COMPARATIVE REVIEW

Unpacking a Punch

The *VB* Comparative bandwagon moves on to *Windows NT* (workstation) this month, seven months having passed since we last looked at this platform.

Fifteen products were submitted for review. There is the usual collection of names, the only noticeable absentees being products from *Trend Micro Inc* and *Panda Software*.

Detection Rate Tests

Unsurprisingly, the customary *VB* test-sets were used for the detection tests (Polymorphic, Standard, Macro and In the Wild) with the In the Wild (ItW) set aligned to the January 2000 WildList. The product submission deadline was 31 January 2000.

A fifth test-set was constructed from the ItW set – each sample was individually compressed, and the archive copied into its own directory. Nested archives containing each of these individual archives were also created. Both PKZIP and ARJ compression methods were used, thus creating six tests:

1. Samples individually ARJ'ed.
2. Samples individually ZIP'ed.
3. Contents of set 1, compressed within a single ARJ.
4. Contents of set 1, compressed within a single ZIP.
5. Contents of set 2, compressed within a single ARJ.
6. Contents of set 2, compressed within a single ZIP.

Detection of the ItW samples within each of these six sets was measured during on-demand scanning, and, for those products that supported it, on-access scanning. For simplicity, within this review these results are expressed as number of missed samples and simple 'detected' percentages, as opposed to the more familiar normalized percentages.

The ability of each product to handle various types of file archives was also reviewed. For this a small set of files based on the *EICAR* test-file was used.

Complete detection rate results are provided within the large tables and a summary is presented beneath each product heading. A complete list of the samples used in each of the test-sets can be found at the URL detailed at the end of this review.

Performance Tests

The usual speed tests were performed – that is, on-demand scanning speeds returned against executable and OLE2 file scanning. Additionally, and in keeping with the emphasis upon archive handling in this review, the on-demand scanning speeds against archived executables and OLE2 files were also measured.

The scanning speed tests double up as false positive tests, and for the first time in *VB* Comparative Reviews, the criterion of 'no false positives' is added to the VB100% award. This includes only 'full' false positives, and not files flagged as 'suspicious'. To complement the scanning speed tests, the overhead of each of the on-access scanners has also been assessed. The usual process of measuring the time taken for a set of files to be copied between directories on a local drive was performed. A single machine (disconnected from the network) was used for all such tests. The results are provided within this review relative to a common baseline (with no on-access scanning) of 15 seconds.

Similar tests were performed to measure the overhead of scanning file archives for products that supported such a facility. Most of the products were designed not to support on-access archive handling, due to the large impact it can have upon performance. On-access archive handling results are presented as percentages of the baseline times measured without any real-time scanner active.

Aladdin eSafe Desktop v2.2 (31/01/2000)

ItW File	98.1%	Macro	91.9%
ItW File (o/a)	98.0%	Standard	95.3%
ItW Overall (o/d)	98.2%	Polymorphic	86.4%

A lot of anti-virus products adopt very similar user interfaces and one can step from one to the next with relative ease. Not so *eSafe Desktop* from *Aladdin Knowledge Systems* – familiarity with the rather individual interface is extremely helpful.

The detection rates observed were slightly disappointing, perhaps not living up to the claim of 'You are now free to connect and surf the Internet without fear of virus and vandal attacks' presented during installation. Ignoring the results against the Standard, Macro and Polymorphic sets, *eSafe* should have coped better with the ItW set, from which 21 samples were missed (including Win32/Oporto, the polymorphic W97M/Ded.A and a couple of the variants of VBS/Freelinks).

eSafe handles a good selection of archive formats but, unfortunately, does not fully support nested archives – it only detects the first infected file within a nested archive

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /2000/$0.00+2.50**

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Missed	%	Missed	%	%	Missed	%	Missed	%	Missed	%
Aladdin eSafe Desktop	0	100.0%	21	98.1%	98.2%	299	91.9%	273	86.4%	73	95.3%
Alwil AVAST32	0	100.0%	8	98.3%	98.4%	128	96.3%	98	89.1%	32	95.7%
CA InoculateIT	0	100.0%	0	100.0%	100.0%	1	99.9%	17	97.8%	5	98.9%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	30	99.2%	265	94.4%	7	98.5%
DialogueScience DrWeb	0	100.0%	0	100.0%	100.0%	25	99.2%	0	100.0%	17	97.3%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	2	99.5%	7	98.5%
F-Secure Anti-Virus	0	100.0%	0	100.0%	100.0%	0	100.0%	0	100.0%	4	99.1%
GeCAD RAV	0	100.0%	2	99.8%	99.8%	24	99.3%	17	97.8%	13	98.0%
Grisoft AVG	0	100.0%	14	97.3%	97.4%	49	98.6%	124	91.8%	42	97.3%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	8	99.7%	0	100.0%	1	99.8%
NAI VirusScan	0	100.0%	10	98.1%	98.2%	19	99.6%	17	97.8%	17	97.3%
Norman Virus Control	0	100.0%	0	100.0%	100.0%	6	99.7%	289	90.7%	4	99.1%
SoftWin AntiVirus eXpert	1	96.4%	50	95.3%	95.5%	66	98.1%	1573	82.7%	189	89.0%
Sophos Anti-Virus	0	100.0%	0	100.0%	100.0%	82	97.6%	191	95.1%	24	97.8%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	54	98.4%	265	94.2%	5	98.9%

and therefore scored poorly on the archived ItW sample tests. Detection of the individually archived (ARJ and ZIP) samples was as for the uncompressed, with 21 samples being missed.

Data for the speed tests is incomplete due to the fact that *eSafe* consistently hung the test machine whilst scanning a number of executables in the Clean sets. Consultation with the developers identified this problem to be due to a recently discovered bug.

Alwil AVAST32 v3.0.219 (31/01/2000)

ItW File	98.3%	Macro	96.3%
ItW File (o/a)	99.7%	Standard	95.7%
ItW Overall (o/d)	98.4%	Polymorphic	89.1%

Despite sporting a somewhat updated interface from that seen in previous incarnations (though still bearing the cartoon mouse), *AVAST32* was the same as ever to test. Previously, it has skirted close to earning a VB100% award but failure to scan a variety of file types resulted in samples infected with Win95/Babylonia, VBS/Freelinks and VBS/BubbleBoy kept the award at bay once more.

On-access detection was measured by setting *AVAST32* to scan on file writes, and then using XCOPY to copy the test-set to a local drive. Detection rates were higher than those observed on-demand, predominantly because the product defaults to include 'All Files'. As observed in previous Comparatives, a couple of samples infected with the 1003- and 1019-byte variants of Win95/CIH were missed from the ItW set during on-access scanning.

Speedwise, *AVAST32* sits at the slightly slower end of the range exhibited by the other products. Sadly, a false positive was registered in the Clean set, a file unjustly being reported as infected with Tequila.2468.

The ARJ compression format was not handled by the product submitted, neither were nested archives. Both these factors caused poor overall figures in the archived ItW set. Eight infected samples were missed from the set of individually zipped samples – Set 1 – the same as were missed during the regular ItW tests. This was thanks to the omission of certain file types from the default extension list.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.0%	22	98.0%	98.1%	299	91.9%	273	86.4%	73	95.3%
Alwil AVAST32	3	89.2%	3	99.7%	99.3%	128	96.3%	98	89.1%	32	96.0%
CA InoculateIT	3	89.2%	0	100.0%	99.5%	1	99.9%	17	97.8%	5	98.9%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	30	99.2%	765	91.7%	10	98.3%
DialogueScience DrWeb	n/t	n/t	3	99.8%	n/a	43	98.8%	0	100.0%	14	97.4%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	1	99.61%	7	98.5%
F-Secure Anti-Virus	0	100.0%	0	100.0%	100.0%	1	99.9%	0	100.0%	4	99.1%
GeCAD RAV	n/a	n/a	2	99.8%	n/a	24	99.3%	17	97.8%	13	98.0%
Grisoft AVG	0	100.0%	15	97.8%	97.9%	55	98.5%	292	89.1%	59	95.7%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	8	99.7%	0	100.0%	1	99.8%
NAI VirusScan	0	100.0%	1	99.9%	99.9%	19	99.6%	17	97.8%	1	99.8%
Norman Virus Control	3	89.2%	0	100.0%	99.5%	6	99.7%	288	90.7%	4	99.1%
Sophos Anti-Virus	0	100.0%	0	100.0%	100.0%	82	97.6%	191	95.1%	24	97.8%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	54	98.4%	265	94.2%	12	97.9%

CA InoculateIT v4.53 (28/01/2000)

ItW File	100.0%	Macro	99.9%
ItW File (o/a)	100.0%	Standard	98.9%
ItW Overall (o/d)	100.0%	Polymorphic	97.8%

Complete on-demand and on-access ItW file coupled with no false positives in the Clean set was not enough to earn the first *Computer Associates'* (*CA*) offering, *InoculateIT*, another VB 100% award. Unfortunately, failure to detect infected boot sectors with invalid BPBs was to blame – a fact that has been reported in previous Comparatives.

Earlier reviews have commented upon the slight instability of the on-access scanner. Thankfully, such worries seem unnecessary now – *InoculateIT* behaved impeccably throughout testing. The detection rates measured for on-access scanning mirrored those on-demand, with only 25 samples missed across all the test-sets. The bulk of these misses were due to the complex polymorphic virus Win95/SK.8044. Other than this, a number of VBS viruses were missed, including VBS/Fool and VBS/Tune.B. A single document template infected with Iseng.A was missed in the Macro set.

The speed and overhead tests reveal *InoculateIT* to be no slouch in the engine department. Scanning speeds of well over 1500 KB/s were registered for both executable and OLE2 file scanning.

On-demand detection in the archived ItW set was perfect – all of the 712 samples within each of the six sets were detected. Following on from *AVAST32*, *InoculateIT* is another product which supports the on-access scanning of archives. In keeping with the fast on-demand archive scanning, the overhead of on-access archive scanning was approximately 150% – the smallest observed out of the five products providing such a facility.

CA Vet Anti-Virus v10.1.7.1 (31/01/2000)

ItW File	100.0%	Macro	99.2%
ItW File (o/a)	100.0%	Standard	98.5%
ItW Overall (o/d)	100.0%	Polymorphic	94.4%

Striding ahead of its *InoculateIT* stablemate, *Vet Anti-Virus*, the second of *CA's* products, provides another excellent performance earning its fourth successive VB 100% award. Its high ItW detection was matched in the archived ItW set, where *Vet Anti-Virus* managed to detect all of the infected samples in each of the six sets.

Product	File formats handled (on-demand scanner)										Nested archives?	O/A archive handling?
	ZIP	ARJ	GZIP	RAR	LZH	TAR	LHA	UUE	MIME	CAB		
Aladdin eSafe Desktop	●	●	●		●	●	●				No	No
Alwil AVAST32	●							●	●		No	Yes
CA InoculateIT	●	●	●		●	●	●	●	●		Yes	Yes
CA Vet Anti-Virus	●	●	●		●			●	●	●	Yes	No
DialogueScience DrWeb	●	●		●							Yes	Yes
Eset NOD32	●	●		●							Yes	No
F-Secure Anti-Virus	●	●	●	●	●	●	●	●	●	●	Yes	Yes
GeCAD RAV	●	●	●				●				No	No
Grisoft AVG	●	●		●							Yes	No
Kaspersky Lab AVP	●	●	●	●	●	●		●	●	●	Yes	Yes
NAI VirusScan	●									●	No	No
Norman Virus Control	●	●			●						Yes	No
SoftWin AntiVirus eXpert	●	●			●		●				Yes	No
Sophos Anti-Virus	●	●	●	●		●					Yes	No
Symantec Norton AntiVirus	●	●			●		●			●	Yes	No

Samples of Win95/WinExt.A and Win32/NewApt.F accounted for some of the misses in the Standard set. *Vet* still fails to detect the polymorphic XM/Soldier.A, along with a variety of other samples in the Macro set, including both W97M/Opey.U and W97M/Thus.G. Once again, failure to detect the A and B variants of ACG contributes to a slightly lower percentage against the Polymorphic set. All 500 samples of Baran.4968 were missed from this set during on-access scanning.

DialogueScience DrWeb v4.16 (31/01/2000)

ItW File	100.0%	Macro	99.2%
ItW File (o/a)	99.8%	Standard	97.3%
ItW Overall (o/d)	100.0%	Polymorphic	100.0%

Despite achieving complete on-demand ItW file and boot detection, *DialogueScience's DrWeb* does not earn another VB 100% award thanks to missing three *PowerPoint* files infected with the C variant of O97M/Tristate, and registering a false positive in the Clean set. The on-access component of *DrWeb*, *SpiDer Guard*, treats *PowerPoint* files as archives. By default, archives are unpacked during on-demand scanning, but not during on-access scanning, which explains why the *PowerPoint* files remained undetected. Elsewhere, the misses were predominantly due to recently introduced samples. Additionally, it was not possible to verify boot infections with *SpiDer Guard* – access to infected floppies was not denied, and no on-screen warning messages were observed. Thus on-access detection of the ItW boot samples has not been measured. Hopefully, the situation will be resolved before the next Comparative.

Though not handling a great number of archive formats, *DrWeb* coped successfully with the ZIP and ARJ files presented to it in the archived ItW test-set. It detected all of the archived ItW samples in each of the six sets.

Performance tests showed *DrWeb* returning moderate scan rates in keeping with the bulk of products. More noticeable was the on-access scanning overhead which was fairly high for both uncompressed and compressed file scanning – the latter resulting in an overhead of over 2000%, significantly larger than that for the other four products.

Eset NOD32 v1.13 (31/01/2000)

ItW File	100.0%	Macro	99.8%
ItW File (o/a)	100.0%	Standard	98.5%
ItW Overall (o/d)	100.0%	Polymorphic	99.5%

In picking up another VB 100% award in this Comparative, *NOD32* maintains its record of receiving the VB 100% in each test to which the product has been submitted. On-demand and on-access detection differed by only one sample – a single sample (from the 500 in the test-set) of the polymorphic

	Hard Disk Scanning Speed									
	Executables			OLE2 files			Zipped Executables		Zipped OLE2	
	Time (min:sec)	Throughput (kB/s)	FPs [susp]	Time (min:sec)	Throughput (kB/s)	FPs [susp]	Time (min:sec)	Throughput (kB/s)	Time (min:sec)	Throughput (kB/s)
Aladdin eSafe Desktop	n/t	n/t	n/t	1:08	1166.7	0	n/t	n/t	1:34	793.7
Alwil AVAST32	11:00	828.7	1	3:54	339.0	0	5:58	445.3	3:54	318.8
CA InoculateIT	4:24	1925.8	0	0:30	2644.5	0	3:06	857.1	0:41	1819.7
CA Vet Anti-Virus	8:45	1041.8	0	0:46	1724.6	0	4:56	538.6	1:23	898.9
DialogueScience DrWeb	18:59	480.2	1+[17]	0:51	1555.6	[1]	8:35	309.5	1:06	1130.4
Eset NOD32	2:27	3720.6	0	0:21	3777.8	0	2:54	916.2	0:48	1554.3
F-Secure Anti-Virus	17:44	514.0	0	3:35	369.0	0	2:16	1172.2	0:27	2763.2
GeCAD RAV	24:01	379.6	1+[1]	0:58	1367.8	0	11:09	238.3	1:00	1243.5
Grisoft AVG	10:24	876.5	7+[2]	0:18	4175.5	0	5:28	486.0	0:57	1311.2
Kaspersky Lab AVP	6:03	1506.7	[2]	1:13	1086.8	0	4:53	544.1	1:43	724.3
NAI VirusScan	3:58	2298.0	0	0:36	2203.7	0	7:57	334.2	1:42	731.4
Norman Virus Control	4:54	1860.3	0	0:52	1525.6	0	40:16	66.0	7:12	172.7
SoftWin AntiVirus eXpert	20:55	435.8	28+[64]	0:51	1555.6	[18]	8:04	329.4	0:56	1332.3
Sophos Anti-Virus	4:27	2048.4	0	1:20	991.7	0	3:04	866.4	1:21	921.1
Symantec Norton AntiVirus	10:01	910.0	0	0:58	1367.8	0	5:20	498.2	1:02	1203.3

W97M/Splash.A was missed during on-demand scanning. The remainder of the misses were partly attributable to JS/Kak.A, W97M/Garb.A, variants of VBS/Tune, and the Win95/WinExt.A worm.

NOD32 displayed the highest overall on-demand scanning rates, returning throughputs of over 3500 KB/s for both executable and OLE2 file scanning. Archive scanning was a little more moderate, but still faster than the average observed across all the products. All of the samples within sets 1 and 2 of the archived ItW test-set were detected. Unfortunately, only the first nine samples within each of the nested archives (sets 3 to 6) were detected, thus causing a fairly poor overall score against this test-set.

F-Secure Anti-Virus v5.02.5528 (27/01/2000)

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

F-Secure Anti-Virus (*FSAV*) has undergone something of a makeover since its last appearance in a *VB* Comparative. A quick glance at the results shows that the high detection rates associated with this product still remain. Only four samples, all from the Standard set, were missed across all of the test-sets – these were VBS/Tune.B, VBS/Fool and the E and F variants of Win32/NewApt.

If high detection rates have come to be associated with *FSAV*, then so has a degree of sluggishness, owing to the use of two engines (*AVP* and *F-Prot*). Though not the slowest scanner, *FSAV* was at the slower end of the pack. Interestingly, *FSAV* is the only product to return greater throughputs (almost twice as large) for archive file scanning compared to non-compressed file scanning.

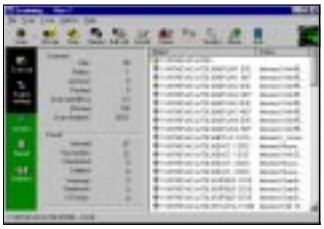
Scanning logs are now generated in HTML, with a hyperlink to the *F-Secure* on-line virus description library for each reported infection. Though a nice feature for users, setting *FSAV* to scan a large virus collection resulted in various 'out of

memory' errors, and no scanning log was produced whatsoever. The test-sets were scanned individually therefore, and a separate log for each was thus generated successfully.

FSAV handles an impressive array of archive formats, and provides the option to enable real-time archive scanning if so desired. During on-demand scanning of the archived ItW set, all of the individually compressed samples were detected (sets 1 and 2), but four compressed (ZIP or ARJ) HLP files infected with Win95/Babylonia.A were missed from each of the nested archives (sets 3 to 6). The same samples were also missed during real-time scanning of the archived ItW set, and a single Babylonia.A-infected executable was also missed from all of the sets.

GeCAD RAV v7.6.360 (30/01/2000)

ItW File	99.8%	Macro	99.3%
ItW File (o/a)	99.8%	Standard	98.0%
ItW Overall (o/d)	99.8%	Polymorphic	97.8%



After a couple of VB 100%-worthy performances in the latter half of 1999, *GeCAD's Romanian Anti-Virus* (*RAV*) puts in another strong performance this time around. Not strong enough for a VB 100% award, however, thanks to missing an OCX (ActiveX control) file infected with the recently seen Win32/Funlove and a VxD infected with the polymorphic Win95/Fono. Furthermore, on-access ItW boot sample detection rates could not be measured since *RAV Monitor* provided no such facility in the submitted product.

RAV's main weakness, when presented with the archived ItW set, was its inability to cope with nested archives. Accordingly, none of the archived samples compressed within the single ZIP or ARJ archive in sets 3 to 6 were detected. Detection of the individually archived samples was achieved: the same two samples as were missed in the conventional detection tests were missed in set 1 (ARJ compression used). Against set 2 (containing individually zipped samples), in addition to these two samples, a handful of others were also missed.

Grisoft AVG v6.0.116 (31/01/2000)

ItW File	97.3%	Macro	98.6%
ItW File (o/a)	97.8%	Standard	97.3%
ItW Overall (o/d)	97.4%	Polymorphic	91.8%

The detection rates observed for *AVG* appear a little lower than those observed in recent Comparatives. Most obvious was the failure to detect a series of ItW viruses – namely Win32/Oporto, the destructive Win32/Kriz.4029, VBS/BubbleBoy and the JO variant of XM/Laroux. A number of samples were missed elsewhere in the test-sets, the performance being poorest in the Polymorphic set where samples infected with ACG.B, Win95/SK.8044 and Win95/SK.7972 were missed.

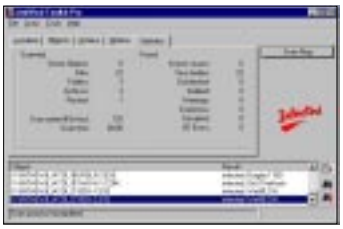
AVG performed identically with each of the sets within the archived ItW test-set – the same samples were missed in each as were missed in the regular (non-compressed) test-sets.

Traditionally fairly anonymous in the performance tests, it was surprising to observe *AVG* reproducibly returning very high throughputs during OLE2 file scanning. Sadly, a number of false positives were registered during scanning of the Clean set, caused by the overkeen heuristics. The overhead of the relatively recently introduced on-access scanner was in keeping with the bulk of other products.

Kaspersky Lab AVP v3.0.132.4 (29/01/2000)

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

Three viruses account for all the samples missed by *Kaspersky Lab's AVP Platinum* tested in this review. The misses were W97M/Opey.U, the potentially destructive W97M/Thus.G from the Macro set and VBS/Tune.B from the Standard set.

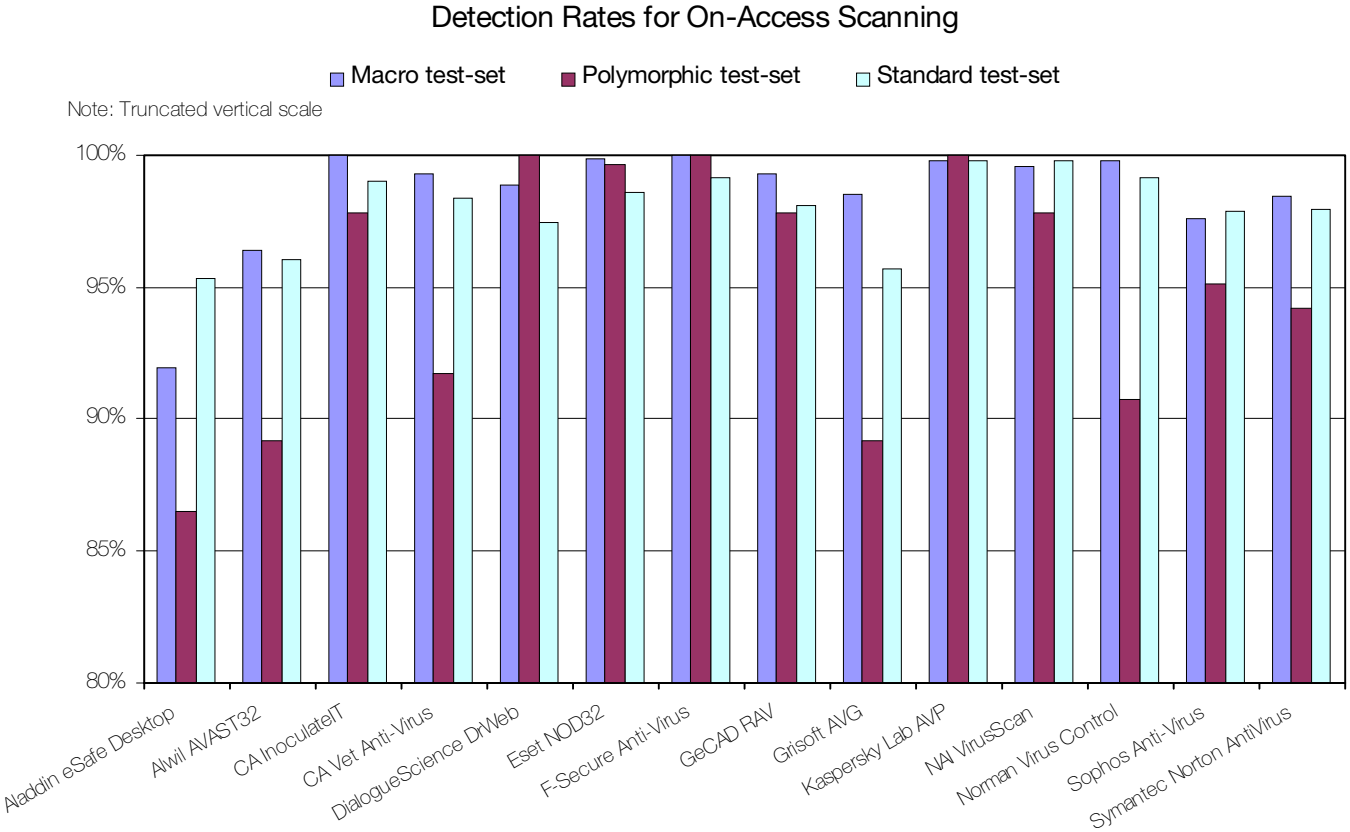


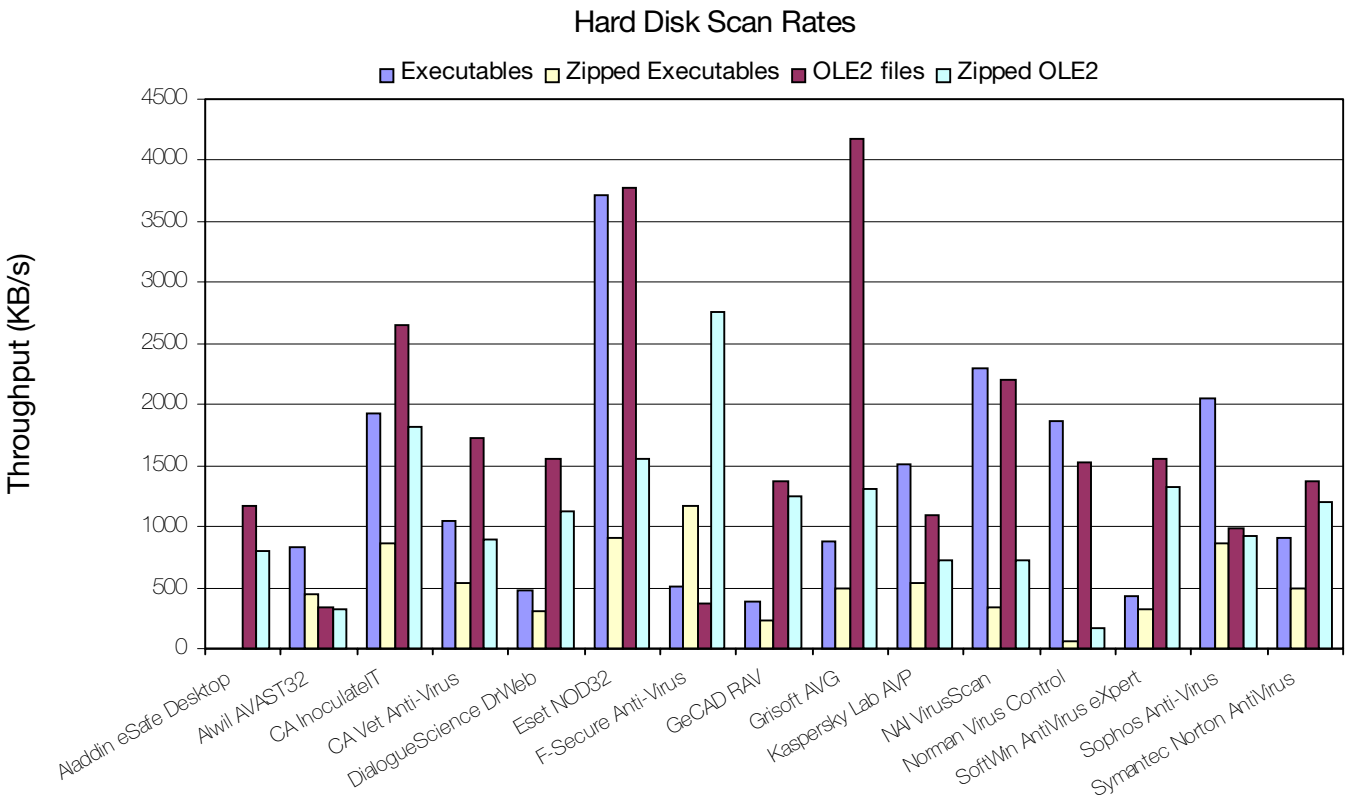
Complete ItW file detection was maintained when *AVP* was pointed to the archived ItW set, with all samples being detected across each of the 6 sets during both on-demand and on-access scanning. As can be seen, the overhead of on-access archive scanning was fairly large (as might be expected, hence the exclusion of such a facility in the majority of the products) at just over 1200%.

NAI VirusScan v4.0.3a.4062 (26/01/2000)

ItW File	98.1%	Macro	99.6%
ItW File (o/a)	99.9%	Standard	97.3%
ItW Overall (o/d)	98.2%	Polymorphic	97.8%

Compared to recent performances by *VirusScan*, the detection rates presented here are slightly disappointing. This was due mainly to the product failing to scan sufficient file types in its default configuration. VBS, HLP and OCX files (among others) were skipped, thus causing a variety of misses to be registered across the test-sets. These misses included samples of VBS/Freelinks, Win95/Babylonia.A, and Win32/FunLove from the ItW set, keeping the VB 100% award at bay. The submitted version of *VirusScan* only supported the ZIP archive format, and did not scan within nested file archives. Only set 2 in the archived ItW





test-set yielded any detections therefore, the only misses mirroring those listed above for the regular (non-compressed) ItW tests.

Speedwise, *VirusScan* returned high throughputs for both executable and OLE2 file scanning, and the overhead of the on-access was in line with that of the other products. No false positives were recorded against the Clean sets.

Norman Virus Control v4.73 (28/01/2000)

ItW File	100.0%	Macro	99.7%
ItW File (o/a)	100.0%	Standard	99.1%
ItW Overall (o/d)	100.0%	Polymorphic	90.7%

Norman Virus Control (*NVC*) puts in another strong performance, but failing to detect three boot sectors infected with ItW viruses (those with invalid BPBs) prevents it from picking up its fourth successive VB 100% award. The weakest area of detection was observed in the Polymorphic set, owing to samples infected with the A and B variants of ACG, Win95/SK.8044 and Win95/SK.7972 being missed.

NVC returned fairly fast scanning speeds against the executable and OLE2 file sets, but slowed down dramatically when scanning the same files zipped. When faced with the archived ItW set, *NVC* ploughed though the individually archived samples, detecting all of the samples (sets 1 and 2) successfully. A large number of the samples were missed in the nested archive sets – only 547 samples were detected in sets 3 to 6.

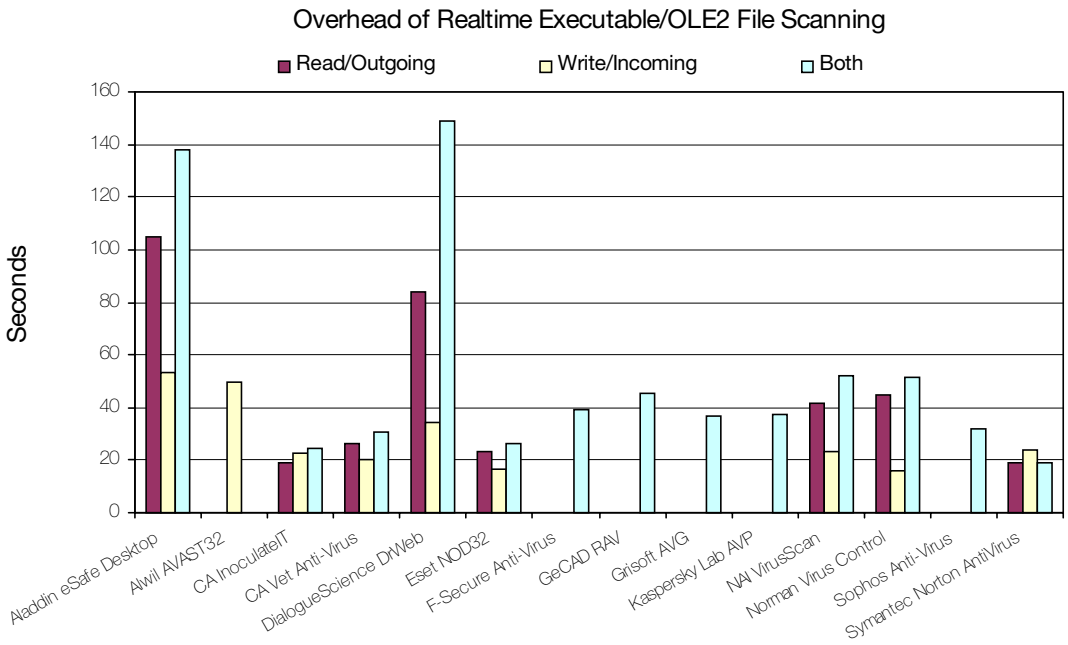
SoftWin AntiVirus eXpert (31/01/2000)

ItW File	95.3%	Macro	98.1%
ItW File (o/a)	n/t	Standard	89.0%
ItW Overall (o/d)	95.5%	Polymorphic	82.7%

A new face in the *VB* Comparative crowd, and the second product from Romania, is *AntiVirus eXpert* (*AVX*) from *SoftWin*. As expected given its virgin status, *AVX* missed a number of samples across the test-sets.

Unfortunately, on-access detection rates have not been measured because, due to a bug, the *AVX* on-access scanner failed to block access to infected files. Hopefully, the on-access component of *AVX* product versions submitted to *VB* future Comparatives can be reviewed as normal.

Whereas low detection might not be a surprise against the Standard, Macro and Polymorphic test sets, a slightly higher percentage might have been expected against the ItW set. Sadly, a number of viruses were missed here, including Win95/Babylonia.A, Win32/Oporto, TMC_Level-69, Win95/Fono, X97M/Manalo.E and X97M/PTH.D, to name but a few.



AVX worked its way happily through the archived ItW test-set, detecting 663 samples in each of the six sets, the missed samples mirroring those missed during the above tests.

In terms of performance, only the on-demand scanning speed of *AVX* has been assessed due to the aforementioned bug. Scanning speeds of approximately 450 and 1550 KB/s were returned for executable and OLE2 file scanning respectively. The throughputs dropped only slightly to just over 300 and 1300 KB/s for scanning of the zipped files.

It will be interesting to see how *AVX* measures up in subsequent reviews – one would predict a significant increase in the detection rates, which, if realised, would certainly make *AVX* a competitive product in the *VB* Comparative product arena.

Sophos Anti-Virus v3.30 (01/02/2000)

ItW File	100.0%	Macro	97.6%
ItW File (o/a)	100.0%	Standard	97.8%
ItW Overall (o/d)	100.0%	Polymorphic	95.1%

Complete on-demand and on-access ItW file and boot detection coupled with no false positives in the Clean set earns *Sophos Anti-Virus* (*SAV*) its tenth VB 100% award.

SAV missed its traditional sprinkling of viruses, a proportion of which are detected if the 'full' scanning mode is enabled, as opposed to the default 'quick' mode. New misses included samples infected with W97M/Divi.B, X97M/Weit.A, the F and G variants of W97M/Verlor, PE samples infected with Win98/Caw.1416, the E and F variants of Win32/NewApt, and the Win32/WinExt.A worm.

The tested version of *SAV* is the first in which only the archive handling product is supplied. Dealing with a variety of archive formats, *SAV* skipped happily through the archived ItW set, successfully managing to detect all of the samples within each of the six sets.

In terms of on-demand scanning speed, *SAV* is positioned at the upper end of the bulk of products, for both compressed and non-compressed file scanning. The overhead of *InterCheck*, *SAV's* on-access component, is reasonably small at a little over 100%.

Symantec Norton AntiVirus 2000 v6.00.03 (24/01/2000)

ItW File	100.0%	Macro	98.4%
ItW File (o/a)	100.0%	Standard	98.9%
ItW Overall (o/d)	100.0%	Polymorphic	94.2%

Rounding off this Comparative, *Symantec's Norton AntiVirus* (*NAV*) managed to carry on where it left off last time around, earning its ninth VB 100% award.

The bulk of the misses were registered in the Polymorphic set, thanks to samples infected with the A and B variants of ACG. A number of recent additions to the Macro set were also missed, including W97M/Melissa.AL, W97M/Thus.G, the B, C and D variants of W97M/Lys and the F and G variants of W97M/Verlor. Only a handful of samples were missed in the Standard set, most notably, and in common with a number of products in this review, the E and F variants of Win32/NewApt.

On-Demand Detection of Archived ItW sample test-set	Archived ItW Set Number											
	1		2		3		4		5		6	
	No. Missed	% Detected	No. Missed	% Detected	No. Missed	% Detected	No. Missed	% Detected	No. Missed	% Detected	No. Missed	% Detected
Aladdin eSafe Desktop	21	97.1%	21	97.1%	711	0.1%	711	0.1%	711	0.1%	711	0.1%
Alwil AVAST32	n/a	n/a	8	98.9%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CA InoculateIT	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
CA Vet Anti-Virus	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
DialogueScience DrWeb	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
Eset NOD32	0	100.0%	0	100.0%	703	1.3%	703	1.3%	703	1.3%	703	1.3%
F-Secure Anti-Virus	0	100.0%	0	100.0%	4	99.4%	4	99.4%	4	99.4%	4	99.4%
GeCAD RAV	2	99.7%	7	99.0%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Grisoft AVG	14	98.0%	14	98.0%	14	98.0%	14	98.0%	14	98.0%	14	98.0%
Kaspersky Lab AVP	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
NAI VirusScan	n/a	n/a	10	98.6%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Norman Virus Control	0	100.0%	0	100.0%	165	76.8%	165	76.8%	165	76.8%	165	76.8%
SoftWin AntiVirus eXpert	49	93.1%	49	93.1%	49	93.1%	49	93.1%	49	93.1%	49	93.1%
Sophos Anti-Virus	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%

The archive handling capabilities of *NAV* were, like *SAV* and four other products before it, impeccable. All of the 712 samples in each of the six sets were detected successfully.

Performance-wise, *NAV* did not let itself down, returning above average on-demand scanning throughputs, and displaying a relatively small on-access scanning overhead of approximately 120%.

Summary and Conclusions

The October 1996 issue of *VB* saw the first Comparative Review of products for the *Windows NT* platform. Back then the products were still in gestation – only four of the thirteen provided real-time protection, and a number were only slightly developed from their *Windows 3.x* brethren, with little familiarity with the *NT* operating system. The situation is different now – most notably, the provision for on-access scanning is a necessity, and duly all of the fifteen products in this review comply.

Detection-wise, things have tightened up as well, with six of the products achieving complete on-demand and on-access detection of the ItW file and boot viruses. Happily, none of these products triggered any false positives in the Clean set (although *AVP* sailed close to the wind in flagging a couple of samples as suspicious), and thus each earns the VB 100% award for this review. So, congratulations to these six – *Computer Associates' Vet Anti-Virus*, *Eset NOD32*, *F-Secure Anti-Virus*, *Kaspersky Lab AVP*, *Sophos Anti-Virus* and *Symantec Norton AntiVirus*.

Investigation of the archive handling capabilities of the products proved interesting, and the results provide an additional yardstick by which to judge performance. Looking at the detection rates within the archived ItW set, six products managed to detect all of the ZIP'ed and ARJ'ed (sometimes recursively) samples, namely *InoculateIT*, *Vet Anti-Virus*, *DrWeb*, *AVP*, *SAV* and *NAV*. Two other products came close (*FSAV* and *NVC*), but failed to detect all of the samples within the recursive archives.

Five of the products submitted offered on-access archive handling – a feature whose inclusion in a product currently remains up to the individual product developers. Looking at the large overheads that were observed in testing, it is clear that all of the products are a long way from being able to set real-time archive scanning by default.

[*For the purposes of this PDF, this Comparative has been modified to correct an error in the printed version.*]

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 NT 4.0 SP5*.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/200004/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.