COMPARATIVE REVIEW

NTirely Up to You

Nick FitzGerald

The first *Virus Bulletin* comparative review I oversaw was on the *NT* platform, so perhaps it is fitting that it is the platform for this, likely my last. Eighteen months ago, eighteen products lined up. Now, with several 'new' products relative to that review, we again have eighteen products to test due to various acquisitions and mergers.

Twelve products in the September 1997 review sported on-access scanners. Thirteen of the reviewed products here have full-featured on-access scanners – meagre progress – but one consistently crashed when this option was enabled. The more things change, the more they stay the same…

Test-sets and Procedures

All of the detection tests were run on three essentially identical machines under *NT 4.0* with Service Pack 4 applied. To remove any possible variation due to inconspicuous hardware differences, a single machine was used for all speed and overhead tests.

The *VB* test-sets were updated, and most importantly the In the Wild File and Boot test-sets were aligned to the December 1998 WildList. As that WildList was posted a little later in the month than is usual, the product developers were given an extended submission deadline of 6 January 1999. Of some personal interest to the reviewer was the performance of the products against W97M/ColdApe – the A variant of which was new to the December WildList, but both were clearly 'doing the rounds' at the time.

Also newly added to the In the Wild test-set were several Laroux variants. As a few products have shown something of a weakness on *Excel* macro viruses in the past, the impact of this development, if any, on the the In the Wild File results should be noted.

Whenever possible, the tests were run against a copy of the test-sets stored on a read-only share on a server. Various, but fortunately few, problems were encountered with this setup and they were resolved by copying the test-set from CD to a local drive for the duration of each test that required this. One or two test cases were run directly against the test-sets on CD, removing the need to copy the virus samples to hard disk, though this was prone to triggering 'inpage operation' faults from *NT*, and on occasion Blue Screens of Death (BSOD).

In all cases, the software under test was installed and configured in its default form, unless the requirements of a given test condition dictated otherwise. For example, on-access components were completely disabled while running on-demand tests and report files were always generated for the main detection tests, regardless of the default setting for that option but left at the default setting for speed tests. All tests were run from the local Administrator usercode on the workstation and as a very low-privileged usercode on the server, having only read access to the test-set directory tree.

The products were, of course, subjected to *VB's* typical speed and overhead tests. The hard disk scanning test, combining speed and false positive testing on the 5500 executables of the *VB* Clean test-set, should produce results directly comparable with recent *NT* comparatives.

The overhead introduced by the on-access scanner was tested using XCOPY to move large numbers of executables, the results being compared against a baseline and normalized across the products for subsequent presentation. Floppy disk speed tests were performed upon two almost identical disks, differing only in that the files on one were universally infected with Natas.4744.

As usual, developer requests to run in 'all files' mode or with special commandline options were ignored. Whilst it is undoubtedly true that many 'typical users' of these products run them with other than the 'out of the box' settings, this observation provides little indication of what might represent 'typical usage'. Much of the general use of these products will simply be with the 'factory settings', and that condition is easily configured by others wishing to reproduce the test conditions.

It should also be noted that the same vendors who ask for 'full-paranoia' modes (all files, high heuristics), often equally strongly advocate 'standard settings' when speed and false positive testing is under discussion. You can't have your cake and eat it too…

In fact, this issue accounts for the differences often seen between *VB* test results and those of various certification agencies. A product *VB* claims fails to obtain 100% against the touchstone In the Wild test-set, may well do so if run in full-paranoia mode. Unless false positive and speed tests are run with the same settings, however, the meaning of the results as a whole is an open question.

The complete detection tests are reported in the main tables. The results reported in the summaries are only the on-demand ones, plus the on-access result for the combined In the Wild test-sets, where applicable.

Aladdin eSafe Protect v2.0

ItW Overall	99.3%	Macro	91.3%
ItW Overall (o/a)	99.2%	Polymorphic	91.8%
ItW Boot	98.8%	Standard	97.7%

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Protect	83	98.8%	840	99.4%	99.3%	2426	91.3%	13637	91.8%	1010	97.7%
Alwil Avast32	84	100.0%	856	99.9%	99.9%	2578	96.7%	14435	98.7%	1046	99.7%
CA InoculateIT	83	98.8%	853	99.5%	99.4%	2608	97.9%	14433	99.1%	1046	99.7%
Command AntiVirus	84	100.0%	844	99.6%	99.5%	2647	99.4%	14198	97.4%	1036	99.2%
Cybec Vet Anti-Virus	84	100.0%	842	99.5%	99.5%	2555	96.1%	14185	97.3%	1043	99.5%
Data Fellows FSAV	84	100.0%	856	99.9%	99.9%	2665	99.8%	14444	100.0%	1037	99.5%
DialogueScience Dr Web32	75	89.3%	857	100.0%	99.0%	2511	94.2%	14444	100.0%	1051	99.7%
ESET NOD32	84	100.0%	857	100.0%	100.0%	2657	99.5%	14444	100.0%	1046	99.7%
GeCAD RAV	83	98.8%	843	99.6%	99.4%	2631	98.6%	13668	94.5%	1001	96.1%
Grisoft AVG	76	90.5%	856	99.9%	99.1%	2071	77.4%	13496	93.3%	913	87.9%
iRiS AntiVirus	84	100.0%	857	100.0%	100.0%	2652	99.4%	14433	99.1%	1046	99.7%
Kaspersky Lab AVP	84	100.0%	857	100.0%	100.0%	2626	98.3%	14444	100.0%	1046	99.7%
NAI NetShield NT	84	100.0%	857	100.0%	100.0%	2653	99.5%	14091	96.7%	1046	99.7%
Norman Virus Control	84	100.0%	857	100.0%	100.0%	2612	98.1%	14444	100.0%	1046	99.7%
Proland Protector Plus	48	57.1%	470	58.8%	58.6%	1219	46.3%	1735	10.7%	494	54.1%
Sophos Anti-Virus	84	100.0%	857	100.0%	100.0%	2614	98.6%	14444	100.0%	1035	99.2%
Symantec Norton AntiVirus	83	98.8%	856	99.9%	99.8%	2644	99.1%	14443	98.7%	1037	99.5%
Trend OfficeScan NT	82	97.6%	856	99.9%	99.7%	2496	93.8%	14319	96.8%	1026	98.7%

Recently purchased by *Aladdin Knowledge Systems* (*AKS*), the former *eSafe* product shows little sign of change yet, if in fact, any is likely. Virus scanning is one part of the complex of functionalities that *eSafe Protect* provides and finding the desired configuration settings amongst its plethora of options could be daunting to the less-experienced user. This is not necessarily a bad thing!

Hare.7610 on a 1.44 MB diskette is still *eSafe's* bugbear in the ItW Boot test-set, but was not solely responsible for the product's failure to reach VB 100% performance. The Win95/Fono VxD, Win95/Marburg-infected screen savers and all *Windows* (NE) EXE samples of TPVO.3783.A were also missed.

Detection percentages in the low nineties on the Macro and Polymorphic test-sets are not encouraging compared to most other products in the review. *eSafe Protect* has something of a penchant for missing the template sample forms of *Word* macro viruses (those samples usually being derived from the NORMAL.DOT off the replication machine). Given that whilst not necessary, most successful macro viruses do infect the default global template, the persistence of this effect in *eSafe's* results (and in those of its forerunner, *ViruSafe*) is of concern.

Initially, on-access tests proved problematic, with Dr Watson intervening part-way through the tests and closing what it considered was an errant process – namely the *eSafe Protect* scanning service. *AKS* staff confirmed a problem and were working on a fix as this copy went to proof. After reporting this to *AKS*, however, another fresh install was tried and this time the on-access tests ran to completion.

AKS claimed that the on-access scanner should detect exactly the same viruses as the on-demand one, and the (mainly) small difference between the results of the two scanning tests may be due to lingering issues with a not fully functional service. But then, I have been told innumerable times by many vendors that both test modes should return the same results, and experience tells me this is the exception rather than the rule. That said, *eSafe Protect's*

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Protect	82	97.6%	840	99.4%	99.2%	2420	91.1%	12617	84.7%	1010	97.7%
Alwil Avast32	84	100.0%		n/t	n/a		n/t		n/t		n/t
CA InoculateIT	73	86.9%	841	99.1%	97.9%	2595	97.4%	14187	96.5%	1046	99.7%
Command AntiVirus	73	86.9%	844	99.6%	98.4%	2647	99.4%	14198	97.4%	1036	99.2%
Cybec Vet Anti-Virus	84	100.0%	796	93.0%	93.6%	2560	96.2%	12669	86.9%	363	31.1%
Data Fellows FSAV	84	100.0%	856	99.9%	99.9%	2645	99.4%	14444	100.0%	1037	99.5%
ESET NOD32	84	100.0%	857	100.0%	100.0%	2657	99.5%	14444	100.0%	1041	99.5%
Kaspersky Lab AVP	84	100.0%	857	100.0%	100.0%	2636	98.7%	14444	100.0%	1046	99.7%
NAI NetShield NT	84	100.0%	845	99.6%	99.6%	2653	99.5%	14091	96.7%	1046	99.7%
Norman Virus Control	73	86.9%	844	99.6%	98.4%	2612	98.1%	14198	97.4%	1038	99.5%
Sophos Anti-Virus	84	100.0%	857	100.0%	100.0%	2614	98.6%	14444	100.0%	1035	99.2%
Symantec Norton AntiVirus	83	98.8%	856	99.9%	99.8%	2644	99.1%	14443	98.7%	1037	99.5%
Trend OfficeScan NT		n/a	856	99.9%	n/a	2502	94.0%	14319	96.8%	1026	98.7%

past test results show it does detect the same viruses in both modes consistently, so the divergence here probably was due to the problems noted with the service.

The on-access scanner would appear to have been rewritten, or at least seriously tweaked, since the previous *NT* comparative, as an overhead approaching 100% is nothing like the current incarnation's performance. On these tests, *eSafe Protect* joins *Vet AntiVirus* and *Sophos Anti-Virus* in returning a slightly negative 'overhead'.

Alwil Avast32 v7.70

ItW Overall	99.9%	Macro	96.7%
ItW Overall (o/a)	n/a	Polymorphic	98.7%
ItW Boot	100.0%	Standard	99.7%

Alwil's Avast32 turned in a highly creditable performance, being pipped at the VB 100% post by a single sample – the VxD form of Win95/Fono. Staking 96.7% against the Macro test-set as the weakest result should bring satisfaction to any developer, and with on-demand detection levels around 99% and higher on all other test-sets, this was yet another solid outing from this Czech product.

VB's standard on-access testing mechanism does not allow the detection rate of *Avast32's* resident scanning function to be assessed. This is due to the latter's dependence on file execution rather than 'file open' or 'file read' operations, which other products intercept. The clean hard disk speed test result appears unflattering but as we have noted before, this is a feature. *Avast32* runs on-demand scans in a low priority thread and thus can be left performing a full drive scan with minimal impact on other applications.

CA InoculateIT v4.5

ItW Overall	99.4%	Macro	97.9%
ItW Overall (o/a)	97.9%	Polymorphic	99.1%
ItW Boot	98.8%	Standard	99.7%

Returning good, solid-looking detection on-demand, *InoculateIT's* on-access detection may not be up to the mark these results suggest. It missed a VB 100% award by not detecting W97M/ColdApe.A and the polymorphic boot infector Win95/Fono in the ItW Overall test-set.

InoculateIT's on-access component has no 'deny access' option. Thus, a variation on the usual test method, which depends upon 'on open' detection and a 'deny access' response, had to be employed. In this case, the alternative process involved copying the complete test-set from the server to the test machine with the shield program set to detect only on writes and to delete infected files.

Once completed, about 75% of the test-set resided on the workstation's drive. This was a surprisingly high proportion of the total test-set. A further round of copying this partial

	Scanning Speed						False Positives
	Diskette - Clean		Diskette - Infected		Hard Drive - Clean		
	Time (seconds)	Throughput (KB/s)	Time (seconds)	Throughput (KB/s)	Time (min:sec)	Throughput (KB/s)	
Aladdin eSafe Protect	58	17	116	10	14:48	601	0
Alwil Avast32	64	15	76	16	45:32	196	0
CA InoculateIT	156	6	184	6	6:56	1284	0
Command AntiVirus	62	16	70	17	8:06	1099	1
Cybec Vet Anti-Virus	57	17	66	18	2:27	3633	0
Data Fellows FSAV	120	8	138	9	16:51	528	2
DialogueScience Dr Web32	70	14	170	7	24:00	371	19
ESET NOD32	35	28	65	18	3:20	2671	0
GeCAD RAV	60	16	63	19	11:18	788	8
Grisoft AVG	59	10	67	17	3:43	2395	0
iRiS AntiVirus	57	17	70	17	8:00	1113	0
Kaspersky Lab AVP	60	16	74	16	6:12	1436	2
NAI NetShield NT	241	4	266	4	8:13	1083	0
Norman Virus Control	59	17	95	12	5:24	1648	0
Proland Protector Plus	114	9	125	9	1:16	4606	61
Sophos Anti-Virus	57	17	64	18	3:40	2428	0
Symantec Norton AntiVirus	155	6	169	7	7:35	1174	0
Trend OfficeScan NT	60	487	62	20	5:41	1566	2

test-set to another folder on the PC, wiping the source directory, copying the remaining files back and so on was tried. This resulted in further detections. In total, more than thirty iterations of this procedure were required before three successive runs saw no further files being deleted.

The on-access results presented here were recorded at that point. Although close to the on-demand results, they are not the same and the testing procedure clearly uncovered a weakness in the scanner's architecture. Despite this, the general stability of the product seems much improved over recent-past outings in *VB* tests. Speed was middling and on-access overhead approached 75%.

Command AntiVirus v4.54 8 Dec 1998

ItW Overall	99.5%	Macro	99.4%
ItW Overall (o/a)	98.4%	Polymorphic	97.4%
ItW Boot	100.0%	Standard	99.2%

Command Software AntiVirus (*CSAV*) failed to detect the screen saver (SCR) samples of TPVO.3783.A and Win95/Marburg, as well as the Win95/Fono VxD in the In the Wild File test-set, thus missing out on a VB 100% award.

With detection rates in the high ninety percent range, *CSAV* performs well, if a little more slowly than most of its competitors. Its main weakness in these tests was 86.9% against the ItW Boot test-set under on-access scanning.

Samples with invalid BPBs simply resulted in 'not accessible' error dialogs, rather than notification of the viruses thereon. These same diskettes were correctly identified as infected by the on-demand scanner, so *CSAV* is its own proof that what we were asking of it was not unreasonable.

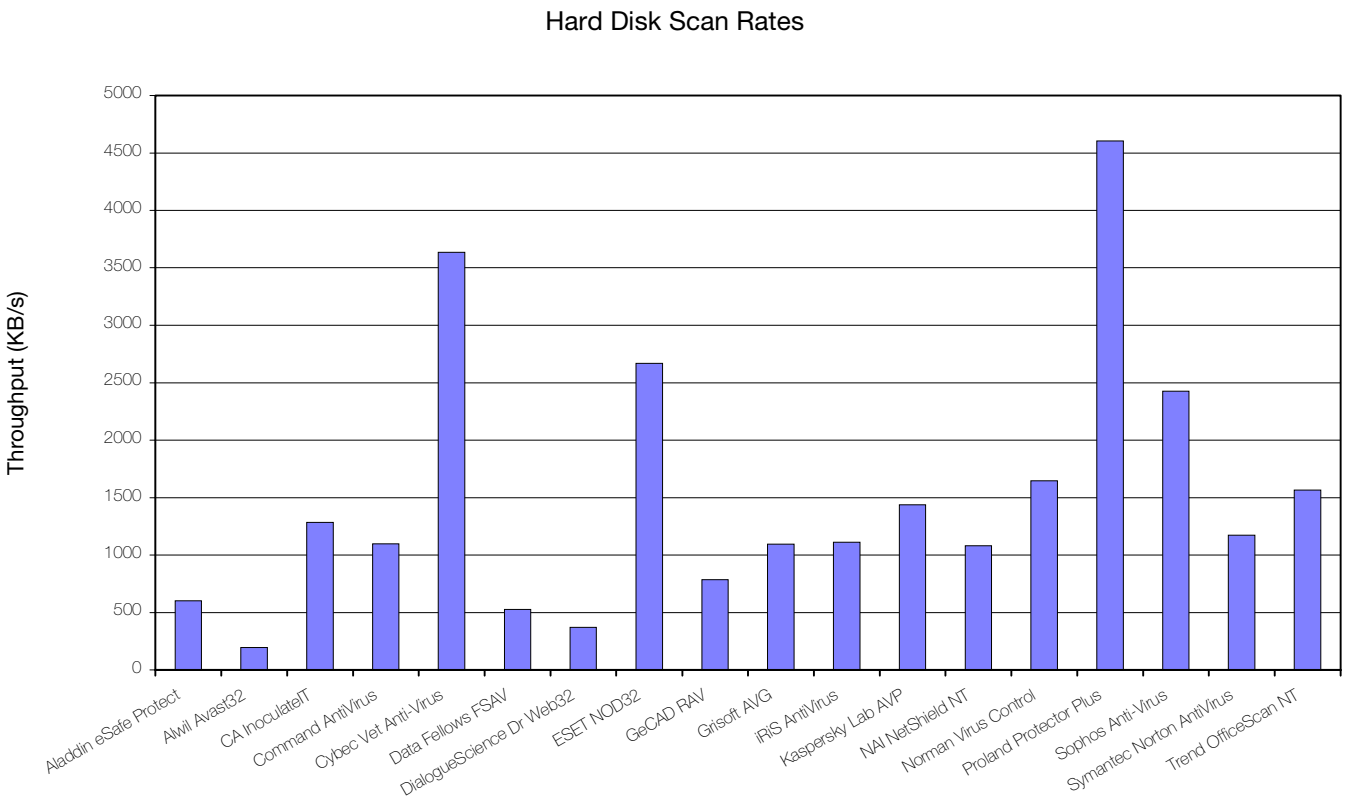
One false positive was registered against the Clean test-set – a 'destructive program'. In keeping with the less than meteoric speed, *CSAV's* overhead was on the high side at 143% once DVP (Dynamic Virus Protection) was enabled.

Cybec Vet AntiVirus v9.93

ItW Overall	99.5%	Macro	96.1%
ItW Overall (o/a)	93.6%	Polymorphic	97.3%
ItW Boot	100.0%	Standard	99.5%

Cybec's Vet was another product to miss SCR infections of TPVO.3783.A and Win95/Marburg in the In the Wild File test-set. It also missed three samples of XM/Compat.A in XLA files. These same Compat and Marburg factors accounted for all its misses in the Polymorphic test-set.

As usual, speed was of the essence with *Vet* and, ignoring *Proland Protector Plus*, it returned 40% higher throughput than the next fastest product. It again returned reliably



negative on-access overhead – as with *eSafe Protect* and *Sophos Anti-Virus*, some file I/O operations are actually faster when its on-access scanner is installed and enabled, than prior to installation of the product.

Overall, on-access detection rates are somewhat lower than their on-demand counterparts. This appears to be by design, with the less common members of the Standard test-set more likely to be missed relative to on-demand performance. The oddity among these results occurred in the Macro test-set, where a slightly higher detection rate was recorded on-access – this was accounted for by *Vet* detecting the XLM samples, generated naturally by five of the *Excel 95* viruses in that set.

One may question the wisdom of electing not to detect viruses 'officially recognized' as being in the wild. Even if one's customers have not (yet) reported the vermin in question, their detection would seem important given these viruses are (or have been), in some strong sense, 'common'.

Data Fellows F-Secure Anti-Virus v4.03

ItW Overall	99.9%	Macro	99.8%
ItW Overall (o/a)	99.9%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.5%

The Win95/Fono VxD was all that stood between *Data Fellows' F-Secure Anti-Virus* (*FSAV*) and another VB 100% award for the Finnish developer's trophy room. Returning results within 0.5% of perfect detection in all test-sets is certainly a laudable performance.

The differences between on-demand and on-access detection were all in the Macro test-set, with twenty fewer samples being detected on-access. These comprised two of the four A97M/AccessiV.A and all four A97M/AccessiV.B samples, plus the eleven XM/Compat.A and three of the four XM/Dado.A samples.

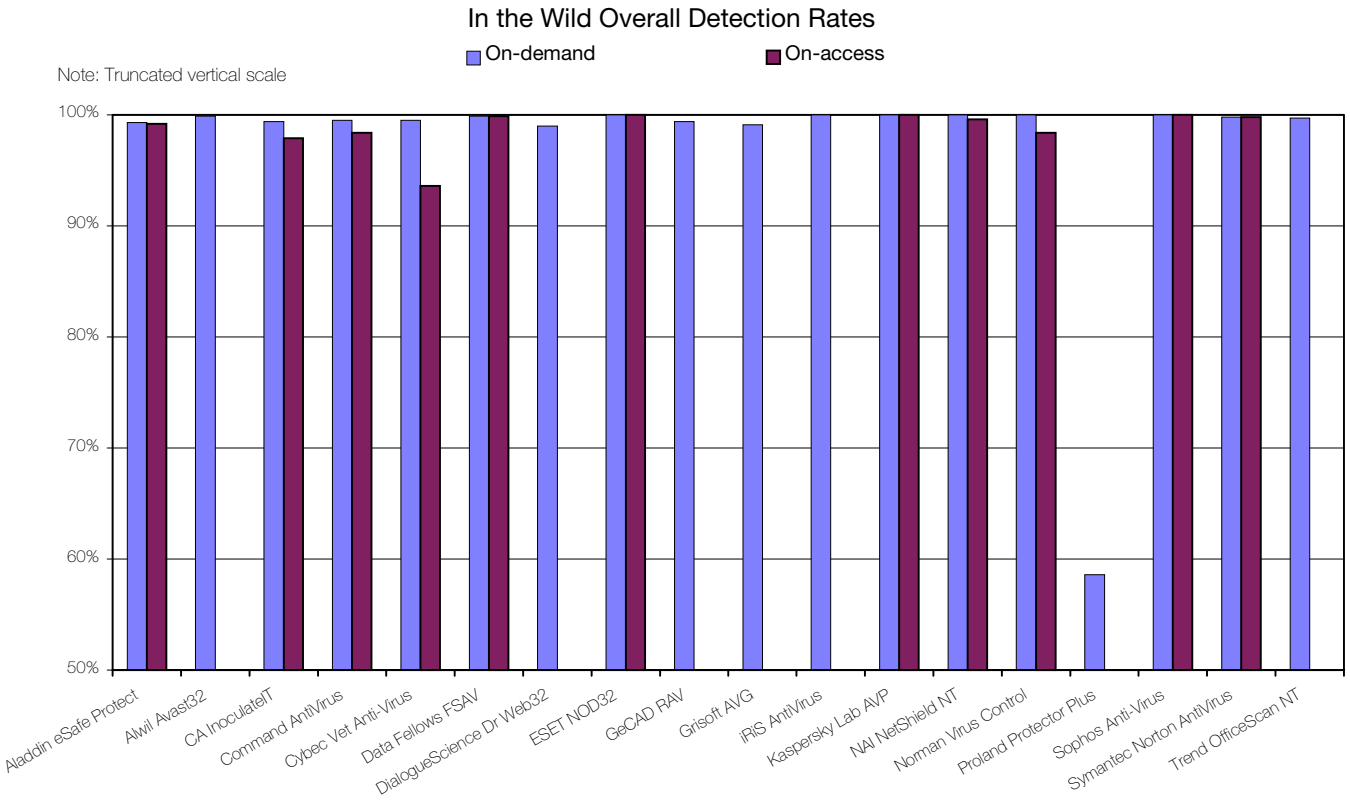
FSAV's great strength is that two good detection engines are glued together in one package, in such a way as to avoid the potential problems of running two active, independent scanners simultaneously. However, this contributes to what is, perhaps, its greatest drawback – neither of the engines it uses are renowned for their speed, so the combined effect of the two causes *FSAV* to place poorly in the speed stakes.

DialogueScience DrWeb32 v4.03aß

ItW Overall	99.0%	Macro	94.2%
ItW Overall (o/a)	n/a	Polymorphic	100.0%
ItW Boot	89.3%	Standard	99.7%

Detecting all the In the Wild File samples is a feat not matched by several of its better-known foes. Unfortunately for *DrWeb's* developers, it is not sufficient to pick up a VB 100% award either.

The scanner found nothing amiss with the diskettes holding the ItW Boot samples of viruses that have invalid BPBs (at least, invalid on the host media in *VB's* test-set – 3.5-inch DD or HD diskettes). Eight viruses that caused similar detection problems for other on-demand and/or on-access scanners were thus missed.



High detection rates were otherwise the norm. Historically the slowest scanner in *VB* reviews, performance has been sufficiently improved for this version to leave that 'honour' to *Avast32*, which as noted elsewhere, runs its scanner as a low priority thread and certainly was not as sluggish in the recent DOS comparative as it appears in those on the Win32 platforms.

ESET NOD32 v1.13

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.7%

Following an impressive debut in the DOS comparative of February 1998 and picking up a VB 100% award with its first Win32 incarnation in the May 1998 comparative, *ESET's NOD* has continued to impress. Capturing another VB 100% award here, this Slovak product detected more samples across all the test-sets than any other.

The only viruses missed were amongst the newest in the test-set – W97M/Marker.A and B, Win32/Redemption and XF/Sic.A. These were 'supplemented' under on-access testing with four rare viruses from the Standard test-set.

NOD32 was second fastest of the useful products, but surprisingly this did not translate into a very low overhead. The on-access scanner's impact on the test machine's performance was not onerous, but certainly not as slight as that of some others. No false positives were recorded.

GeCAD RAV v6.53

ItW Overall	99.4%	Macro	98.6%
ItW Overall (o/a)	n/a	Polymorphic	94.5%
ItW Boot	98.8%	Standard	96.1%

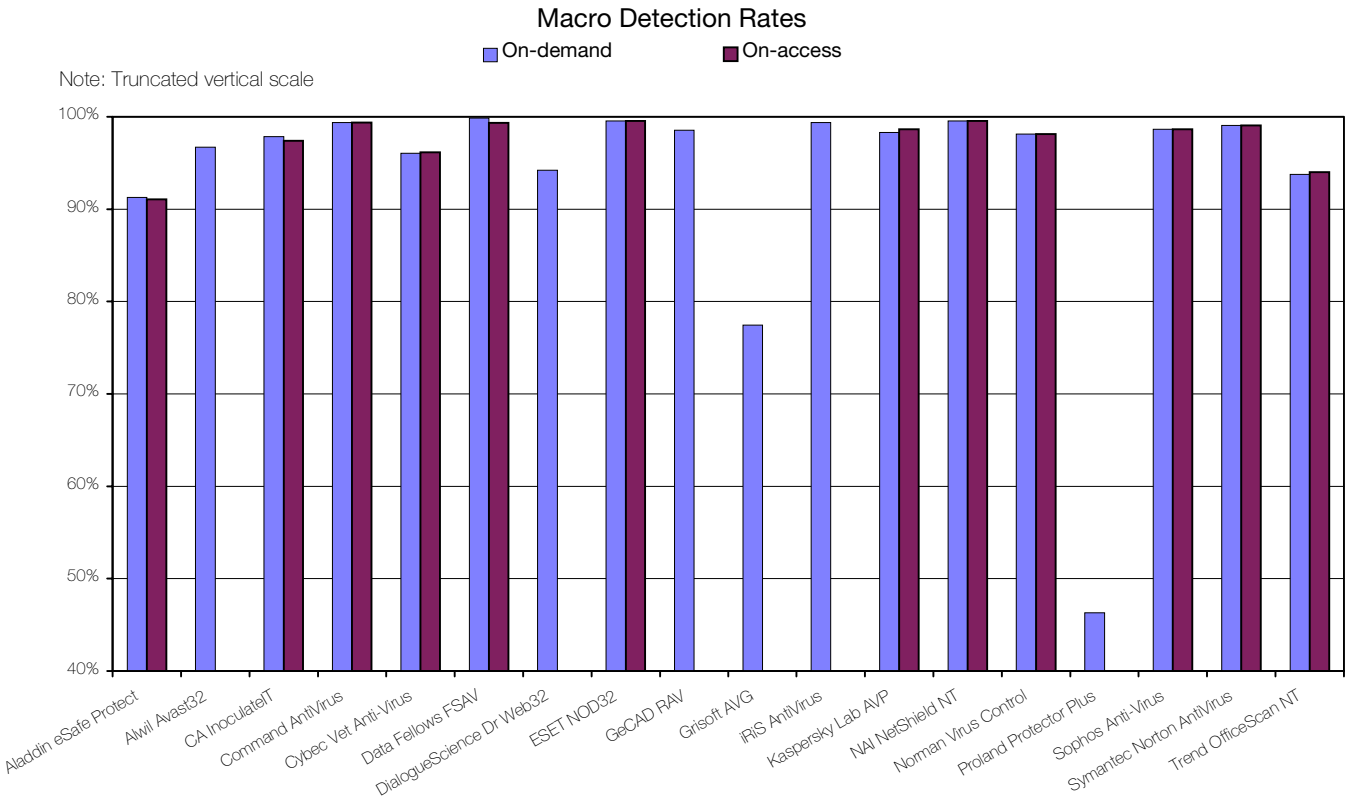
Another relative newcomer from Eastern Europe, *GeCAD's RAV* has performed well through recent comparatives. Showing steady improvement, it has not yet reached VB 100% standard but is clearly striving for it. Marburg is something of an Achilles heel for *RAV* at present – it missed all samples in the Polymorphic test-set but managed to detect five of the eighteen in the ItW File set.

Speedy it is not, but nor is it unusably slow. With some reliance on heuristics, it is not unusual that it produces a number of false-positives (eight this time). Not having an on-access component, there is little else to comment on.

Grisoft AVG v5.0 build 1238

ItW Overall	99.1%	Macro	77.4%
ItW Overall (o/a)	n/a	Polymorphic	93.3%
ItW Boot	90.5%	Standard	87.9%

Another Eastern European product striving for wider acceptance, *Grisoft's AVG* was dealt a cruel hand in the In the Wild Boot test, failing to detect any viruses on the diskettes with invalid BPBs. The only other mark against it from the ItW tests was that it missed the Win95/Fono VxD. Oddly, this version scored 5% lower on the unchanged Polymorphic test-set than the DOS version did in January.



AVG has several pre-configured scanning configurations and, as such, none is clearly the 'default' mode. All detection and speed tests in this review were run in the so-called 'Complete test' mode. This results in *Grisoft's* speed appearing slower than in previous *VB* reviews. Happily, no false positives were reported.

iRiS AntiVirus v22.16 6 Jan 1999

ItW Overall	100.0%	Macro	99.4%
ItW Overall (o/a)	n/a	Polymorphic	99.1%
ItW Boot	100.0%	Standard	99.7%

The second of the Israeli contingent in this comparative, *iRiS AntiVirus* picked up its third VB 100% award. The small handful of misses on the rest of the test-sets were due to the most recently added samples, apart from the eleven Cryptor.2782 samples missed in the Polymorphic test-set.

On the Clean test-set, *iRiS AntiVirus* returned a mid-range throughput and no false alarms. The *NT* product still does not sport an on-access component, and the user interface, whilst functional and familiar to users of earlier *Windows* versions, is starting to show its age.

Kaspersky Lab AVP v3.0.128 29 Dec 1998

ItW Overall	100.0%	Macro	98.3%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.7%

Regular readers of recent comparative reviews will not be surprised to see *AVP* from *Kaspersky Labs* achieve yet another VB 100% award. The detection levels against the non-ItW test-sets should not be surprising either.

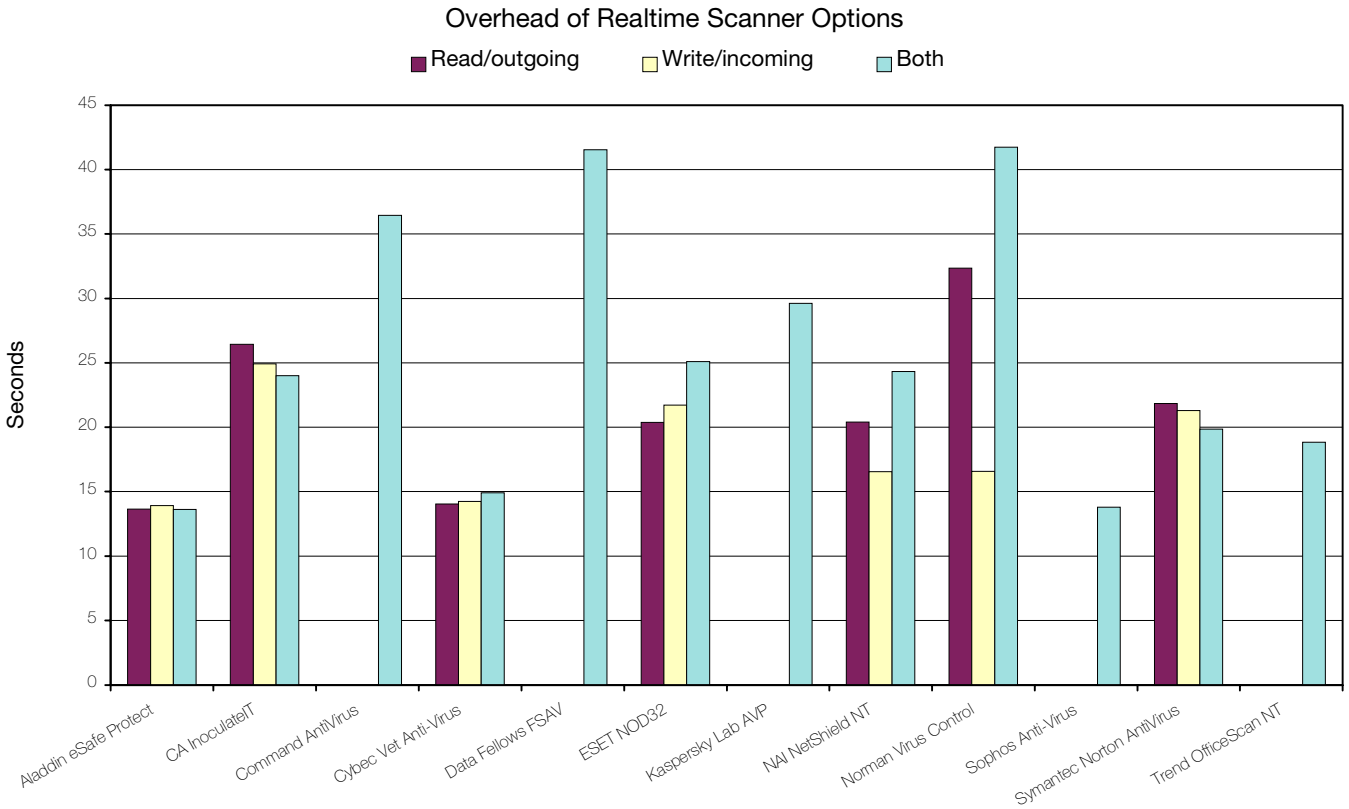
What *is* surprising, perhaps, was that a slightly greater number of macro viruses were detected on-access than on-demand. Throughput of the Clean test-set is at the top end of a large group of middling performances and overhead approached 100%, which may sound daunting but was certainly not the highest recorded.

NAI NetShield NT v4.0.2.4008

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	99.6%	Polymorphic	96.7%
ItW Boot	100.0%	Standard	99.7%

This is the first showing of an *NT* product from *NAI* powered by the *Dr Solomon's* engine. Characteristic of the high detection rates of that engine in its former incarnation, a VB 100% performance was returned against the ItW Overall test-set.

Interestingly, the screen savers (SCR files) infected with Win95/Marburg and TPVO.3783.A, which were troublesome to some other products, were detected on-demand, but not on-access. Failure to check SCR files by default, thus missing a large chunk of the Marburg samples therein, also explains much of the uncharacteristically low score against the Polymorphic test-set. The other 'problem' *NetShield*



faced in that test-set was with W97M/Splash.A. This virus' practice of morphing its code by inserting ever more random comments into itself has been noted in previous reviews as causing trouble for several products.

NetShield's traditionally very slow speed has been improved markedly by the change of engine. Given this, it should not be surprising that its high overhead has reduced commensurately. There were no false alarms.

Norman Virus Control

ItW Overall	100.0%	Macro	98.1%
ItW Overall (o/a)	98.4%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.7%

Another product with an all but unbroken string of VB 100% awards, *Norman Virus Control* (*NVC*), provided a typically staunch, Scandanavian showing. The gloss of its VB 100% award was slightly tarnished by its on-access component ignoring SCR and VxD files, thereby failing to detect TPVO.3783.A and Win95/Marburg in several of the former and one sample of Win95/Fono in the latter.

Testing on-access detection was complicated slightly because, as with *CA's InoculateIT*, *NVC* only has detect on read and/or write operations. This was simply resolved by copying the test-set from the server, scanning on file writes and deleting infected files. Also as with *InoculateIT*, detection in this mode was not as thorough as on-demand and repeat testing led to further detections. This took several iterations to converge on three successive runs with no further detections occurring, but performance was still lower than in the on-demand case.

NVC's mid-range throughput on the speed test is not a reliable guide to its overhead. Oddly, its overhead is significantly lower when only intercepting write operations than in other modes. No false positives were recorded.

Proland Protector Plus

ItW Overall	58.6%	Macro	46.3%
ItW Overall (o/a)	n/a	Polymorphic	10.7%
ItW Boot	57.1%	Standard	54.1%

Indian *Protector Plus* was the newest entrant to *VB's* comparatives in the previous *NT* scanner round-up in September 1998. The current performance represents an improvement of 20–25% over that first showing.

The 'on-line scanner' seemed to be more of a scheduler for the on-demand scanner. More could not be decided however, as the initial scan that starts immediately on enabling this component always caused Dr Watson to object in its strongest terms, stopping the service.

As in the previous *NT* comparative, *Protector Plus* blitzed the field in the speed tests. Outpacing *Vet* by more than 25% would be the envy of most anti-virus developers, but coupled with this product's detection rate, such speed provides little comfort. Add the 61 false-positives against the Clean test-set and the formula is even more lopsided.

With lower than 50% detection of macro viruses (presumably benefiting from its default 'detect suspicious macros' option) and clear stability problems, this is a product with quite some maturing ahead of it.

Sophos Anti-Virus v3.17

ItW Overall	100.0%	Macro	98.6%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.2%

Another regular recipient of VB 100% awards, *Sophos Anti-Virus* (*SAV*) was not to disappoint on this outing. As with several other products, the relative stasis of the non-ItW test-sets since the major update prior to the January DOS comparative has allowed *SAV* to catch up to its more typical performance on those tests. The viruses missed were the very newest added to the test-sets, plus Positron which SAV only detects in 'full scan' mode.

On-access and on-demand detection was identical – as alluded to earlier, something of a rare occurrence. *SAV's* speed is quite respectable on NT, resulting in a throughput of almost 2500 KB/s – a result that is somewhat anomalous with *SAV's* speed on other platforms.

Symantec Norton AntiVirus v5.01.01

ItW Overall	99.8%	Macro	99.1%
ItW Overall (o/a)	99.8%	Polymorphic	98.7%
ItW Boot	98.8%	Standard	99.5%

As with several other recent top-performers, *NAV's* run at another VB 100% award fell foul of Fono. *NAV* detected the EXE samples of this virus but missed its VxD and a Fono-infected diskette boot sector. Aside from this, *NAV* detected all but one or two viruses in each of the other test-sets. It still misses a single EXE sample of Marburg in the Polymorphic test-set. The product's results were the same under both on-access and on-demand conditions.

Returning a throughput rate a little over 1000 KB/s placed *NAV's* speed solidly in the middle of the pack. No false positives were reported.

Trend OfficeScan NT 98.5 VPN 489

ItW Overall	99.7%	Macro	93.8%
ItW Overall (o/a)	n/a	Polymorphic	96.8%
ItW Boot	97.6%	Standard	98.7%

The first showing of *Trend's OfficeScan* in a *VB* review shows the promised improvement in detection rates and speed seem to have been realized. It will take time to tell if the product's stability has improved, though it reported two false alarms. VB 100% status was denied by Fono's VxD and boot sector forms, and the ancient V-Sign boot virus.

OfficeScan provides no on-access boot sector scanning, save at shut-down – a feature that all products should provide. Given *NT's* legendary shut-down and restart speed, running the on-access Boot test via this mechanism was not even considered an option.

Following in the footsteps of *InoculateIT* and *NVC*, testing on-access detection of the viruses in the file-based test-sets with *OfficeScan* required copying the test-sets from the server to a local disk. This was required for a different reason from that of those products. *OfficeScan* adamantly refused to intercept file I/O requests involving remote files. This is an intriguing way to require your users to install your product on both servers and workstations. This philosophy of ignoring network file sources extends throughout the workstation product, with network drives never appearing in selection lists and the like. Oddly, however, the context menu in Explorer lists *OfficeScan* as an option for network drives and folders, and *OfficeScan* happily obliges by scanning the selected object.

As a beta version was submitted for testing, it may seem churlish to point out stability issues, but some things should be 'too obvious'. For example, *OfficeScan* adds an option to scan a drive or folder to the context menus in Explorer. This consistently disappeared following the first reboot after installation, thus removing the only available method of scanning the test-sets stored on the server.

Conclusion

Several products missed small numbers of *Excel* macro viruses because they do not look at a wide enough range of file extensions. The extension XL? is a highly recommended one to add to default extension lists, if the product supports wildcards in that list. If it does not, then users have to pray the developer is keeping up with the state of play or be very alert themselves. These results suggest some are not. There are related issues with SCR and VxD files.

A surprising observation was that some products do not provide a 'deny access' action for infected objects. A product that leaves system administrators trusting that their users will 'do the right thing' when warned of a virus, seems unduly optimistic to me.

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 NT v4.0 (SP4)*. 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 for the duration of 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/NT/199903/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.c om/Comparatives/Win95/199801/protocol.html.