COMPARATIVE REVIEW

Compare and CoNTrast

Matt Ham

Every month has its theme as far as Comparatives are concerned. In my carefree youth, I may have been able to construe that light-heartedly, but it now seems that a more ‘grumpy old man’ state of grouchiness has been entered. This might not be entirely due to age, however, as the products this month were in some cases worthy of insults not printable in a family journal.

Specific rants will come later but include the obligatory blue screens, a few buckets of application lethargy, a dash of unscannable files and a sprinkling of obtuse terminology. Those of you who have a spare moment or two might well wish to link the problem to the product before starting to read – and may well be surprised.

There were added to this a few upsets in the pursuit of VB 100% awards and a few near misses either through oversight or misadventure. Overall, despite being responsible for the destruction of several vendors’ hopes this month, it was definitely an interesting review to write and, it is hoped, will make interesting reading too.

Test Procedures

The last *NT* Comparative was featured in September 1999’s *VB*. Readers are advised to refer to the testing procedures and protocol detailed there. For this Comparative, test-sets were updated and the ItW File and Boot aligned to the September 2000 WildList.

As before, full details of the results are presented in the tables. The results featured under the product headings are all for on-demand scanning unless otherwise indicated.

Aladdin eSafe Desktop v2.2

ItW Overall	98.1%	Macro	95.1%
ItW Overall (o/a)	97.9%	Standard	93.9%
ItW File	98.0%	Polymorphic	80.9%

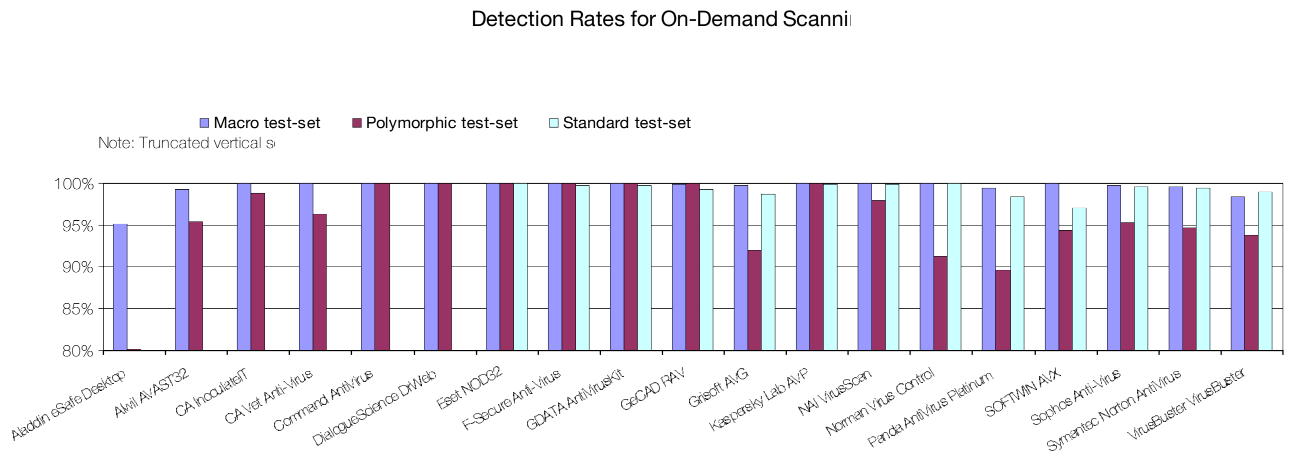
The *eSafe Desktop* is a whole range of programs forced into one application, with some odd interrelations as far as accessing the virus scanner part is concerned, and no note as to version number included within the applications. This complexity might be behind the mystery of the disappearing scan – whereby a scan was started, the operation was clearly occurring as far as disk accesses went, and yet no scan could be discovered through any of the methods available. This proved an isolated incident, however, and other scans progressed without further hitches.

The few problems incurred in producing the results were not particularly indicative of great detection. On-access there were considerable misses in the Polymorphic sets, and the Macro set threw up some weaknesses too. On many occasions in the latter set the product detected a virus in all but the template form.

Alwil AVAST32 v3.0.293.0

ItW Overall	100.0%	Macro	99.2%
ItW Overall (o/a)	n/t	Standard	98.9%
ItW File	100.0%	Polymorphic	95.4%

AVAST32 has a most remarkable on-access component, which seems to be triggered only by the method of not wanting it to trigger. Straightforward on-access testing for viruses proved, after exhaustive fiddling, to be an impossible task. However, since the *AVAST32* engine has heuristics and checks for such operations as copying files, the



On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	1	98.13%	98.18%	191	95.13%	1144	80.09%	117	93.92%
Alwil AVAST32	0	100.00%	0	100.00%	100.00%	31	99.21%	28	95.36%	13	98.93%
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	9	98.87%	2	99.61%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	178	96.37%	0	100.00%
Command AntiVirus	0	100.00%	3	99.70%	99.71%	0	100.00%	1	99.98%	13	99.23%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
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%	1	99.50%	99.51%	0	100.00%	0	100.00%	2	99.71%
GeCAD RAV	0	100.00%	1	99.75%	99.76%	8	99.79%	0	100.00%	8	99.25%
Grisoft AVG	0	100.00%	2	99.50%	99.51%	11	99.71%	124	92.01%	30	98.67%
Kaspersky Lab AVP	0	100.00%	1	99.50%	99.51%	0	100.00%	0	100.00%	1	99.81%
NAI VirusScan	0	100.00%	1	99.93%	99.93%	0	100.00%	17	97.87%	7	99.86%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	286	91.23%	0	100.00%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	26	99.35%	889	89.69%	50	98.34%
SOFTWIN AVX	0	100.00%	2	99.69%	99.70%	2	99.95%	55	94.36%	63	97.07%
Sophos Anti-Virus	0	100.00%	1	99.93%	99.93%	13	99.65%	191	95.24%	14	99.55%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	264	94.74%	16	99.46%
VirusBuster VirusBuster	0	100.00%	29	96.16%	96.27%	66	98.34%	292	93.77%	10	99.01%

on-access scanner was all too easily triggered by the overhead testing regime which employs the notorious XCOPY command. Adding insult to the already considerable mental injuries imparted by these circumstances, the product failed, during floppy on-access tests, to detect Michelangelo.A and Stoned.June_4th.A.

Unfortunately, Clean set testing produced a single false positive, but *AVAST32's* scan times were very much in the 'respectable' range. All in all, *AVAST32's* performance ItW was impeccable, but the lack of a testable on-access scanner, and the false positive, denied it a VB 100% award.

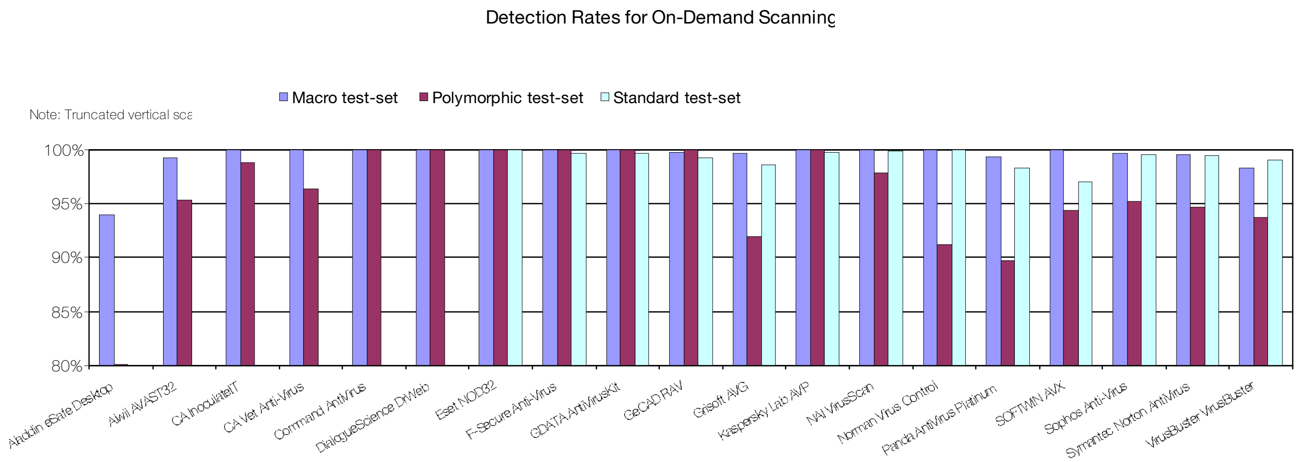
CA InoculateIT v4.53 16.24

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	99.6%
ItW File	100.0%	Polymorphic	98.9%

The main niggle with *InoculateIT* turned out to be at the installation stage. This process required several different patches, some self-extracting, others using *CA's* own custom decompression utility. Having worked through this and a subsequent install with numerous option selections, all was plain sailing.

Despite being the first product to claim a VB 100% award this month, it must be mentioned that the usually reliable *InoculateIT* did display signs of instability, eventually performing well after several false starts. Having said that, the results speak for themselves and the first of *Computer Associates'* products can rest assured that its reputation for a solid performance has been maintained.

There are currently rumours abounding about changes to *CA's* anti-virus product lines. It may be that by the next Comparative, *CA* no longer offers two distinct products. So, how did *Vet* compare this time round?



CA Vet Anti-Virus v10.2.2

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	96.4%

The traditionally stable *Vet* managed to get off to an impressively unusual start with a blue screen during browsing for a scan area. The product also performed oddly in that its default ‘action’ mode for files only reported viral infections – it did not deny access to them. Added to this was the continuing offer of a ‘format’ after the accessing of any infected floppy.

When combined with the developer warnings of ‘bugginess’ within the virus definitions, there were no great hopes held out. However, no further problems ensued and *Vet* turned in a solid performance. *CA’s* second product is, once more, the proud possessor of a VB 100% award.

Command AntiVirus v4.59.4

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

Command AntiVirus was something of a pleasant exception to the rule in this review, exhibiting no real problems, glitches or irritations in its operations.

The product was let down by its on-demand scanner, which detected slightly fewer viruses than its on-access counterpart. An average scan speed placed *Command* pretty much in the middle of the pack, and while no false positives were discovered, the only thing that really distinguished this product was ease of use and stability.

DialogueScience DrWeb v4.21

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	97.1%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

The oddities evinced by *DrWeb* were thankfully of the non-destructive sort, especially in the case of reboots. Unlike another product’s unannounced reboot feature, *DrWeb* states that a reboot will occur and is required, though this never comes to pass. This feature was particularly glaring due to the nature of the on-access component. Each alteration to this requires a reboot to be effective, irritating in a normal environment and enraging when testing a product under various configurations.

The singularity of the on-access scanner was not limited to these antics, however, since it operates a ‘smart mode’ for deciding which files should be scanned. No files were detected as being viral, however, since this ‘smartness’ was not pronounced enough to trigger a reaction.

Selecting ‘open’ as the trigger proved rather more effective, though it should be noted that the detection rates on-access are therefore not those produced under a default configuration. This alone would be sufficient to deny *DrWeb* a VB 100% award, though the point was moot given the lack of on-access boot sector scanning in this product.

Eset NOD32 v1.47

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

This month *NOD32* was denied a VB 100% award for the first time in living memory. This was not due to poor detection, however, as every file in the *VB* test-sets was detected as viral. The problem came in this case with false positives – the little-known HLLC.Fataler virus apparently showing up in some Clean set files.

A few new (to this reviewer at least) features cropped up as well, most of which appeared to be for the sole purpose of securing *NOD32* from those interfering busybodies also known as users. This took the form of password-protection for settings within the program. This product remains the fastest in terms of scanning speed for executables – its handling of OLE files is hardly sluggish either.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	12	97.98%	98.04%	191	95.16%	1144	80.09%	122	93.58%
Alwil AVAST32	2	91.67%	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.61%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	10	99.86%	768	91.10%	3	99.81%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	9	99.22%
DialogueScience DrWeb	24	0.00%	3	99.88%	97.07%	19	99.79%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	1	99.93%	99.93%	0	100.00%	0	100.00%	21	99.71%
GDATA AntiVirusKit	24	0.00%	649	22.26%	21.63%	1488	60.82%	623	83.30%	34	98.26%
GeCAD RAV	0	100.00%	1	99.75%	99.76%	8	99.79%	0	100.00%	8	99.25%
Grisoft AVG	24	0.00%	3	99.61%	96.81%	12	99.74%	292	89.47%	46	97.22%
Kaspersky Lab AVP	24	0.00%	1	99.50%	96.70%	0	100.00%	0	100.00%	1	99.81%
NAI VirusScan	0	100.00%	1	99.93%	99.93%	0	100.00%	99	95.71%	8	99.85%
Norman Virus Control	0	100.00%	7	99.50%	99.51%	26	99.46%	300	90.40%	2	99.77%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	26	99.35%	889	89.69%	52	98.21%
SOFTWIN AVX	24	0.00%	2	99.69%	96.89%	2	99.99%	56	94.36%	77	96.59%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	264	94.74%	18	99.44%
VirusBuster VirusBuster	24	0.00%	29	96.16%	93.46%	66	98.34%	292	93.77%	292	93.77%

F-Secure Anti-Virus v5.2 Build 6382

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

FSAV's system of logging – entailing large amounts of data being held for analysis after scans – again seemed the cause of instability during testing. This manifested itself in an apparently innocent pause, which unfortunately turned out to be a hang sufficient to prevent reloading the scanner without a reboot. As with other products, the circumvention of stability problems involved detection by deletion.

On-access boot scanning, despite being 100% effective on the detection front, showed a peculiarity with alerting. Upon detection, two windows pop up. The topmost one is unusable and it is in the hidden window that choices, not easily apparent in this state, must be made. It would presumably make more sense in a network setting, though the software was installed in a dedicated standalone mode.

Despite being capable of detecting the .DLL part of W32/MTX on-demand, *FSAV* somehow missed it on-access ItW and thus avoided a VB 100% award. Other misses were more consistent over the on-access and on-demand scans, including the .BAT forms of 911.A and 911.B.

GDATA AntiVirusKit Generation 10

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	21.6%	Standard	99.7%
ItW File	99.5%	Polymorphic	100.0%

The first sighting of this line in a *VB* Comparative would suggest a new product, though beneath its exterior beats a reliable heart – the *AVP* engine. Having spent many happy, and a few not so happy, hours with *AVP* I noticed that the products definitely share a similarity in approach. One major difference lies in the matter of macro virus detection.

On-access, these files are, by default, simply not searched for. This might seem a glaring omission yet it is not quite as bizarre as it might seem. *AntiVirusKit* includes an *Office*-integrated virus scanner which would lead to effective redundancy were OLE files scanned on-access. Whether this is a good or bad idea overall is open to debate, but the on-access detection rates are very much altered by this fact. The objects and actions scanned are subject to some alterations in scope, though until the product has been through a full standalone review the options selected were deliberately limited to a simple 'on/off'.

The perils of a product not 100% home-built were apparent in its uncharacteristic (for *AVP*) instability. This was noted during on-demand floppy scanning, where alerts consisted of three different windows – the alert itself, an analysis and a report. With many samples to scan, speed is usually of the essence, though in this case there were altogether too many visits to Dr Watson.

As well as the misses produced by the option of not scanning for macros, *GDATA's* product also missed other files all of which (apart from VBS/Netlog.D) were detected successfully by *AVP*. The problem is mainly the choice of extension scanned, and some old favourites, namely W32/Marburg-infected screensavers and W95/Navrhar-infected VXDs, made an unwelcome return to the missed list. More disturbingly, there were some simply unaccountable misses, including several samples of the venerable Digital in the Polymorphic set.

GeCAD RAV Desktop v8.0.56.29

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

RAV has undergone something of a facelift in its latest, pre-release incarnation – to the extent that it now sports skins in the same way as programs such as *WinAmp* do. Admittedly, one of those supplied would make all but the most ardent dog-lover cringe, though the other is agreeable in an 'oval' kind of way.

Such improvements will remain unseen by some users, however, as several of the configuration screens are of a fixed size and too large to use in lower resolutions. Even with the correct resolutions it was not possible to activate all features and in the absence of a functioning log file the scan was performed by deletion.

The scan itself was notably slow, though by no means the worst on offer, with Neuroquila proving particularly soporific for the *RAV* engine. Having said all this, detection rates showed a significant improvement over *RAV's* last outing in an *NT* Comparative.

Grisoft AVG v6.0.198

ItW Overall	99.5%	Macro	99.7%
ItW Overall (o/a)	96.8%	Standard	98.7%
ItW File	99.5%	Polymorphic	92.0%

The finest hour in *AVG's* attempt upon the reviewer's sanity came in, of all things, the update procedure. Having downloaded the correct version of the virus definition updates file and installed it, nothing happened. Consultation with the developer led to the interesting revelation that the English (UK) and English (US) versions are mutually incompatible. It also seems that there is no immediately obvious source for the former on the *AVG* Web sites. When an update was finally triggered the installation required the program to restart – which, in turn, triggered an unannounced reboot of the machine. With such a start it came as no great surprise that scans are quite fiddly to set up under the *AVG* Task Manager.

On-access misses included the now notorious JS/Unicle and the extensionless O97M/Tristate.C, together with the .OCX part of W32/Funlove. The remaining Tristate samples in the Macro test-set were also missed in the same extensionless form, though overall *AVG's* performance was respectable, with only the WM/Password and A97M/AccessiV samples missed otherwise. The Polymorphic set too showed only the 'usual suspect' misses of ACG.A and .B, plus the samples of Win95/SK8044 and Win95/SK7972.

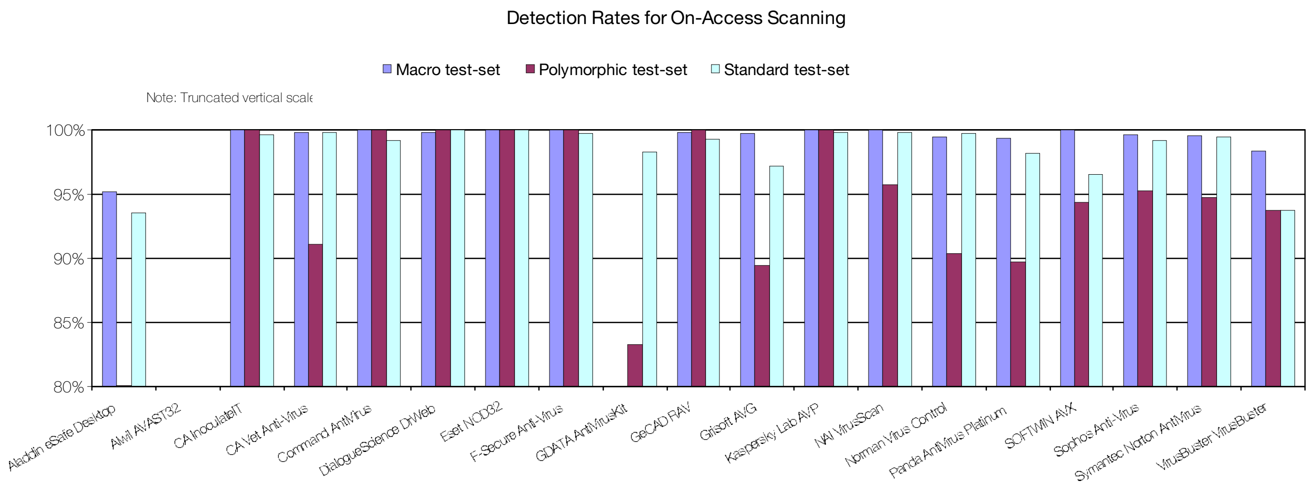
Kaspersky Lab AVP v3.5.133.0

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	96.7%	Standard	99.8%
ItW File	99.5%	Polymorphic	100.0%

AVP was denied a VB 100% award in the *NetWare* Comparative by dint of dubious default extensions and the missing of a single sample of VBS/Netlog.D. This glitch was a cause of some consternation since the chaps at *Kaspersky Lab* were adamant that they detected this virus. Exchanges of samples proved this to be a naming issue – their Netlog.D was most other folks' Netlog.B, though numerous other names popped up on competing scanners.

This might cause some readers to wonder how the *VB* test-set samples are chosen, if the AV developers cannot decide how viruses should be named. The answer is thankfully simple, our ItW samples are replicated from WildList samples which have been directly replicated from the wild. Thus, we can be sure that the *VB* Wildset reflects precisely those samples in the WildList.

The non-detection of VBS/Netlog.D in this month's Comparative was the only thing which stood between *AVP* and 100% detection of all file samples on-access. *AVP* was also, however, another of those scanners whose *NT* on-access boot scanning capability is notable by its absence, and thus missing the VB 100% award was not simply a naming problem after all.


Detection Rates for On-Access Scanning

NAI VirusScan v4.5.0.534

ItW Overall	99.9%	Macro	100.0%
ItW Overall (o/a)	99.9%	Standard	99.9%
ItW File	99.9%	Polymorphic	97.9%

The *NAI* scanning front end has mutated recently from an all bells and whistles affair to one which stresses purity and simplicity. If only this were matched in the field of virus detection. At first, problems seemed to be centred upon sluggish performance, but as the tests proceeded this became progressively worse. Left to its own devices the scan crashed repeatedly and was thus performed under a more watchful eye and by deletion. This soon proved to be far too painful, as upon scanning samples of W97M/Splash affairs became all but stationary.

W97M/Splash is a polymorphic macro virus, but it is polymorphic in the most basic way – by the insertion of random comments at each generation. Since these are never deleted the viral macros tend to become rather large and *VirusScan* accordingly had problems with the sizes. Earlier generations took minutes to scan, later ones were left to their own devices after the best part of a day had passed.

When the on-demand scan was eventually completed, I regarded the on-access scan with some trepidation but it proved eventful for other reasons. W97M/Splash samples were presumably subject to a time-out within the on-access scanner since there was no detection of these as viruses after a certain size.

The scan did, however, succeed in unloading the *McShield* component of the application after a certain point. Further investigations proved this to be the fault of the W32/Parvo virus, one sample of which could reproducibly unload the on-access scanner.

VirusScan was by no means alone in missing the .PIF versions of W32/MTX.B. The addition of Win95/SK8044 in the Polymorphic set and the .PIF portions of BAT/911.A and BAT/911.B rounded off its misses during both on-demand and on-access scans.

Norman Virus Control v4.86

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	99.5%	Standard	100.0%
ItW File	100.0%	Polymorphic	91.2%

Usually a safe bet as far as stability is concerned, *NVC* was thankfully still on good form. There was a rather tedious delay incurred by the slowness of the zipped throughput test files but otherwise no problems were encountered.

NVC suffered the same fate as others with misses on the .PIF W32/MTX.B files, though a smattering of other misses on-access took the VB 100% award from *Norman's* grasp anyway. These misses were, unlike in most other cases this month, seemingly without rhyme or reason.

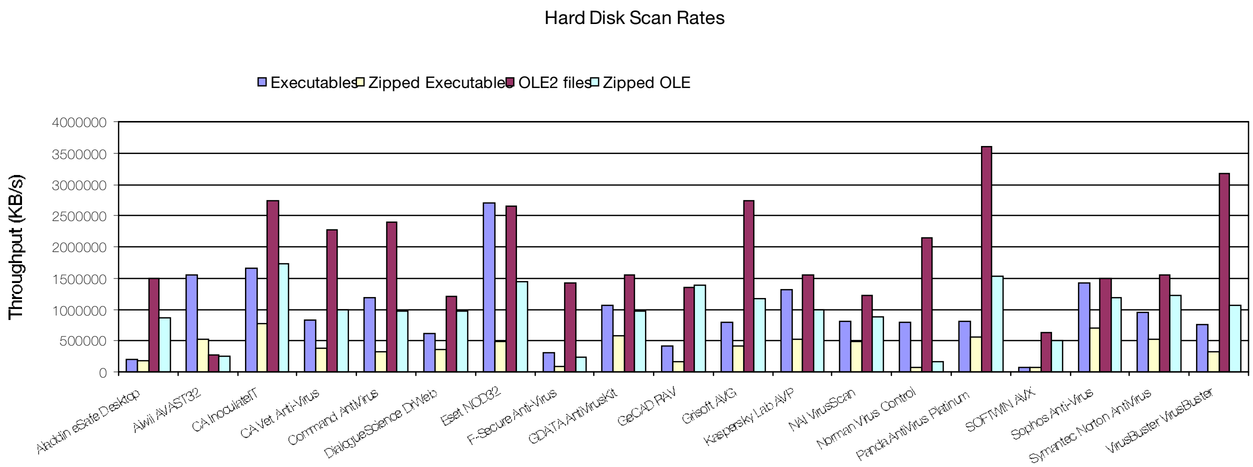
Panda Antivirus Platinum v6.20.00

ItW Overall	100.0%	Macro	99.4%
ItW Overall (o/a)	100.0%	Standard	98.3%
ItW File	100.0%	Polymorphic	89.7%

A good, solid performance by *Panda Antivirus Platinum* was nevertheless shanghai'd (as far as the VB 100% award goes) by the discovery of a single fasle positive. This product showed an admirable stability under most circumstances and was one of the more user-friendly on offer.

One oddity here seemed to be a lack of any way to restore the on-access scanner after it had been unloaded, short of restarting *Windows*. This did, however, give plenty of time to admire the ghostly panda's head which appears in the pre log-on screen of *NT* when *Panda Antivirus* is active. On-demand too there were strange forces at work, the speed tests culminating in an access violation which caused the scanner to cease operation.

While this product was far and away the speediest of the pack when scanning OLE files, traditional weaknesses remain within the Polymorphic set, where it missed an assortment of both old and new viruses.



SOFTWIN AntiVirus eXpert 2000 Desktop v5.8.0.12

ItW Overall	99.7%	Macro	99.9%
ItW Overall (o/a)	96.9%	Standard	97.1%
ItW File	99.7%	Polymorphic	94.4%

A product which recently passed through the *VB* standalone review process, this product gave no great surprises. It was mentioned in the last review that on-access scanning was not tested and this turned out to be due to the absence of protection within *NT* DOS boxes. Using a native *Windows* test application allowed on-access results to be obtained on this occasion, though real-time overhead tests were still not available since the standard *Virus Bulletin* test is itself run in a DOS box.

On-access, the ItW misses were few – one of the JS/Unicle samples and a .EXE version of Babylon – while in the Macro set just a couple of Win95/Navrhar-infected documents slipped past. More misses were apparent in the Polymorphic set, though *AVX* managed to detect ACG.A in the majority of samples proffered, whereas usually this virus is an ‘all or nothing’ affair.

Sophos Anti-Virus v3.38

ItW Overall	99.9%	Macro	99.7%
ItW Overall (o/a)	100.0%	Standard	99.6%
ItW File	99.9%	Polymorphic	95.2%

The problems encountered by *SAV* on this outing were relatively minor, being relegated to a poor selection of files to scan. This was particularly galling given that the resulting failed detections only occurred on-demand. The offending files were the .PIF versions of W32\MTX.B which, although not scanned by default, triggered the file type detection algorithms within *SAV’s* on-access scanner.

Other than this, the misses and hits achieved by *SAV* followed an almost predictable pattern – stability was traditionally excellent and the overall performance solid.

Symantec Norton AntiVirus 2000 v6.00.03

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	100.0%	Standard	99.5%
ItW File	100.0%	Polymorphic	94.7%

Norton AntiVirus cut straight to the chase this month, blue screening almost as soon as it was installed. This proved a precursor to yet more blue screens on the on-access testing which was finally performed by deletion. The deletion method did show forethought in the choice of files to be deleted – Byway and DirII.A were not deleted despite being detected as viral. These two viruses act by inserting themselves in the directory structure and an infection fixed by simple deletion is surely a cure worse than the disease as it leaves data in a non-accessible form.

NAV’s slight instability on-access was presumably accentuated by the continuous stream of alerts generated, even when these were turned off at every mention in configuration. The on-access process also seemed to hang at several points, only to be reactivated by keyboard activity, which remains a most mystifying ‘feature’.

Having said all this, *NAV* turned in a characteristically good performance and certainly deserves its VB 100% award this month. It is also a distinctly user-friendly product. In terms of scan speed, *NAV’s* time test results place it within the respectably ‘average’ category.

VirusBuster VirusBuster v3.002

ItW Overall	96.3%	Macro	98.3%
ItW Overall (o/a)	93.5%	Standard	99.0%
ItW File	96.2%	Polymorphic	93.8%

Having tested the *NT* version of *VirusBuster* recently there were few problems anticipated when its turn came. Logging seemed to have become substantially harder to perform than in that review, and once more deletion was used as method of choice when testing scans.

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	2752	198739		53	1496863		927	171970	87	857557
Alwil AVAST32	352	1553784	1	300	264445		307	519272	298	250360
CA InoculateIT	329	1662407		29	2735647		205	777641	43	1735058
CA Vet Anti-Virus	658	831203		35	2266679		418	381379	75	994766
Command AntiVirus	457	1196788		33	2404053		499	319472	77	968928
DialogueScience DrWeb	889	615221	[25]	66	1202026	[1]	439	363135	77	968928
Eset NOD32	203	2694247	3	30	2644458		328	486026	52	1434759
F-Secure Anti-Virus	1802	303513.		56	1416674		1684	94665	330	226083
GDATA AntiVirusKit	515	1062004		51	1555564		280	569344	77	968928
GeCAD RAV	1337	409074		59	1344640		1003	158939	54	1381620
Grisoft AVG	683	800779	7	29	2735647		382	417320	64	1165742
Kaspersky Lab AVP	413	1324290		51	1555564		307	519272	75	994766
NAI VirusScan	677	807876		65	1220519		330	483080	84	888184
Norman Virus Control	689	793805		37	2144155		2483	64203	454	164333
Panda AntiVirus Platinum	672	813887	1	22	3606080		290	549712	49	1522601
SOFTWIN AVX	7756	70517		125	634670		2329	68448	146	511010
Sophos Anti-Virus	385	1420603		53	1496863		225	708518	63	1184245
Symantec Norton AntiVirus	569	961216		51	1555564		304	524396	61	1223073
VirusBuster VirusBuster	724	755431	18 [4]	25	3173350	[1]	500	318833	70	1065821

The product remains slightly behind the pack in terms of detection – changes are happening but they are fairly slow to be felt at present. Average scanning speeds are made up for by a reliable stability.

Conclusion

The products seem in many cases to have achieved the complexity of Windows NT with the stabilty of early versions of Windows 3.0. There is a place for products to achieve both stability and functionality, and those products which managed this took very little coaxing to produce good results. The products without stability are mostly associated with a constant push for more and better features, though is this really needed?

For some products the answer must be yes. The two great forces for constant change are *Symantec* and *NAI*, as a result of their pushing towards domestic sales – the domestic user is often swayed to an inordinate extent by a feature list. This acts as a further push to all other developers, and the features are included; whether they are the results of ego or marketing needs is irrelevant.

If this sounds all too familiar then it might well be because *NT* itself is subject to the same forces, responsible for such wonders as ‘VBS and VBA for all’. Those nasty users and their demands – they’re to blame for everything!

Technical Details

Test Environment: 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* with *Service Pack 5* applied. The workstations could be rebuilt from image back-ups. All timed tests were performed on a single machine that was not connected to the network for the duration of the timed tests, but was otherwise configured identically to that described above.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/2000/11test_sets.html.

A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

ERRATA

NT Comparative Update

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	11	98.44%	98.48%	191	95.16%	1144	80.09%	122	93.58%
Alwil AVAST32	1	95.65%	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.61%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	10	99.86%	768	91.10%	3	99.81%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	9	99.22%
DialogueScience DrWeb	0	100.00%	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t	n/t
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	1	99.93%	99.93%	0	100.00%	0	100.00%	21	99.71%
GDATA AntiVirusKit	23	0.00%	626	22.33%	21.71%	1488	60.82%	623	83.30%	34	98.26%
GeCAD RAV	0	100.00%	1	99.74%	99.75%	8	99.79%	0	100.00%	8	99.25%
Grisoft AVG	23	0.00%	3	99.60%	96.83%	12	99.74%	292	89.47%	46	97.22%
Kaspersky Lab AVP	23	0.00%	1	99.49%	96.72%	0	100.00%	0	100.00%	1	99.81%
NAI VirusScan	0	100.00%	1	99.93%	99.93%	0	100.00%	99	95.71%	8	99.85%
Norman Virus Control	0	100.00%	7	99.49%	99.50%	26	99.46%	300	90.40%	2	99.77%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	26	99.35%	889	89.69%	52	98.21%
SOFTWIN AVX	23	0.00%	2	99.68%	96.90%	2	99.99%	56	94.36%	77	96.59%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	13	99.66%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	264	94.74%	18	99.44%
VirusBuster VirusBuster	1	95.65%	25	96.55%	96.53%	66	98.34%	292	93.77%	10	99.01%

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	9	98.58%	98.62%	191	95.13%	1144	80.09%	117	93.92%
Alwil AVAST32	0	100.00%	0	100.00%	100.00%	31	99.21%	28	95.36%	13	98.93%
CA InoculateIT	0	100.00%	0	100.00%	100.00%	0	100.00%	9	98.87%	2	99.61%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	178	96.37%	0	100%
Command AntiVirus	0	100.00%	3	99.78%	99.79%	0	100.00%	1	99.98%	13	99.23%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
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%	1	99.49%	99.50%	0	100.00%	0	100.00%	2	99.71%
GeCAD RAV	0	100.00%	1	99.74%	99.75%	8	99.79%	0	100.00%	8	99.25%
Grisoft AVG	0	100.00%	2	99.49%	99.50%	11	99.71%	124	92.01%	30	98.67%
Kaspersky Lab AVP	0	100.00%	1	99.49%	99.50%	0	100.00%	0	100.00%	1	99.81%
NAI VirusScan	0	100.00%	1	99.93%	99.93%	0	100.00%	17	97.87%	7	99.86%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	286	91.23%	0	100.00%
Panda AntiVirus Platinum	0	100.00%	0	100.00%	100.00%	26	99.35%	889	89.69%	50	98.34%
SOFTWIN AVX	0	100.00%	2	99.68%	99.69%	2	99.95%	55	94.36%	63	97.07%
Sophos Anti-Virus	0	100.00%	1	99.93%	99.93%	13	99.65%	191	95.24%	14	99.55%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	264	94.74%	16	99.46%
VirusBuster VirusBuster	0	100.00%	25	96.55%	96.65%	66	98.34%	292	93.77%	10	99.01%

Regrettably, last month's *NT* Comparative contained a number of minor errors which, in turn, raised several issues regarding testing. The mistake which has the least effect upon the figures is, ironically, that which is in most urgent need of correction. Hawk-eyed developers at *Aladdin Knowledge Systems* pointed out that the ItW non-detection of Byway by *eSafe Desktop* showed a problem with the test-sets, since this virus should not have been on the WildList for September 2000.

The test-sets and WildLists were examined and the root of the problem found to be slight inconsistencies in the WildList relating to some of the viruses which, like Byway, had dropped out of the main WildList that month. This resulted in the incorrect version of data being used. This did not, in the majority of cases, affect detection rates by more than a fraction of a percent and virus collection upkeep has been safeguarded against future repetitions. This did not affect VB 100% award ratings, or any tests other than this. The charts here correct this matter and present the final results as they should have been.

There were also some problems while testing *DialogueScience's DrWeb* which affected the results here and raised important issues as to the *VB* testing protocol. Errors in testing resulted in *DrWeb* being erroneously declared to miss files which it did indeed detect. This leaves it with 100% detection of files, though this required a certain degree of tweaking. Under current protocol it is thus denied a VB100% award. The figures in these charts reflect results for default settings rather than detection capability, the same being the case for *AVAST32*.

Since the failure in these cases to gain a VB100% award is by design rather than inefficiency, it has been decided to implement new tools to provide testing of these products in default mode. Details of this change in protocol will be announced in the next Comparative.