COMPARATIVE REVIEW

Smash and Grab?

Matt Ham

Another month, another platform – and after the relatively meagre installation-base of *Windows ME* we are off to much more business-relevant climes in this *Windows 2000* Comparative Review. As was suggested in the previous test, new operating systems tend to play havoc with previously stable parts of anti-virus software, historically especially when floppy access has been considered.

Windows ME showed this to a very minor extent, no more than could be expected in any Comparative Review in fact – whereas affairs were not so pleasant on this occasion. The exact nature of these problems will be unveiled; so on with the preamble. There were also a number of errors and features firmly placeable in the 'bizarre' category, which will also be exposed in due course.

The Test-sets

The Comparative tests were performed on the standard *Virus Bulletin* test-sets, with the ItW samples aligned with the February 2001 WildList. There was a good deal of inquisitiveness, both in personal mail and in last month's Letters pages, concerning additional samples which might or might not be added to the test-sets. These were centred on the question of whether files of a more-or-less Trojan nature and which are dropped by ItW viruses, should be included in *VB's* ItW test-set.

An example of this type of file is the .EXE file which could at one time be downloaded by JS/Unicle or the modified AUTOEXEC.BAT files produced by the O97M/Cybernet.A virus, a newcomer to the ItW set on this occasion. To clarify the matter, our test-sets will include such files only as part of the Standard test-set, and even then may not be included in the final test results. The JS/Unicle-associated .EXE file was in this state for some months and the .INI file produced by W32/MTX has also been tested against but never included in results. Files included in the ItW test-set will only include those files which are a part of the infectious capability of the viruses in question, rather than those which are associated non-viral malware or ephemeral non-viral helper files.

Aladdin eSafe Desktop v3.0

ItW Overall	100.0%	Macro	98.8%
ItW Overall (o/a)	99.5%	Standard	98.8%
ItW File	100.0%	Polymorphic	94.5%

The Israeli product *eSafe Desktop* was the first to fall victim to the woes of floppy disk scanning on-access, with Michelangelo specifically the culprit. As this appears to be a non-formatted floppy to the watchful eye of *Windows 2000*, the operating system appears to pre-empt the on-access scanner with its declaration that the disk is not formatted and should be scanned.

This was seen when *Windows NT* entered the picture and *Windows* became more convoluted in the way that disk changes and contents were determined. Other than this, the detection rates were an improvement yet again, with, for the Wild set, only the extensionless version of O97M/Tristate.C being missed on-access.

Only one major barrier remained for the gaining of *eSafe's* VB 100% award if these two misses are dealt with and that was the 30 false positives during the Clean set scanning test. Perhaps as a result of the heuristic processes giving rise to the false positives, the scanning rate of the clean files was somewhat slower than the rest of the products tested.

Alwil AVAST32 v3.0.321.0

ItW Overall	99.4%	Macro	99.2%
ItW Overall (o/a)	90.5%	Standard	98.2%
ItW File	99.4%	Polymorphic	95.7%

As ever, the complications concerning *AVAST32* were primarily centred around on-access scanning in particular and the configuration of scanning in general. The *AVAST32* scanning configuration is, at the very best, labyrinthine in its control methods, making it a simple matter to set one small feature in the wrong manner and thus make results non-existent, unusable or in some other way awkward.

The on-access scans in the end resulted in a slightly less than stellar detection rate, especially on the .VBS files which were not registered when scanned on-access. There was also the recurrence of a hang while processing the on-access false positives testing on the OLE2 file set.

Further investigations failed to show any problems with the files which are apparently being scanned when the hang occurs, or indeed those directly before and after in the test-set, so this can be considered an on-going mystery, hopefully to be solved in time for the next review. The on-access problems ignored, however, the detection rate was good for all areas and on-demand scanning against the ItW test-set showed a 100% detection rate.

CA InoculateIT v4.53

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	98.8%

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	0	100.00%	100.00%	49	98.82%	52	94.59%	21	98.89%
Alwil AVAST32	0	100.00%	2	99.45%	99.49%	30	99.23%	27	95.74%	23	98.21%
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	9	98.87%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	0	100.00%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	6	99.71%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.99%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	3	99.97%	1	99.81%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	21	99.71%
GDATA AntiVirusKIt	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	1	99.77%	99.79%	4	99.90%	0	100.00%	1	99.90%
Grisoft AVG	0	100.00%	2	99.54%	99.58%	16	99.58%	124	92.01%	37	98.28%
Kaspersky Lab KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	19	97.86%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	1	99.97%	528	94.70%	32	98.74%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	6	99.83%	512	92.78%	19	99.51%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	28	99.38%	191	95.24%	37	99.15%
Symantec NAV	0	100.00%	0	100.00%	100.00%	13	99.62%	0	100.00%	14	99.85%
VirusBuster VirusBuster	0	100.00%	5	99.54%	99.58%	27	99.30%	6	99.24%	5	99.81%

The perils of the *InoculateIT* patching process were by far the most complex and irritating part of the whole of its testing process. A complex procedure at best, this was enhanced in the last Comparative by the wrong required patch list being supplied by *CA* for the *Windows ME* Comparative.

This time the test was performed with a new and extended set of patches in place, dispensing with February's Michelangelo detection problems and allowing *InoculateIT* to be the recipient of yet another VB 100% award, the first of many in this first ever *Windows 2000* Review. The changing of patches also removed the designation of all .VBS files as 'viral' – surely a good thing.

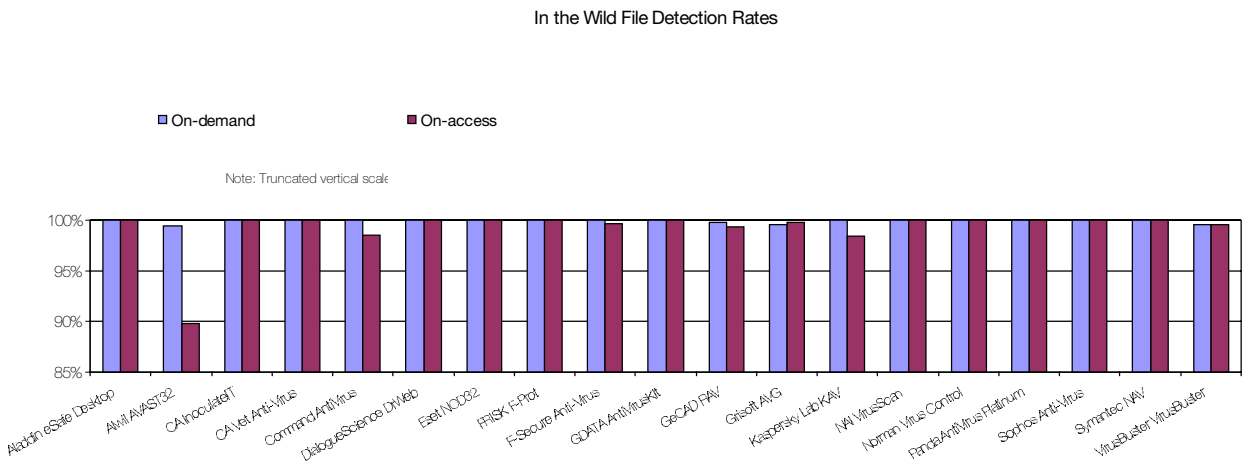
The only misses were in the Polymorphic set where the culprit was W95/Sk.8044. This has proved to be a stumbling block for many, with 11 out of the 19 products in this review having partial or no detection of this virus.

CA Vet Anti-Virus v10.2.10.0

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	93.7%

With another VB 100% to Vet's name, this has been another good month for *Computer Associates*. The main difference in performance here remains the Polymorphic set, where *InoculateIT* has the upper hand. *Vet* had misses in the cases of ACG.B, W95/Sk.8044 and W95/Sk.9972, all of them in the category of common misses across the board.

It is good to note, however, that their fellow polymorphic virus ACG.A is now becoming more universally detected rather than being in the same set of commonly missed viruses. Other than these, all files were detected both on-access and on-demand.



CA Vet and *InoculateIT* also showed a peculiarity in the scanning of the compressed OLE files for the Clean set – also shared by a number of other products. This is that the data throughput is faster for files which are compressed rather than uncompressed. Since the sizes used for the calculation of data throughput are uncompressed, this is doubly odd. It is possibly explained by the massively upgraded *VB* test machines used in the last two tests. With added memory and processing power, the manipulation of data may no longer be the limiting factor on these files, but rather the raw size which influences the rate at which data can be extracted from the hard disk. This would mean that uncompressed size is less important than compressed, thus giving the seemingly impossible results seen in the tests.

Command AntiVirus v4.61.0

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	98.5%	Standard	100.0%
ItW File	100.0%	Polymorphic	99.9%

One of three products in this review using the *FRISK* engine, this offering was notable for the differences between the detection performance on-access and on-demand. This is not an infrequent occurrence admittedly, though in this case the differences were seen almost exclusively in .COM files due to an engine error.

This oddness aside, detection rates were good, with only a single miss of ACG.A in the polymorphics and a smattering of Bat/911 and several viruses in the Standard set against *CAV's* good name. This was the first product in this review which, although demonstrating full detection of floppies on-access, was definitely affected unhappily by *Windows 2000*. Change detection was poor and in some cases could only be triggered by alternating disks between the standard floppy and LS120 on the test machines.

A final comment must be made concerning the lethargic initialistaion of *Command AntiVirus's* on-demand scanner which certainly led me to think that it had crashed the first time a scan was attempted.

DialogueScience DrWeb v4.23

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

The disk problems continued with *DrWeb*, and they were sufficient to deny the product a VB 100% due to the missing of Michelangelo on-access. A minor difference between this and previous results showed in two samples of the ageing polymorphic virus PeaceKeeper.B also being missed. This glitch in detection is possibly a result of a drive to reduce false positives – now standing at the relatively low number of fifteen warnings.

The developers at *DialogueScience* will no doubt be disappointed by the very narrow margin by which a VB 100% award was lost, although to be fair, the problems with *Windows 2000* are not likely to manifest themselves on any other current platform.

Eset NOD32 v1.70 NT

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

This Slovakian product has gone from strength to strength, and after a momentary absence from the VB 100% holders list *NOD32* is once more a worthy recipient.

Again, all files in all sets were detected, new families which were added to the Macro test set proved no problem here. With speed tests as well as detection results being favourable, there is little to add but congratulations.

FRISK F-Prot for Windows v3.09

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

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	1	94.44%	1	99.96%	99.54%	47	98.93%	52	94.59%	22	98.85%
Alwil AVAST32	0	100.00%	39	89.79%	90.56%	37	99.12%	28	95.36%	60	94.18%
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	9	98.87%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	0	100.00%
Command AntiVirus	0	100.00%	8	98.46%	98.57%	0	100.00%	161	96.55%	172	88.56%
DialogueScience DrWeb	1	94.44%	0	100.00%	99.58%	0	100.00%	2	99.99%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	20	97.84%	1	99.81%
F-Secure Anti-Virus	0	100.00%	4	99.63%	99.66%	0	100.00%	0	100.00%	22	99.68%
GDATA AntiVirusKIt	18	0.00%	0	100.00%	92.37%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	1	94.44%	5	99.31%	98.94%	4	99.90%	0	100.00%	1	99.90%
Grisoft AVG	0	100.00%	2	99.73%	99.75%	22	99.48%	292	89.47%	53	96.82%
Kaspersky Lab KAV	0	100.00%	5	98.39%	98.52%	0	100.00%	0	100.00%	3	99.71%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	19	97.86%	1	99.96%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	1	99.97%	528	94.70%	32	98.74%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	6	99.83%	1012	90.14%	19	99.51%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	28	99.38%	191	95.24%	37	99.15%
Symantec NAV	0	100.00%	0	100.00%	100.00%	13	99.62%	0	100.00%	14	99.85%
VirusBuster VirusBuster	1	94.44%	5	99.54%	99.15%	27	99.30%	6	99.24%	5	99.81%

Traditionally strong against the Macro test-sets, *F-Prot* lived up to its reputation with a 100% detection here – add to this full detection in the wild, and it becomes the recipient of a VB 100% award, another in the growing list this month.

A slightly lower detection on-access was made up for, at least in the eyes of a reviewer, by the ease of use of the scanner – particularly for the scanning of floppies both on-access and on-demand. The extra misses came from the ever problematical W95/SK.8044, various polymorphics and VBS/Verlor.F.

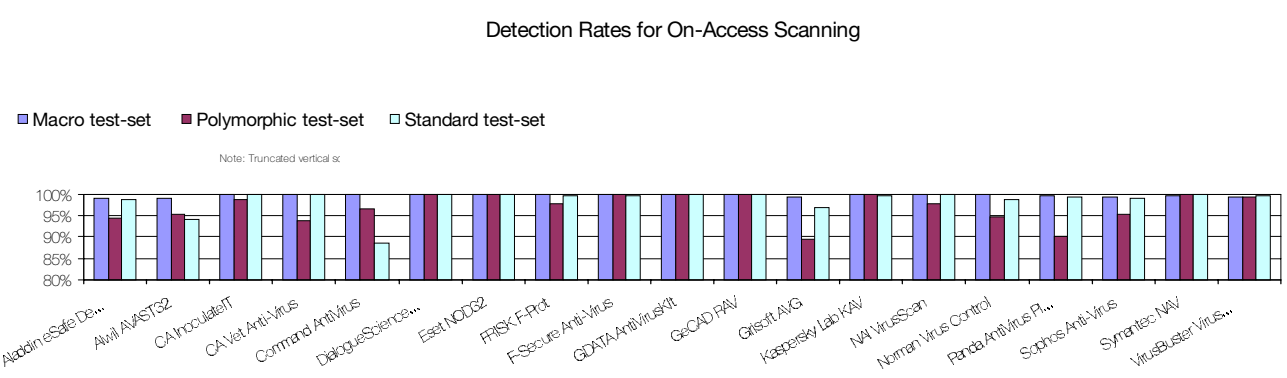
The *F-Prot* engine is also used by both *Command* and *F-Secure* in their products, and the speed ratings are fairly close between *F-Prot* and *Command AntiVirus*, with *F-Secure's* offering being notably slower. Detection-wise, however, *FRISK's F-Prot* is better than the other pair, as might be expected the engine's original development team.

F-Secure Anti-Virus v5.22 build 7072

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	99.6%	Standard	99.7%
ItW File	100.0%	Polymorphic	100.0%

With talk of *F-Prot* in mind we move on to *F-Secure Anti-Virus* (*FSAV*). Although not really relevant here, the lower speeds seen in this product are possibly a result of the more network-integrated nature of *FSAV*, which results in many more options being built into the engine and the provision of HTML reports for cross-platform viewing. These are at least convertible to text format for analysis. They cannot, however, be held responsible for the rather long time taken to initialise the program.

FSAV also showed some problems on the on-access boot tests, though not enough to deny it full detection. The big disappointment will be the missing on-access of the



W32/MTX .DLL sample in the Standard and ItW sets, which removed a VB 100% award from *F-Secure's* grasp.

GDATA AntiVirusKit v10.0.1.0

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	92.3%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

AntiVirusKit (*AVK*) is a relative newcomer to the *VB* test ranks and, after initial hiccups, has shown itself a worthy product. A sticky start on the on-demand floppy tests did not bode well for *AVK* on this occasion, though after many attempts the full set was detected, and no detection was possible on-access by design. This was in marked comparison with the tests on file viruses, since all other tests showed a full detection rate.

With such a good detection rate elsewhere, the floppy detection is something of a disappointment and denies *AVK* its first VB 100% award.

GeCAD RAV v8.2.1.4

ItW Overall	99.7%	Macro	99.9%
ItW Overall (o/a)	98.9%	Standard	99.9%
ItW File	99.7%	Polymorphic	100.0%

RAV was home, in this test, to perhaps the most bizarre of the idiosyncrasies seen in *VB* testing for a long while. Files on-access were at first impossible to scan at all, despite all being well on the installation front and the ability to detect the *EICAR AV* test file without problems. The test-sets were shuffled, moved and retested several times to no avail. In a moment of inspiration it was realised that the only difference between the *EICAR* files and the test files was that the test files were read-only. Sure enough, removing the read-only status of the files allowed testing to progress normally.

After such a mysterious start to the process the subsequent results were more prosaic. *RAV* missed Michelangelo on-access and suffered poor on-access floppy change detection. It also threw up four false positives and thirteen suspicious files in the Clean test-set. Admittedly, detection rates were actually towards the top end of the scale, though were let down by the numerous small problems seen.

Grisoft AVG v6.0.236

ItW Overall	99.5%	Macro	99.5%
ItW Overall (o/a)	99.7%	Standard	98.2%
ItW File	99.5%	Polymorphic	92.0%

AVG missed out on full detection ItW by dint of missing both JS/Unicle and O97M/Tristate.C, though the results were different on-access and on-demand to quite some degree. This difference was apparent across the test-sets, with the on-access scanner failing to detect a fair few more viruses than its on-demand counterpart. Most of these were polymorphs of the families already mentioned several times, to which were added misses in the Standard set which were unique to *AVG*.

The misses in the ItW set are small and should be relatively easily rectified, though the less important but more pronounced problems in the Polymorphic test-sets could be more complex to sort out. One area where *AVG* does shine, however, is in the aspect of speed, with OLE files being particularly fast. There are still false positives in the Clean set scan which is less speedy, perhaps due to the heuristics which cause the false positives.

Kaspersky Lab KAV v3.5.133.0

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

Kaspersky AntiVirus (*KAV*) has suffered recently in the *VB* tests due to the spawning of new virus types with associated new file extensions. This month saw no new additions to the test-set as far as extensions were concerned, and sure enough the infected files were detected in their entirety during on-demand scanning.

The *KAV* engine has traditionally behaved identically on-access and on-demand, thus on-access results would be expected to be the same as those for on-demand.

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
Aladdin eSafe Desktop	1847	296119	30	21	3777798		1126	141578	37	2016419
Alwil AVAST32	114	4797651		N/A	N/A		91	1751831	24	3108646
CA InoculateIT	92	5944915		15	5288918		51	3125815	12	6217291
CA Vet Anti-Virus	247	2214300		20	3966688		86	1853681	15	4973833
Command AntiVirus	154	3551508		18	4407432		59	2701976	20	3730375
DialogueScience DrWeb	275	1988844	[15]	26	3051299		121	1317492	21	3552738
Eset NOD32	104	5258963		14	5666698		86	1853681	28	2664553
FRISK F-Prot	189	2893821		17	4666692		102	1562908	46	1621902
F-Secure Anti-Virus	494	1107150		26	3051299		364	437958	65	1147808
GDATA AntiVirusKIt	216	2532093		35	2266679		108	1476080	37	2016419
GeCAD RAV	664	823693	4 [13]	15	5288918		396	402567	11	6782500
Grisoft AVG	217	2520425	4 [2]	14	5666698		90	1771295	14	5329107
Kaspersky Lab KAV	145	3771946		21	3777798		95	1678069	25	2984300
NAI VirusScan	295	1854007		29	2735647		81	1968106	21	3552738
Norman Virus Control	287	1905687		18	4407432		159	1002620	20	3730375
Panda AntiVirus Platinum	211	2592096		14	5666698		76	2097587	10	7460750
Sophos Anti-Virus	125	4375457		19	4175461		56	2846725	13	5739038
Symantec NAV	250	2187729		29	2735647		112	1423362	30	2486917
VirusBuster VirusBuster	223	2452611		17	2452611	[1]	139	1146882	22	3391250

Unfortunately, however, this was not to be. The on-access scanner for *KAV* now contains an option to activate the scanning of packed files, not activated by default. This is required for the detection of some files ItW and was sufficient to remove both full on-access detection and a VB 100% award from the *Kaspersky Labs* trophy cabinet.

NAI VirusScan v4.5.0.534

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

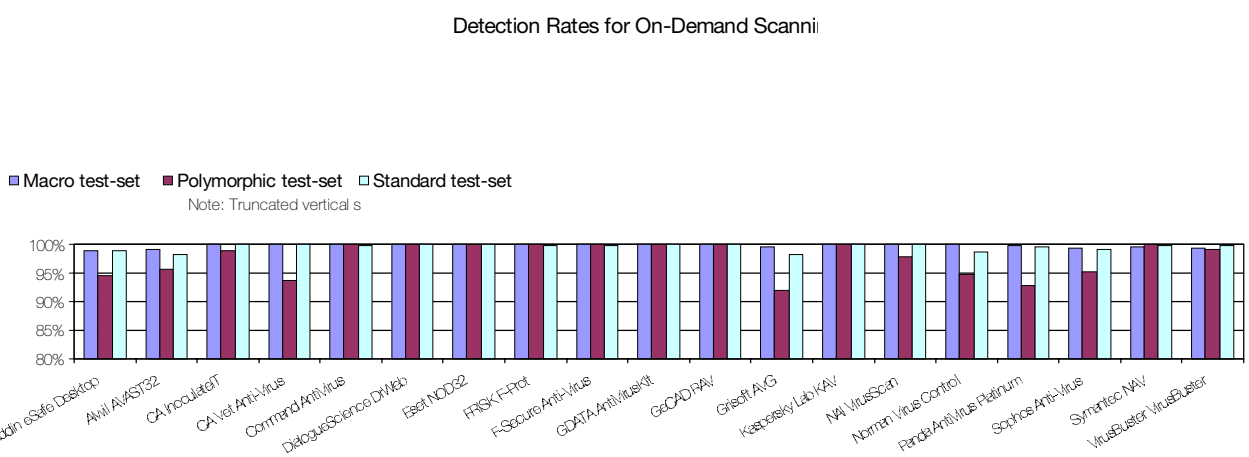
After vituperative words for the team at *NAI* for the last two Comparative Reviews, the tone is this time somewhat mellowed. Starting with old woes, *VirusScan* can still be convinced to deactivate its on-access scanner by one of the files in the test-set which continues to invoke ire in the *VB* test labs. The speed problems and instability are, however, a thing of the past, though possibly partially due to the increased power of the test machines. Floppy detection was an easy and pleasant affair and altogether the gaining of a VB 100% award by *VirusScan* is a well-deserved prize for recent improvements.

It should be noted that testing was performed with Service Packs and patches applied – one patch of the set being that which permanently activates the scanning of all files.

Norman Virus Control v5.0

ItW Overall	100.0%	Macro	99.9%
ItW Overall (o/a)	100.0%	Standard	98.7%
ItW File	100.0%	Polymorphic	94.7%

One of the more unusual programs to run in the Comparative, *Norman Virus Control's* (*NVC*) detection rate has been much improved since the inception of its newest scanning engine. The



interface problems encountered in the last review were markedly less apparent on this second encounter – some helpful prods from the developers and added familiarity making the whole affair much more pleasant.

Detection results were identical on-access and on-demand, with full detection on both swelling this month's bumper crop of VB 100% awards. *NVC's* main weakness is in the Polymorphic sets where Digi.3547, W95/Sk8044 and a sprinkling of Sepultura:MtE-Small were the culprits.

The product's polymorphic detection percentages have, however, improved markedly. *Norman* will, perhaps, be looking for further improvements as the year progresses.

Panda AntiVirus Platinum v6.23.00

ItW Overall	100.0%	Macro	99.8%
ItW Overall (o/a)	100.0%	Standard	99.5%
ItW File	100.0%	Polymorphic	92.7%

Panda AntiVirus (*PAV*) *Platinum* is another product which suffers far greater weakness against the Polymorphic sets than in other areas, though this is more apparent on-access, the number of misses roughly doubling when the detection method is changed. These misses were scattered throughout a number of samples in the Polymorphic sets, with partial detection being more common than no detection at all.

The polymorphics were the only problems, *PAV's* otherwise solid performance being sufficient to reap it a well-deserved VB 100% award. A special mention should also be made of the speed with which *Panda AntiVirus* was able to scan OLE files which was the fastest in the pack whether the files were zipped or not.

Sophos Anti-Virus v3.43

ItW Overall	100.0%	Macro	99.3%
ItW Overall (o/a)	100.0%	Standard	99.1%
ItW File	100.0%	Polymorphic	95.2%

This was a far happier outing for the *Sophos* product than the last two *Windows* Comparatives, where the new viral extensions caused some misery. Detection has improved against the Polymorphic set and more gratifying will be the arrival of a VB 100% for the complete detection both on-access and on-demand.

As has been customary in past tests the detection was identical on-access and on-demand. There was a momentary scare when the on-access scanner was added and tests showed extra misses, but this was tracked down to the purging of temporary virus identities when the product is upgraded. The reasoning behind this is clear – these are not required when the product is properly upgraded, but perhaps more warning would be appropriate.

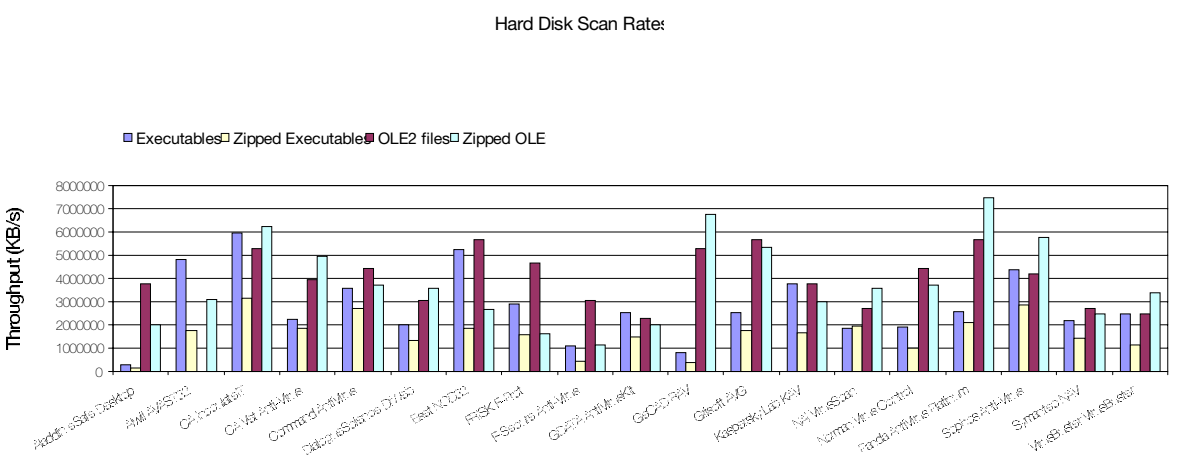
Symantec NAV Corporate Edition v7.50.846

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

Approaching the final entries in this Comparative I can once more enter 'rant' mode. On-demand scanning again caused *NAV's* scanner to lock up – difficult to tell since the initiation process for any activity seemed interminable.

The post-scan reports were the sticking point, being the moment at which crashes occurred, but more oddly they could be exported only in comma-separated or .MDB format, rather than the plain text equivalent .TXT file which might be expected. All these combined to force detection by deletion.

Floppy scanning was also nightmarish, the process of beginning a scan taking up to 20 seconds to reach the scanning process, and with poor change detection this was the cause of many an unpleasant curse. Despite all these problems detection was at NAV's usual high rate, earning a VB 100% award with only a scattering of misses in the Macro and Standard test-sets.



VirusBuster VirusBuster v3.03

ItW Overall	99.5%	Macro	99.3%
ItW Overall (o/a)	99.1%	Standard	99.8%
ItW File	99.5%	Polymorphic	99.2%

Last but not least this month is *VirusBuster*, which suffered as others from the curse of Michelangelo, resulting in a miss for on-access floppy scanning. The February 2001 WildList was also responsible for misses, the samples of Win95/Caw.1262 being undetected in the ItW File test-set. This will be very much a frustration for the *VirusBuster* development team, which has missed a VB 100% by similar slim margins for several months now. With false positives down to a scant single warning and the speed still good, the future should hold better news.

Conclusion

The new platform made several differences to the results of this testing, the new test-sets made less impact – both bear some further examination. What is at first glance contrary to common sense and in opposition to the results of the *Windows ME* test can, in fact, be seen to agree with both these methods of reasoning.

The changes from *Windows NT* to *Windows 2000* are certainly more all-pervading than the changes within the *Windows 95/98/ME* product line, and where file access is affected, anti-virus products will always be impacted. Failure to detect Michelangelo when the operating system is claiming that nothing exists which should be scanned is something which could perhaps be expected more often than was seen in the tests here.

It is doubly compounded by this being only testable on real floppies, when much QA is done on disk images where detection is much simpler. Nor is it necessarily a sign of technical laxness – one anonymous developer stated that his product was only saved from not detecting it because it performed detection in 'not a very clever way.'

As for the matter of the test-sets – while *VB* does intend to continue the use of the Standard test-set, where the so-called Old Fashioned File Viruses mostly reside – most additions are made to the Macro and ItW test-sets.

Of these, the macro test-set is a category in its own right and one which is in general a game of catch-up with the virus writers, with regard to the volume of viruses written rather than complexity. Some major opportunities for mass failures in detection do exist but these are most often concerned with changes in *Office* imposed by *Microsoft*. This is not notably the case at the moment and so the impact on the detection rates is small.

This leaves the ItW set, by its nature a catch-all, where scanning results are likely to fluctuate as test-sets are changed. This is again only under certain circumstances, one of which at least is the introduction of new Operating System features.

The most likely circumstance, however, is currently the addition of new file extensions for scanning, which in this edition of the test-sets turned out not to be the case. So the factors this month seemingly acted to lessen detection failures due to changes in test-set and heighten those due to Operating System.

So much for the discussion, but what does the future hold? The likelihood of new virus types being the major impact upon detection is intrinsically tied in with the new Operating System features which make these viruses possible. So, in the case of *Windows*, the developers can only watch and wait as *Microsoft* expands the capacity for disaster within its various incarnations.

Technical Details

Test Environment: Three 750 MHz AMD Duron workstations with 128 MB RAM, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, all running *Windows 2000*. The workstations were rebuilt from image back-ups and the test-sets restored from CD after each test.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/2001/02test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.