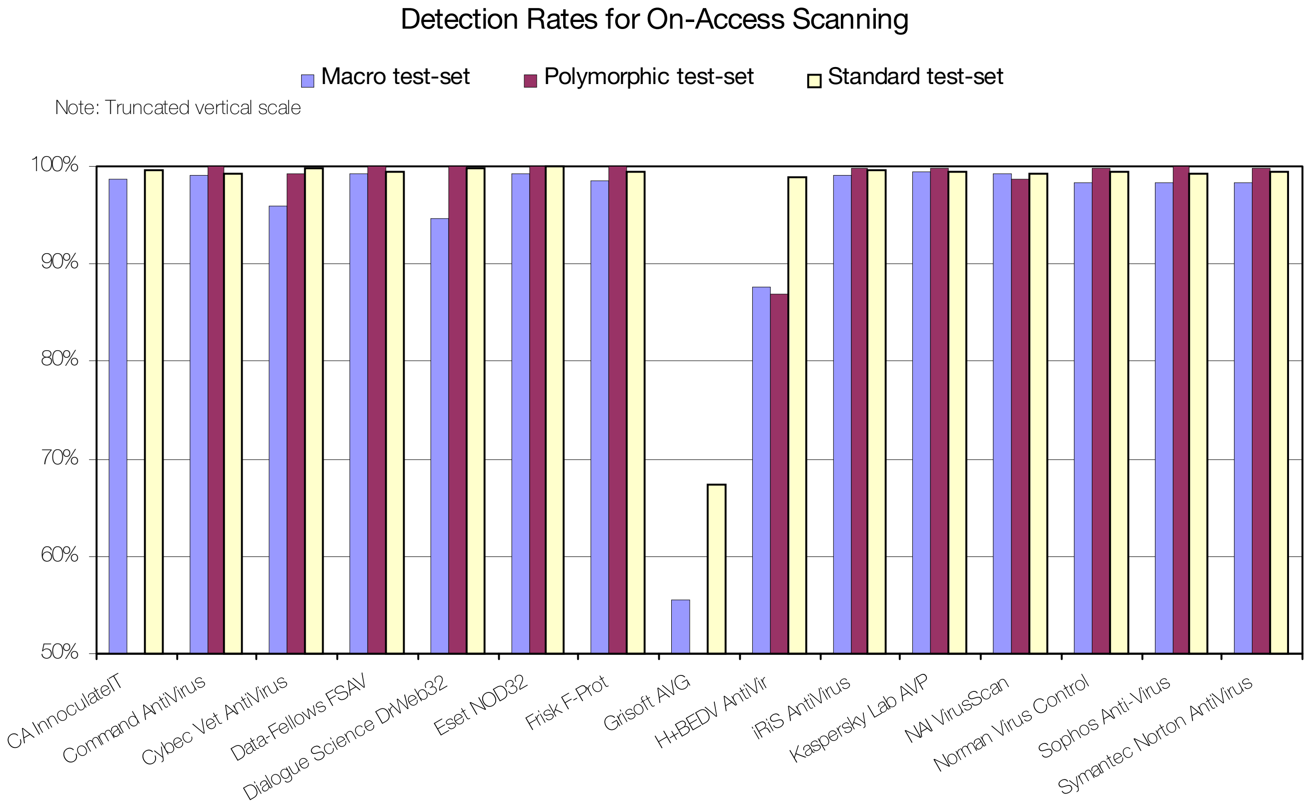
The Icelandic developers obviously believe that first impressions count, and *Frisk F-Prot* is up there with the best of them, delivering high detection rates across all the test-sets. Most importantly, complete ItW detection earns the newcomer a VB 100% award. At present this product is only commercially available in Iceland, Germany, Switzerland and Austria, although it was recently distributed on the cover CD of a major PC magazine. As to its availability elsewhere, it's a case of watch this space.

GeCAD RAV v6.54

ItW Overall	97.0%	Macro	98.6%
ItW Overall (o/a)	n/a	Polymorphic	95.7%
ItW Boot	100.0%	Standard	96.3%

Back in January 1998 Romania-based *GeCAD* submitted their anti-virus product *RAV v5.0* to *Virus Bulletin* for testing. Detection rates were far from perfect, but given that prior to testing the product was directed at a purely regional market, there were promising signs.

More than a year on from its first review, *RAV v6.0* has lived up to some of those early signs. All the ItW boot viruses were detected, but failure to detect 13 Marburg samples, 3 TPVO.3783.A samples as well as the VxD



Win95/Fono sample still keep the VB 100% award well out of reach. Elsewhere across the test-sets, the Polymorphic and Standard test-sets were *RAV's* weakest points in terms of detection rates.

Grisoft AVG v5.0.1241

ItW Overall	99.8%	Macro	94.5%
ItW Overall (o/a)	52.1%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	98.4%

Only one sample stood between *AVG* and its first VB 100% award, and there are no prizes for guessing which one. The VxD sample of Win95/Fono, having tripped up several other products in this review, was also missed by *AVG*. Unfortunately for the *Grisoft* developers, on-demand scanning of the other test-sets revealed slightly lower detection rates, especially in the Standard test-set.

The real weakness of *AVG* showed its face during on-access testing, however. Truly pathetic detection rates were observed against all the test-sets, with over 15,000 out of 19,000 virus samples missed. Little wonder then that the overhead of running the on-access scanner was negligible.

H+BEDV AntiVir v5.17.1.2

ItW Overall	86.1%	Macro	88.5%
ItW Overall (o/a)	87.5%	Polymorphic	85.8%
ItW Boot	95.4%	Standard	99.0%

Missing Win95/Fono and Moloch infected boot sectors coupled with a littering of misses against the ItW File-set led to *AntiVir* having the second worst ItW overall detection rate out of all the products submitted for testing – not pleasing news for the German *H+BEDV* development team. Against the other test-sets, detection rates were equally poor for on-demand and on-access scanning.

Aside from poor detection, the stability problems associated with the *VirusGuard* on-access scanner that were reported in a previous Comparative Review still remain. Numerous lock-ups and fatal exceptions were encountered during the overhead tests, making the process very laborious indeed. As if this were not enough, the 61 false positives reported during scanning of the Clean test-set ensure that the previously awarded timidity prize remains on its German mantelpiece.

iRiS AntiVirus v22.18

ItW Overall	100.0%	Macro	99.2%
ItW Overall (o/a)	100.0%	Polymorphic	99.9%
ItW Boot	100.0%	Standard	99.7%

As has come to be expected of *iRiS Antivirus* (*iRiS AV*) in recent times, detection rates across the board were admirably high. With perfect detection of all the ItW file and boot viruses *iRiS AV* picks up its fourth VB 100% award. Detection in the other test-sets was consistently 99% plus, the Macro test-set being the weakest point of *iRiS AV*.

	Scanning Speed						False Positives + [suspected]
	Diskette - Clean		Diskette - Infected		Hard Drive - Clean		
	Time (seconds)	Throughput (KB/s)	Time (seconds)	Throughput (KB/s)	Time (min:sec)	Throughput (KB/s)	
Alwil Avast32	37	26.9	48	25.0	49:54	182.7	0
CA InnoculateIT	49	20.3	41	29.3	07:40	1189.0	0
Command AntiVirus	47	21.2	48	25.0	06:32	1395.2	[1]
Cybec Vet AntiVirus	25	39.9	30	40.0	02:35	3528.6	[1]
Data-Fellows FSAV	47	21.2	60	20.0	15:02	606.4	3 + [4]
Dialogue Science DrWeb32	43	23.2	40	30.0	15:52	574.5	1+ [17]
Eset NOD32	23	43.3	49	24.5	02:30	3646.2	0
Frisk F-Prot	33	30.2	51	23.5	06:32	1395.2	[1]
GeCAD RAV	38	26.2	65	18.5	11:47	773.6	8
Grisoft AVG	28	35.6	53	22.7	09:37	947.9	8
H+BEDV AntiVir	33	30.2	46	26.1	10:08	899.6	61
iRiS AntiVirus	49	20.3	40	30.0	07:44	1178.7	0
Kaspersky Lab AVP	59	16.9	48	25.0	07:59	1141.8	0
NAI VirusScan	36	27.7	62	19.4	05:10	1764.3	0
Norman Virus Control	31	32.2	56	21.4	04:56	1847.7	0
Proland Protector Plus	59	16.9	60	20.0	06:34	788.1	89
Sophos Anti-Virus	40	24.9	34	35.3	04:06	2223.3	0
Symantec Norton AntiVirus	64	15.6	62	19.4	06:21	1435.5	0

The interface is not pretty and wins no prizes for glamour, but in terms of functionality and performance it leads by example. The scanning rates observed for *iRiS AV* are reasonable, and a modest overhead of approximately 150% was observed when the on-access protection was activated.

Kaspersky Lab AVP v3.0.129

ItW Overall	100.0%	Macro	99.4%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.8%

Another safe bet in the high detection stakes, *AVP* from *Kaspersky Lab* did nothing to disappoint its loyal followers. High detection rates were registered across the board, and the stability problems that have previously been reported during on-access scanning seem to have been fixed, thankfully. The only problem encountered during testing was a build error creating problems for the installation program to overwrite an old system library file. This was solved by simply overwriting the existing library file with a more recent version sent by *Kaspersky Lab*.

Besides achieving 100% detection rates for both on-demand and on-access scanning of the ItW test-set, excellent detection rates were also observed against all the other test-sets. Having said that, on-access scanning of the Polymorphic test-set perhaps exposed a slight weakness in *AVP's* near-infallible armour, the product failing to detect 16 samples distributed across five viruses.

On-demand scanning of diskette boot sectors was a breeze thanks to the multiple disk option which requires only a single keypress in between diskette changes. Speed has not been one of *AVP*'s strong points in the past, and little has changed in this respect. Only modest throughputs of approximately 1140 and 20 KB/s were observed for hard disk and floppy diskette scanning respectively. The overhead of running the on-access scanner was in keeping with the bulk of the other products, at approximately 150%.

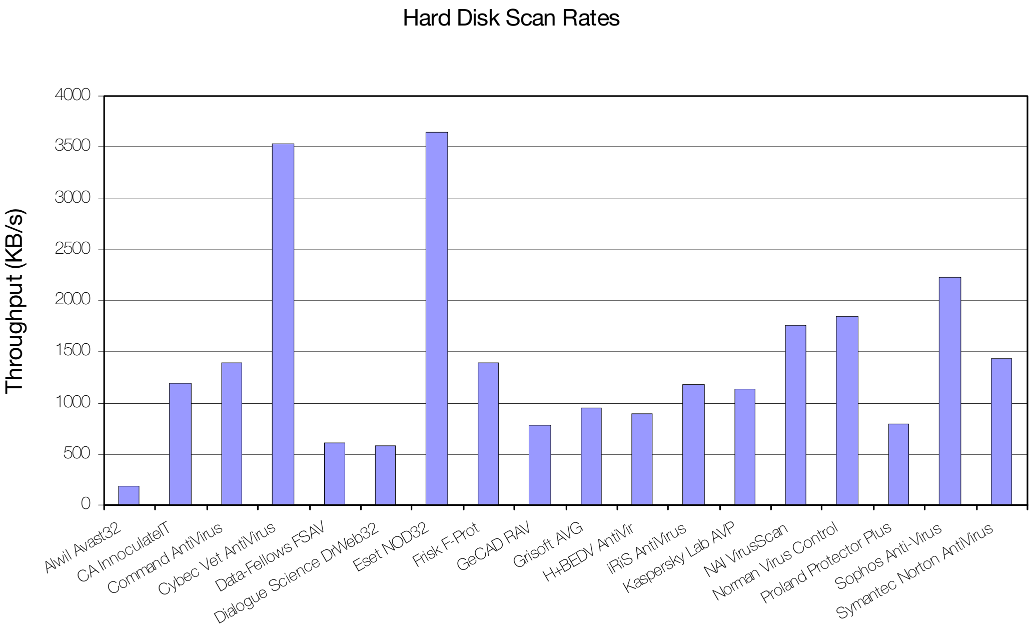
NAI VirusScan v4.0.2.4015

ItW Overall	97.8%	Macro	99.2%
ItW Overall (o/a)	97.7%	Polymorphic	98.8%
ItW Boot	100.0%	Standard	99.9%

Unfortunately for *Network Associates*, overall performance of the *McAfee*/*Dr Solomon's* hybrid seems to have dropped since the last *Windows 98* comparative review back in November 1998. The previously attained VB 100% award was missed this time around, due to the product failing to detect the screen saver (SCR) samples of Marburg and TPVO.3783.A. Just penance for failing either to bring the file extensions list up to date, or to introduce some sort of intelligent file type detection.

On the positive side, *NAI's VirusScan* was one of only two products to detect all the samples against the Standard test-set, and high detection rates were observed against the Macro and Polymorphic test-sets.

The overhead of running the *VShield* on-access scanner was noticeable (approximately 200%), but the stability problems reported in the previous comparative were not in evidence whatsoever.



Norman Virus Control v4.64

ItW Overall	100.0%	Macro	98.3%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.5%

The sole submission from *Norman* this comparative, *Virus Control* maintained the high standards it has set previously, attaining its seventh VB 100% award. A high level of protection is provided across the board by both the on-demand and on-access components, the latter being provided by the *Cat's Claw* component.

The '*Smart Behaviour Blocker*' that forms part of the *NVC* armoury is not testable by the standard procedures used throughout our tests, since as with *Alwil Avast32's* on-access scanner, it requires load-and-execute calls.

Proland Protector Plus v6.5

ItW Overall	62.1%	Macro	46.9%
ItW Overall (o/a)	n/a	Polymorphic	14.5%
ItW Boot	81.8%	Standard	60.5%

This is the third appearance of a *Proland Software* product in a *VB* comparative, the previous two being the *Windows NT*-based product versions. Once again the product name is irony itself, with extremely poor detection rates across the board. The pessimistic (or is it realistic?) will simply scoff at the presented statisitcs, dismissing *Protector Plus* as a contestant barely suitable for a first round warm-up.

The optimistic will see signs of improvement in the detection rates, especially in the detection of boot sector infections. Such signs are there, although many may argue that it would take a fool rather than an optimist to choose to protect their system with this Indian anti-virus offering.

Sophos Anti-Virus v3.19

ItW Overall	100.0%	Macro	98.4%
ItW Overall (o/a)	99.8%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.3%

In the fortunate position of being the alphabetical successor to *Proland Software's* meagre offering, *Sophos AntiVirus* (*SAV*) is the opera singer following the karaoke flop.

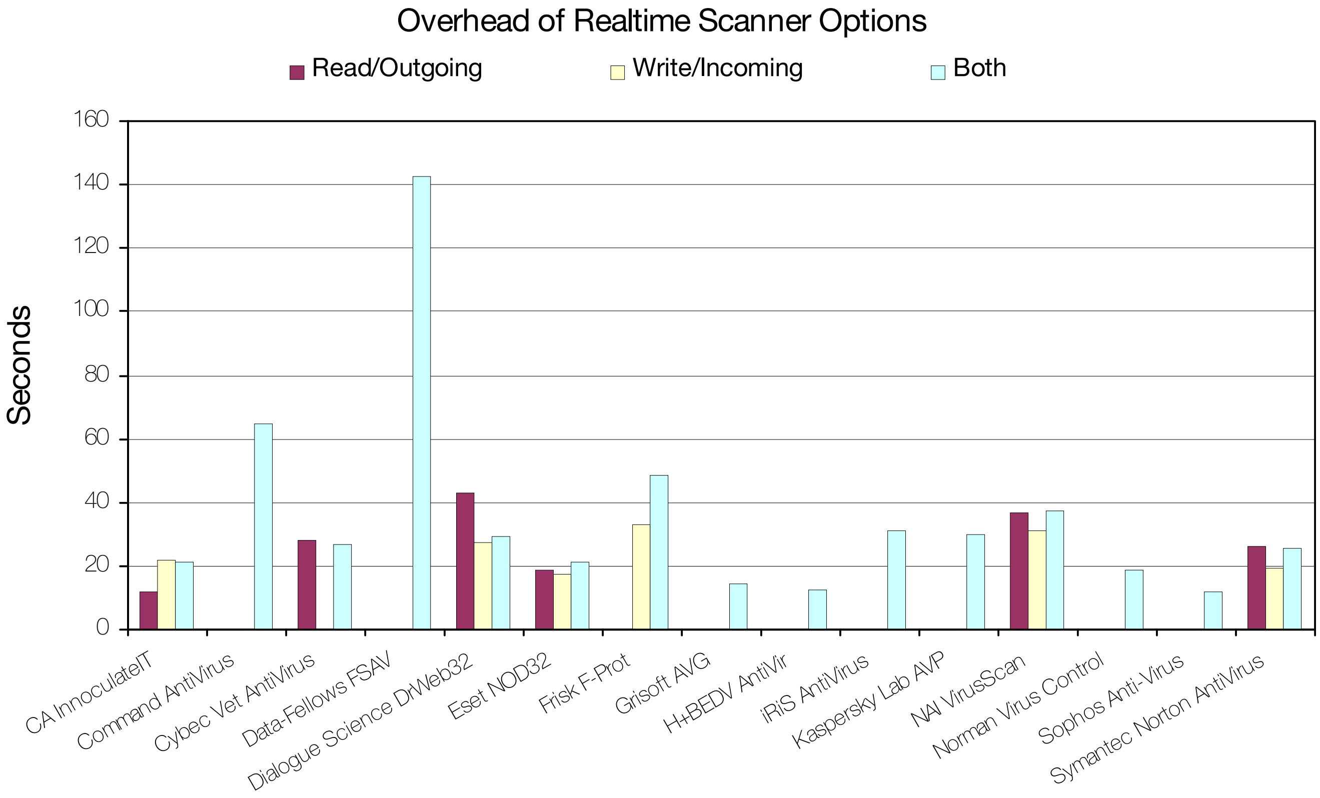
Maintaining the high standard that has been evident through previous comparatives, *SAV* is the last candidate in this line-up to receive the VB 100% award. Interestingly the on-access component *InterCheck* does not quite match up to the on-demand scanner, missing the troublesome VxD sample of Win95/Fono from the ItW test-set.

Along with several other products, detection in the Polymorphic test-set was perfect for both on-demand and on-access scanning. However, detection rates in the Standard and Macro sets though high, are not quite up to the mark set by many of *SAV's* competitors.

Symantec Norton AntiVirus v5.01.03

ItW Overall	99.6%	Macro	98.4%
ItW Overall (o/a)	99.6%	Polymorphic	99.9%
ItW Boot	97.7%	Standard	99.5%

Another 'big name' product failing to deliver the goods that might be expected from previous reviews is *Norton AntiVirus* from *Symantec*. Samples were missed in both the ItW File and Boot test-sets, Win95/Fono being the proverbial eel on both occasions. *Virus Bulletin* has been informed that the detection problems encountered with Win95/Fono have now been sorted out, but only after submission of *NAV* for this review.



Detection in the ItW File test-set was 100% when the on-demand scan was run in 'All Files' mode. However, even the simple remedy of adding VxDs to the default file extension list would not have brought the 100% award home to *NAV*, since the Win95/Fono infected boot sample was also missed.

Conclusions

In answer to the question of stability worries mentioned at the start of this review, thankfully no major problems were encountered. The on-access components caused most of the error messages, blue screens of death and system hangs that were observed.

Detection levels were generally very high, with eight, fourteen and sixteen products detecting 99% plus of the samples in the Macro, Polymorphic and Standard test-sets respectively (on-demand scanning). Similarly high detection rates were observed for on-access scanning of these test-sets for the products offering what has come to be a semi-essential feature of any anti-virus product.

Congratulations are due to the eight finger-on-the-pulse products who managed complete detection (on-demand) of the viruses in the February 1999 WildList. So hats off to *CA InnoculateIT*, *Dialogue Science DrWeb32*, *Eset NOD32*, *Frisk F-Prot*, *iRiS AV*, *Kaspersky Lab AVP*, *Norman Virus Control* and *Sophos AntiVirus*. Win95/Fono has been on the WildList since December 1998, and so the problems it has caused products seem inexcusable. For whatever reasons, various products missed infected files and/or boot sectors.

The age-old issue of what and what not to scan, seems to creep into each and every Comparative Review. This is not surprising – were we to run all the tests with each product set to scan 'All Files' the detection rates would certainly be higher and the marketing teams happier, but unfortunately the VB 100% award would also become cheaper.

With continual developments in the field of Macro viruses, choosing what to scan according to file extension alone is far too simplistic. Samples are not introduced into the *Virus Bulletin* test-sets purely with the aim of catching products out. Instead they simply reflect real world viruses as best possible. Users are not concerned with file extensions or file types. They merely demand what is offered on the box – protection from in the wild viruses. Unless developers are on the ball, forthcoming changes to the WildList could see some of the VB 100% awards slipping from the fingers of some established products.

Technical Details

Test Environment: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, all running *Windows 98*. The workstations could be rebuilt from image backups and the test-sets were in a read-only directory on the server. All timed tests were performed on one machine that was not connected to the network during the timed tests, but otherwise configured identically to the detection test condition.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199905/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.