COMPARATIVE REVIEW

Windows of Opportunity

Another *Windows 95* comparative. We hear you asking: Can it have been six months already? Well, technically it is, but it is less than that since *Virus Bulletin* published the last *Windows 95* comparative. A major contributory factor to the delay in publication of that review was that more than a few fairly major annoyances made themselves felt during testing. Then, while compiling the final results for publication, it seemed that re-testing some products under the same conditions would lead to different results. This was most perplexing, and after failing to resolve why some products behaved like this, we eventually published results that were typical of those seen in the actual tests.

That was not an ideal situation. This time we are playing truth or dare. The vendors who dared submit poorly tested or otherwise inadequate products may not like the truth revealed through the pages of this review. *C'est la vie*.

A reviewer's job is to review. A developer's job is to develop. It seems that some developers believe they can do their job without testing their products, or at least, they believe they need not test their products as thoroughly if they are making a special build to send out for review or testing. That seems a little like Russian Roulette to us, but from a developer's perspective it can make sense.

Anti-virus developers are always under pressure. There are always new viruses to add detection of to one's product. There are sometimes new forms of virus (as in recent months we have seen *mIRC* script, *Excel* formula and *Access* macro viruses arise – all covered in *VB*, April 1998, as chance would have it). The latter can add a significant burden to product developers, who now face possibly having to reverse-engineer a new file format, understand how another part of an OS works, and so on. However, developers are also under pressure to meet promises made to their marketing and sales departments – all those additional and better features, the nicer shade of blue in the splash screen and so on.

Possibly the worst pressure is that 'large new sale' that 'looks promising, so long as we have another good review'. *Virus Bulletin* has had subtle, and at times not so subtle, pressure applied by various vendors to 'test the newer version' so their product looks better in a comparative review. Just days before going to print with this issue, a senior executive at one of the major anti-virus developers said, almost tangentially to our conversation, 'you *do* know the latest updates are on our web site?'.

Unfortunately for us as testers, it appears that many developers yield to these sorts of temptations. We see products with quick fixes and many, perhaps not fully-tested, new virus definitions thrown in right up to the product submission date for the review. At that point, the developer burns a gold CD-ROM and writes the new version number on it with a marker pen.

This is not a complaint about gold CDs *per se* – many perfectly fine products arrive here in such a form, and it is understandable that with the product submission date for comparatives usually just a few days before the end of a month, some vendors may still be waiting to receive their product back from their reproduction plants.

It *is* a gripe about shoddiness. As potential purchasers of these products, *Virus Bulletin's* readers are entitled to see the warts. What follows is the 'no holds barred' version of a *Windows 95* comparative review. Not describing what goes into producing the apparently simple and sane statistics we usually publish does no-one any good in the long run. In the course of performing the current review, it was decided that as the warts finally outweighed the clear complexions, it was time to tell it like it is.

Test Procedures

At the end of February, a total of twenty-two products were submitted for testing, however, one of these proved completely untestable. As the February WildList was released a little later than usual that month (late on the last day the developers had for shipping their products to *VB*), the In the Wild Boot and File test-sets used for testing were updated to the January WildList.

The products were tested following individual installation on standard *Windows 95* workstations. These have their hard drives restored from sector-level backups between products. To ensure the integrity of the virus test-sets, they were stored on a *NetWare 3.11* server and the tests were run by a user who only had read and file-scan rights to the test-set directory.

For the on-demand detection tests, wherever possible, complete reports or detection logs were produced by the program under test, and then parsed for infection reports. In some cases this was either not possible or seemed to provide anomalous results. In these instances, the test-sets were copied to the test machines' hard drives and the software set to delete infected files. The samples remaining were deemed 'missed'.

On-access detection was also normally tested against the undisturbed samples on the server. To test this increasingly important mode of operation, the on-access component of the product under test is configured appropriately ('silent mode' is used if available, and the action on detection is set to deny access). Then a simple *Windows* program is employed. It runs through a directory tree trying to open all

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	87	100.0%	655	100.0%	100.0%	1134	98.7%	12998	95.4%	906	100.0%
Cheyenne Inoculan	86	98.9%	654	99.9%	99.5%	1021	89.1%	12679	91.7%	906	100.0%
Command AntiVirus	87	100.0%	621	97.6%	98.4%	988	86.2%	6968	47.0%	817	92.7%
Cybec VET	84	96.6%	655	100.0%	98.8%	1091	95.0%	13498	99.1%	900	99.3%
Data Fellows F-Secure Anti-Virus	87	100.0%	655	100.0%	100.0%	1142	99.3%	13499	99.1%	906	100.0%
Dr Solomon's AVTK	87	100.0%	655	100.0%	100.0%	1138	99.0%	13500	100.0%	906	100.0%
EliaShim ViruSafe	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
ESET NOD32	87	100.0%	655	100.0%	100.0%	1127	98.1%	13500	100.0%	906	100.0%
GeCAD RAV	85	97.7%	620	97.5%	97.6%	1134	98.7%	13495	99.0%	868	96.7%
IBM AntiVirus	87	100.0%	655	100.0%	100.0%	1122	97.6%	13500	100.0%	906	100.0%
iRiS AntiVirus	86	98.9%	654	99.9%	99.5%	1056	92.1%	13083	94.0%	906	100.0%
Kaspersky Lab AVP	87	100.0%	655	100.0%	100.0%	1146	99.7%	13500	100.0%	906	100.0%
McAfee VirusScan	87	100.0%	655	100.0%	100.0%	1130	98.3%	13441	98.7%	888	98.8%
Norman ThunderByte	87	100.0%	655	100.0%	100.0%	1115	97.0%	13496	98.1%	883	98.1%
Norman Virus Control	87	100.0%	646	99.7%	99.8%	1120	97.4%	13495	99.0%	899	99.7%
Panda Antivirus	87	100.0%	628	96.2%	97.5%	833	72.4%	9344	68.6%	660	80.8%
Quarterdeck ViruSweep	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
Sophos SWEEP	87	100.0%	644	99.4%	99.6%	1107	96.4%	13495	99.0%	904	99.7%
Stiller Integrity Master	85	97.7%	618	96.6%	97.0%	856	74.8%	5044	32.7%	743	85.6%
Symantec Norton AntiVirus	87	100.0%	655	100.0%	100.0%	1119	97.4%	12001	88.0%	891	99.1%
Trend Micro PC-cillin 95	83	95.4%	648	98.7%	97.6%	1053	97.4%	12964	94.2%	884	98.5%

files it finds (and closing them when successful). This utility logs file-open errors, and as no other programs are running concurrently and the test is run after a restart, errors are presumed the result of the scanner under test.

One test machine is reserved for timing and overhead tests. In this case, the Clean test-set is stored on the local hard drive and the workstation is disconnected from the network and restarted standalone. Elapsed scanning time is measured with a digital stopwatch. The overhead tests involve copying 200 executable files (part of the Clean test-set) from one directory to another on the workstation. A baseline measurement is made with all active components disabled (unloaded if possible) and then repeated with various configuration options enabled. Tests are repeated ten times under each condition, and an average recorded. The results for each product are normalized to 20 seconds for the baseline condition, before graphing.

The boot virus samples are all kept on write-protected, 3.5-inch diskettes. On-demand testing is performed from the test product's user interface. On-access detection tests are generally made by attempting to access the infected diskettes from the *Windows* Explorer (by clicking the appropriate drive icon). All manner of tricks have been found necessary to persuade the combination of *Windows*, Explorer and certain products to acknowledge that the diskette in the drive has changed. These include multiple

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	87	100.0%	n/a		n/a	n/a		n/a		n/a	
Cheyenne Inoculan	84	96.6%	654	99.9%	98.7%	1021	89.1%	n/t		906	100.0%
Command AntiVirus	87	100.0%	621	97.6%	98.4%	988	86.2%	6969	47.1%	817	92.7%
Cybec VET	77	88.5%	655	100.0%	96.1%	1091	95.0%	13498	99.1%	900	99.3%
Data Fellows F-Secure Anti-Virus	87	100.0%	635	97.0%	98.0%	1075	93.6%	13499	99.1%	906	100.0%
Dr Solomon's AVTK	87	100.0%	655	100.0%	100.0%	1146	99.7%	12922	90.3%	906	100.0%
EliaShim ViruSafe	86	98.9%	653	99.9%	99.5%	995	86.9%	13163	95.4%	906	100.0%
ESET NOD32	85	97.7%	655	100.0%	99.2%	1127	98.1%	13500	100.0%	906	100.0%
IBM AntiVirus	63	72.4%	496	79.0%	76.8%	884	77.4%	0	0.0%	124	12.2%
iRiS AntiVirus	84	96.6%	654	99.9%	98.7%	1056	92.1%	n/t		906	100.0%
Kaspersky Lab AVP	87	100.0%	655	100.0%	100.0%	1146	99.7%	13500	100.0%	906	100.0%
McAfee VirusScan	51	58.6%	655	100.0%	85.9%	1067	92.9%	13275	93.2%	888	98.9%
Norman ThunderByte	84	96.6%	593	90.8%	92.8%	859	75.0%	n/t		897	99.3%
Norman Virus Control	82	94.3%	n/a		n/a	1143	99.4%	n/a		n/a	
Panda Antivirus	59	67.8%	560	87.5%	80.8%	837	72.7%	n/t		541	71.1%
Quarterdeck ViruSweep	83	95.4%	653	99.9%	98.4%	995	86.9%	13163	95.4%	906	100.0%
Sophos SWEEP	87	100.0%	653	99.4%	99.6%	1107	96.4%	13495	99.0%	904	99.7%
Symantec Norton AntiVirus	86	98.9%	655	100.0%	99.6%	1126	98.0%	13500	100.0%	906	100.0%
Trend Micro PC-cillin 95	83	95.4%	642	97.2%	96.6%	1034	90.2%	n/t		883	98.4%

disk swaps, accessing the drive from other applications and intermingling several non-infected diskettes among the sample diskettes.

So, how did everyone fare? Read on…

Alwil AVAST32 v7.70 (Build 702)

ItW Boot	100.0%	Macro	98.7%
ItW File	100.0%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	95.4%
ItW Overall	100.0%	Standard	100.0%

AVAST32 provided a quiet beginning to this review, along with what came to seem like the unfamiliarity of a product which performed generally as advertised. Its dedication to the purpose at hand – detecting viruses – is justly rewarded with the first VB 100% award in this comparative review. *AVAST32* has an active component, but as we have noted in previous comparatives, *Virus Bulletin* is not geared-up to test products whose active components (reputedly) intercept infected programs at load-and-execute time. This 'limitation' has not changed, so only boot detection has been tested with on-access methods.

The usual collection of beetles graced *AVAST32's* virus alerts, and their only oddities were the boot sector results. The alerts are meant to inform you whether they are due to on-access or on-demand scanning, but if both are operating, confusion is often the result. On occasion, the on-access scanner produced alert boxes that did not have system focus, and were thus invisible behind the on-demand menu. This could only be produced reliably with MISiS, when the message 'a device attached to the system is not functioning' appeared upon scanning.

Another small problem was found, in that AVAST32's log files always seemed truncated or to just completely miss reporting a block of files that the on-screen status monitor had clearly shown being scanned (and found infected). It is suspected that this behaviour may be related to the log file size limitation option. Various settings, from just larger than necessary to many megabytes, did not substantially alter things here. Eventually, the full test-set was copied to the test machine and *AVAST32* asked to delete all infected files.

Cheyenne Inoculan v5.0 (Build 064)

ItW Boot	98.9%	Macro	89.1%
ItW File	99.9%	Macro on-access	89.1%
ItW File on-access	99.9%	Polymorphic	91.7%
ItW Overall	99.5%	Standard	100.0%

Inoculan managed, in the face of stiff competition, to be one of the most frustrating products yet received. Primary in this was its inability to produce any form of report file – binary log files were to be found in the program directory, but no option to produce plain-text or hard-copy reports was evident. Gobsmacked at such an omission, the reviewer assumed he was missing a subtlety in a menu somewhere. Unfortunately, recourse to the on-line help provided no relief – despite being clearly the English version, the review copy of the product was supplied with help files universally written in German! Nice and fully context-sensitive (as far as we could judge with our rudimentary grasp of that language), but nevertheless completely in German.

Perhaps we should have expected such quality from the outset, given that the first screen displayed by the installation program referred to the product as 'Incoulan'. A quality assurance program that does not prevent the misspelling of the product's name could almost be forgiven for providing only alternative-language help files.

Fortunately, an *Adobe Acrobat* PDF file of the English manual was discovered on the gold CD-ROM on which the product arrived. However, after some trolling around, it seemed that reporting the results of a scan was a capability beyond the scope of this version of the product.

On-demand boot sector testing was difficult, due to the product's insistence on performing memory checks prior to checking each diskette. Theoretically, this action could be disabled, but it was spontaneously reset by every virus detection that occurred. This is triggered by the product's default setting, which, upon detection of a virus, will set 'options for highest level of detection for 30 days'.

This seems like a good setting – in theory it increases a user's level of protection once evidence of greater risk is detected. It could be a nuisance in some situations though, unless it can be disabled. In fact, the option that claimed to enable and disable this escalation feature made no difference to performance – on detecting a boot virus, memory scanning was re-enabled. If the memory scan option was not manually deactivated after such a detection, there was a high likelihood the previous virus would be (technically erroneously) detected in memory before scanning the next sample diskette. When this happened, *Inoculan* insisted 'Virus in memory – Reboot with rescue disk'. It was thought that clicking the OK button then closing and restarting *Inoculan* would probably suffice at this point, but it transpired that the supposed warning message (just described) is, in fact, a request from *Inoculan* to restart the machine. As there was only an OK button, it was very onerous when one forgot to disable memory scanning between boot virus detections.

Attempts to test on-access detection across the *Virus Bulletin* collection resulted in a series of reboots and hangs. This could only be resolved, as in several other cases in this review, by splitting the collection into smaller chunks to be scanned separately, interspersing each test chunk with a system restart. Even so, the Polymorphic test-set remained untestable – it would appear that if you have more than a few hundred files infected with a polymorphic virus, you will have to run this product many times and with much finagling of options and locations to scan to obtain a clear picture of the extent of the 'damage'.

Inoculan also managed to have the worst problem with the Clean test-set. A simple false alarm was not lowly enough for *Inoculan*, however – it crashed completely upon scanning a particular file in the test-set. Replacing that file with one of very similar size saw *Inoculan* limp across the line with a time of 1931 seconds and a data throughput rate of 276 KB/second.

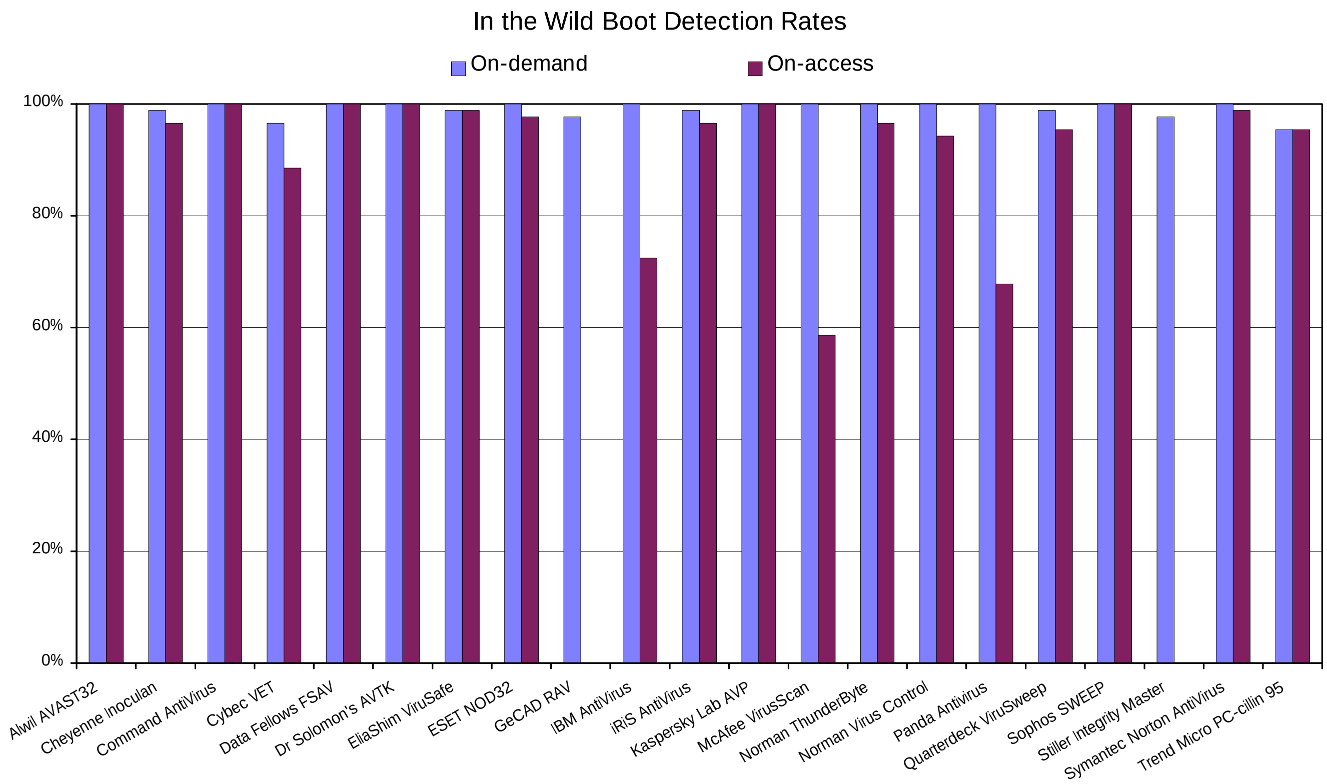
Given that *Microsoft* is known to license *Inoculan* as its corporate-wide anti-virus solution, *Virus Bulletin* hopes the reviewed product is not truly indicative of the anti-virus development efforts at *Computer Associates* since it took over *Cheyenne* (and thus the *Inoculan* product).

Command AntiVirus v4.0

ItW Boot	100.0%	Macro	86.2%
ItW File	97.6%	Macro on-access	86.2%
ItW File on-access	97.6%	Polymorphic	47.0%
ItW Overall	98.4%	Standard	92.7%

Command AntiVirus (*CAV*) proved a strange creation, but did not really qualify for the big league of irritations encountered elsewhere. Boot sector detection was good with 100% detection rates for both on-demand and on-access scanners. However, the program managed to detect a large number of the boot sector viruses *twice* on-access, despite only one method of scanning being active. Performance on all the other test-sets continues to slip with the newer *Word 97* macro viruses being especially challenging.

The product proved deceptive in other areas – the tray icon, which looked like a marker for the on-access scanner, was in fact a shortcut to the whole program. This 'feature' is not



unique to *CAV*, but it caused initial confusion. In another common flaw, the progress bar bore no resemblance to reality in the on-demand scans, and was far too pessimistic. In terms of stability, this product was not the worst offender, but it certainly managed to distress Explorer into a comatose state on more than one occasion.

CAV lacked a proper silent mode for its on-access scanner. Initially, we thought its insistence on popping system modal dialog boxes and freezing the machine until a key was pressed and released would have it register a 'not tested', at least on-access against the Polymorphic test-set (we have some respect for our keyboards!). Similar Registry tweaks as were found to work around the same issue with the *Data Fellows* product (see below), also worked with *CAV*, allowing full testing.

Cybec VET v9.70

ItW Boot	96.6%	Macro	95.0%
ItW File	100.0%	Macro on-access	95.0%
ItW File on-access	100.0%	Polymorphic	99.1%
ItW Overall	98.8%	Standard	99.3%

VET has had something of a facelift. The smart new packaging projects a more up-market image, and there is a clear effort to incorporate this throughout the product, with new program icons, splash screens and the like all blending with the new look. Initial attempts to configure the on-access component to scan boot sectors seemed doomed to failure. Enabling this option (which was supposedly enabled after installation) and rebooting (it requires the loading of a static VxD), repeatedly produced the rather puzzling message on the program's configuration screen that the option was enabled and would be activated following the next restart.

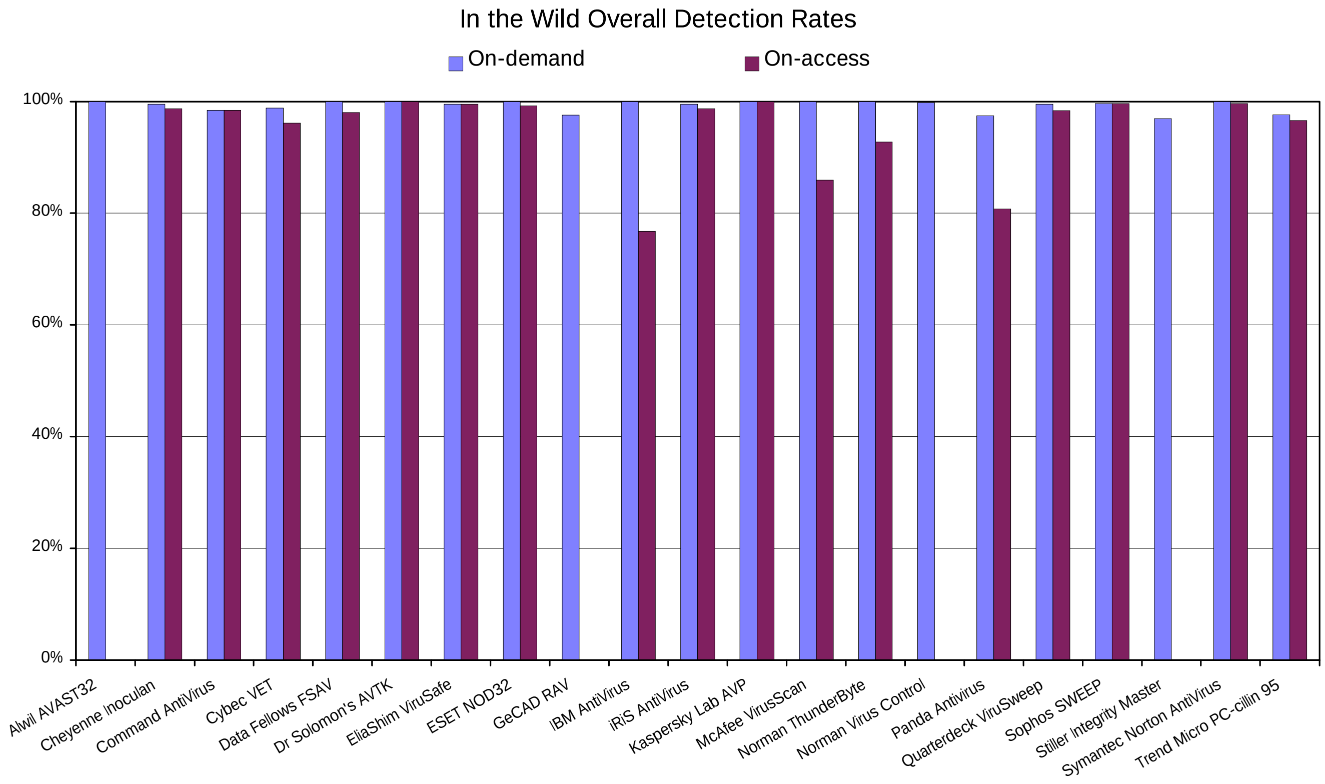
After several discussions with *Cybec's* technical staff, the required VxD was found where it should be and the Registry settings were confirmed as correct. *VB* staff noticed however, that the VxD deposited by the installation process consisted of approximately 17 KB of null characters. The offending item having been replaced and the machine restarted, all came right.

Another bug discovered during testing was that whenever a log file was directed outside the default *VET* directory by typing the full path into the provided entry field, this path would be modified by prepending C:\VET, resulting in several invalid paths (and, we suspect) some of the instability we saw earlier in our attempts to test the product. Using the browse button to specify an alternative path to the log file or closing *VET*, editing the associated Registry setting and restarting the machine 'fixed' this problem.

Cybec is certainly unique among anti-virus developers in offering health care tips for aardvarks in its manuals!

Data Fellows F-Secure Anti-Virus v4.0

ItW Boot	100.0%	Macro	99.3%
ItW File	100.0%	Macro on-access	93.6%
ItW File on-access	97.0%	Polymorphic	99.1%
ItW Overall	100.0%	Standard	100.0%



This is the first time that a multi-engined version of *F-Secure* has featured in a *Virus Bulletin* review, comparative or otherwise. The new product has improved detection over its forerunner and garnered a VB 100% award for its efforts against the In the Wild test-sets. In a previous *Virus Bulletin* test of *F-Secure's* forerunner, the product had some minor stability problems. It seems the subsequent addition of the second engine may have compounded this, although the use of the *AVP* engine is responsible for the significant improvement in detection. That said, the difficulty here is not so much finding problems, as deciding where to start.

Fortunately, as the developers provided an invalid icon offset in the AUTORUN.INF, this allows us to start at the very beginning. This aesthetic bug means that when the CD-ROM is in the drive, Explorer displays an icon usually used with files having no associated application. Not an inspiringly professional look, and this was not a gold CD.

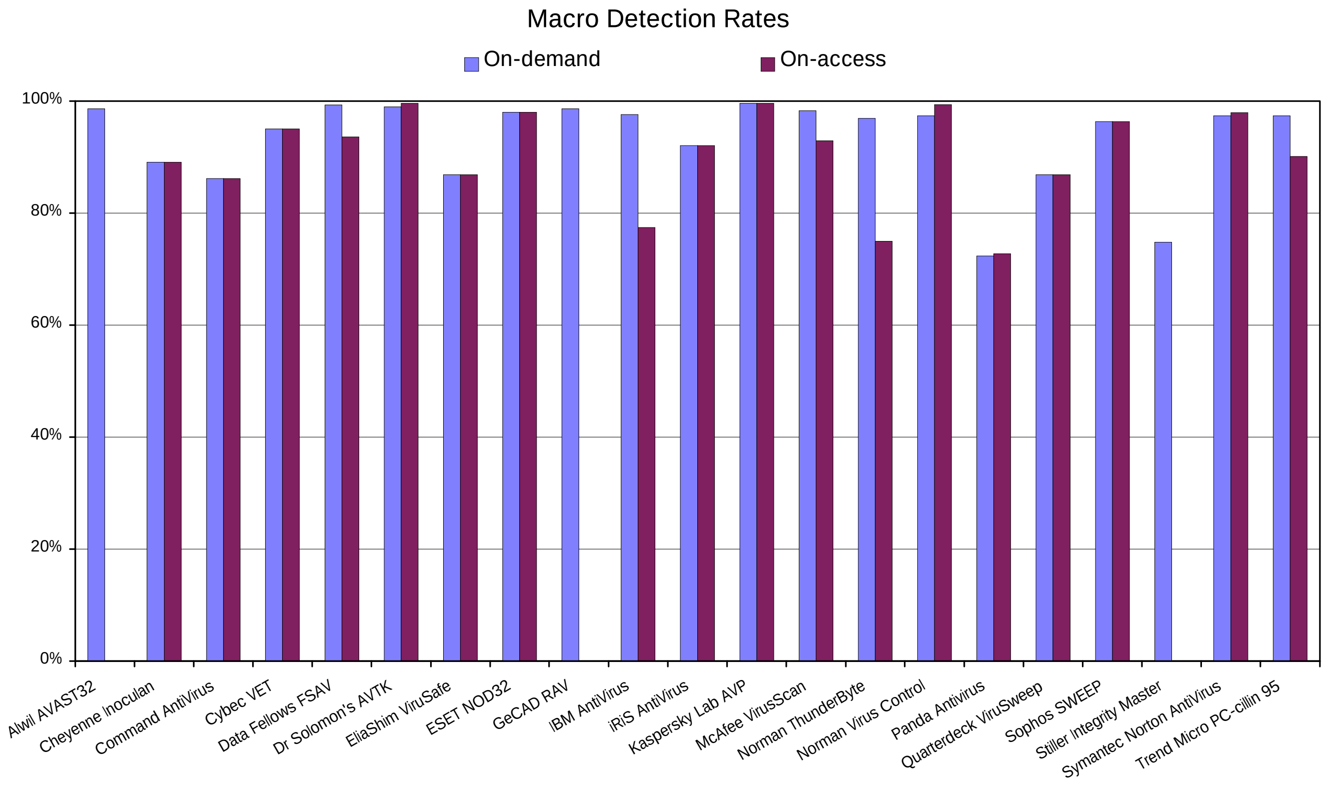
The on-demand scanner was the first tested, and this crashed with great gusto when presented with any significant number of objects to scan. It also proved impossible to scan single files, or indeed to scan more than one branch of a directory tree at one time, though this was due to poor design rather than any errors in the underlying code. One possible cause of the stability problems might be the gargantuan report files, with the two engines each having their say in the case of each file. Entertainingly, this results not only in the detection of more viruses than there are files, but also in the impossibility of knowing at first glance how many files were considered infected. Oh joy.

Related to the design limitation of not being able to scan more than one tree at a time is the fact that there is no browse button on the location to scan field. This omission means that if attempting to scan partial trees, rather than whole drives, one has to type the full path correctly. This should not be a problem, but *F-Secure* does not warn you if an invalid path is entered, and replaces the setting with a weird, semi-random (and still usually invalid) path consisting of some of what was entered and some sub-strings from previous settings.

When scanning directories which did not exist, *F-Secure* performed some madcap antics, and scanned seemingly random paths. As it appeared the log file was not written until scanning ended, the general instability of the program meant that obtaining log files was a hit and miss affair.

So, on to the on-access scanner, which refused to implement one of its options at all. The scanner, without fail, reset itself from merely reporting infections to requiring confirmation and thus a keystroke or mouse click was needed for each virus found. This difficulty was compounded by there being two possible locations to input on-access options, which nevertheless did not necessarily contain the same settings. Unattended testing of the on-access scanner only became possible following discussions with *Data Fellows* technical staff and the manual resetting of some undocumented Registry entries.

The boot sector tests were less fraught affairs. The double declaration of infection continued as an irritation, except in the case of ABCD which was only detected once.



Dr Solomon's AVTK v7.81

ItW Boot	100.0%	Macro	99.0%
ItW File	100.0%	Macro on-access	99.7%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

The *Anti-Virus Toolkit* is beginning to look rather old-fashioned and lacking in options compared to some of the other products on show this month, and had more than its usual quota of problems in this review. However, despite this, it still obtained a VB 100% award.

The on-access scanner was at the root of several problems, insisting upon a reboot at every change of options. Whilst not entirely unexpected, this seems a little too much when the only option changed is the state of report file logging. This component is surely implicated in the problems seen in the on-access boot sector tests, where instability was the order of the day. On-access detection resulted in a notification of infection, followed by a dialog box, apparently of the *Toolkit's* devising. If the diskette was removed from the drive at this point and the retry option chosen, a system hang ensued.

EliaShim ViruSafe 95 v2.6

ItW Boot	98.9%	Macro	86.9%
ItW File	99.9%	Macro on-access	86.9%
ItW File on-access	99.9%	Polymorphic	95.4%
ItW Overall	99.5%	Standard	100.0%

A product displaying no stability problems at all was a great pleasure in this comparative. The multilingual nature of *eSafe Protect* is outdone by this, its sister product, which boasts eight languages to choose from, presumably a number set to increase in future.

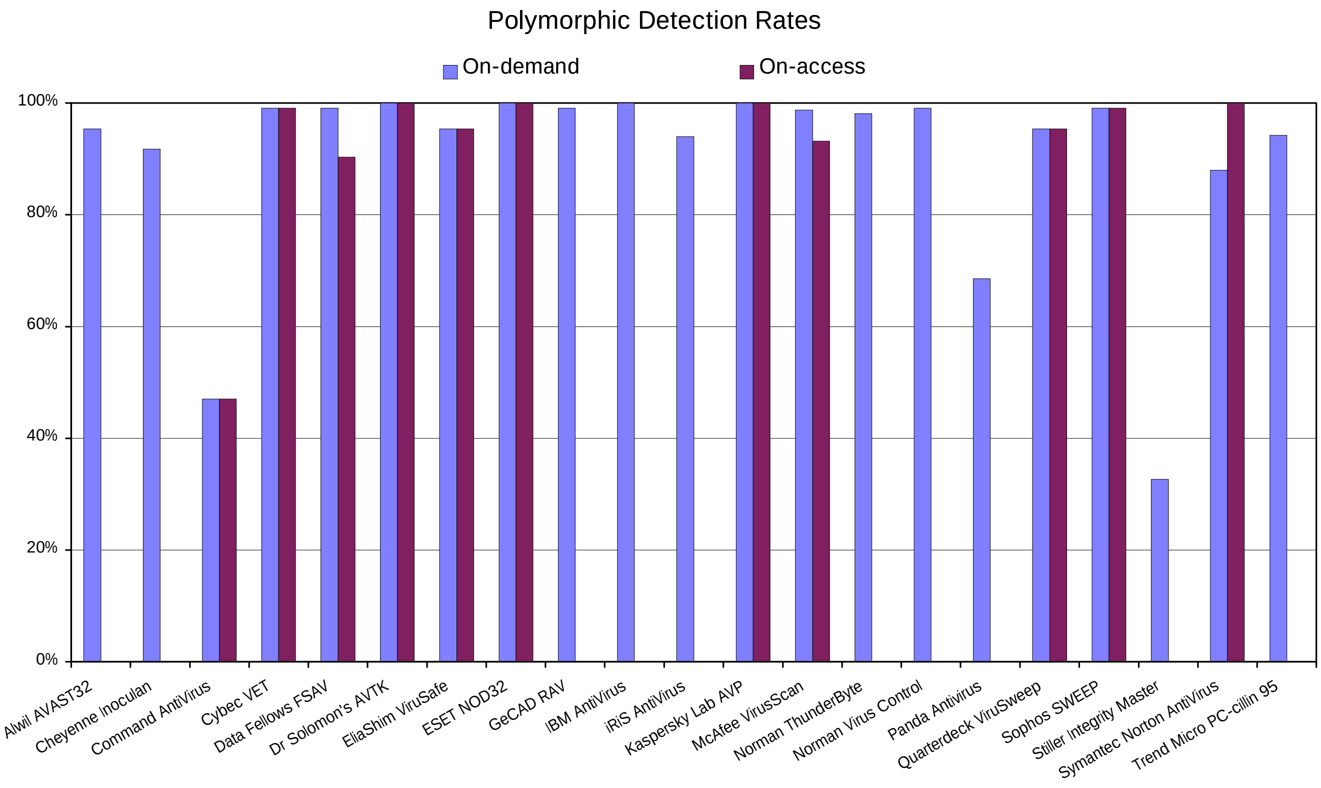
The default scanning configuration installs not only a DOS mode TSR, but also a pre-*Windows* DOS TSR. Again, similar to *eSafe Protect*, there exists an option for a rescue disk, though this is far better documented in the *ViruSafe* manual than in the former product.

Detection results are much on a par with its performance in recent comparatives. Although the *ViruSafe* engine is at the heart of *Quarterdeck's* new *ViruSweep* (see below) – obtaining exactly the same detection in these tests – it seems unlikely that the stability problems with the latter product are due to the *ViruSafe* engine code.

ESET NOD32 v1.00

ItW Boot	100.0%	Macro	98.1%
ItW File	100.0%	Macro on-access	98.1%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

ESET has produced all-new graphics for their *Windows 95* product, though thankfully not at the expense of all-new stability problems. Better yet, detection has been boosted to VB 100% levels in the In the Wild test-set and were tantalizingly close to a clean sweep.



Perhaps not surprisingly, boot sector testing is the area where problems can be found. There were problems for *NOD32* in detecting that disk changes had occurred, leading to very inconsistent detection if the same infected diskette was presented over and over.

On-demand scanning, however, is particularly pleasant to perform, with a full implementation of shortcut keys combined with the holding of focus on those buttons most convenient for scanning a pile of diskettes. The 'directory path a:\ is not valid' messages triggered by diskettes with 'strange' BPBs did not disrupt this convenience, which was topped by the full on-demand detection of the viruses in the Boot Sector test-set. Those same samples prevented *NOD32* from achieving 100% on-access boot detection.

GeCAD RAV v5.22

ItW Boot	97.7%	Macro	98.7%
ItW File	97.5%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	99.0%
ItW Overall	97.6%	Standard	96.7%

The Romanian contingent of this comparative proved far more stable than some of its big name cousins, with only false positives and the lack of on-access scanning as notable concerns. The performance is improving compared to recent outings in *VB* comparatives. The setup provided the only anxious moments, with the program warning that a certain DLL needed to be updated. It is peculiar that, although not mentioned as available, the DLL in question is on the DOS scanner disk supplied with the product.

IBM AntiVirus v3.02bc

ItW Boot	100.0%	Macro	97.6%
ItW File	100.0%	Macro on-access	77.4%
ItW File on-access	79.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

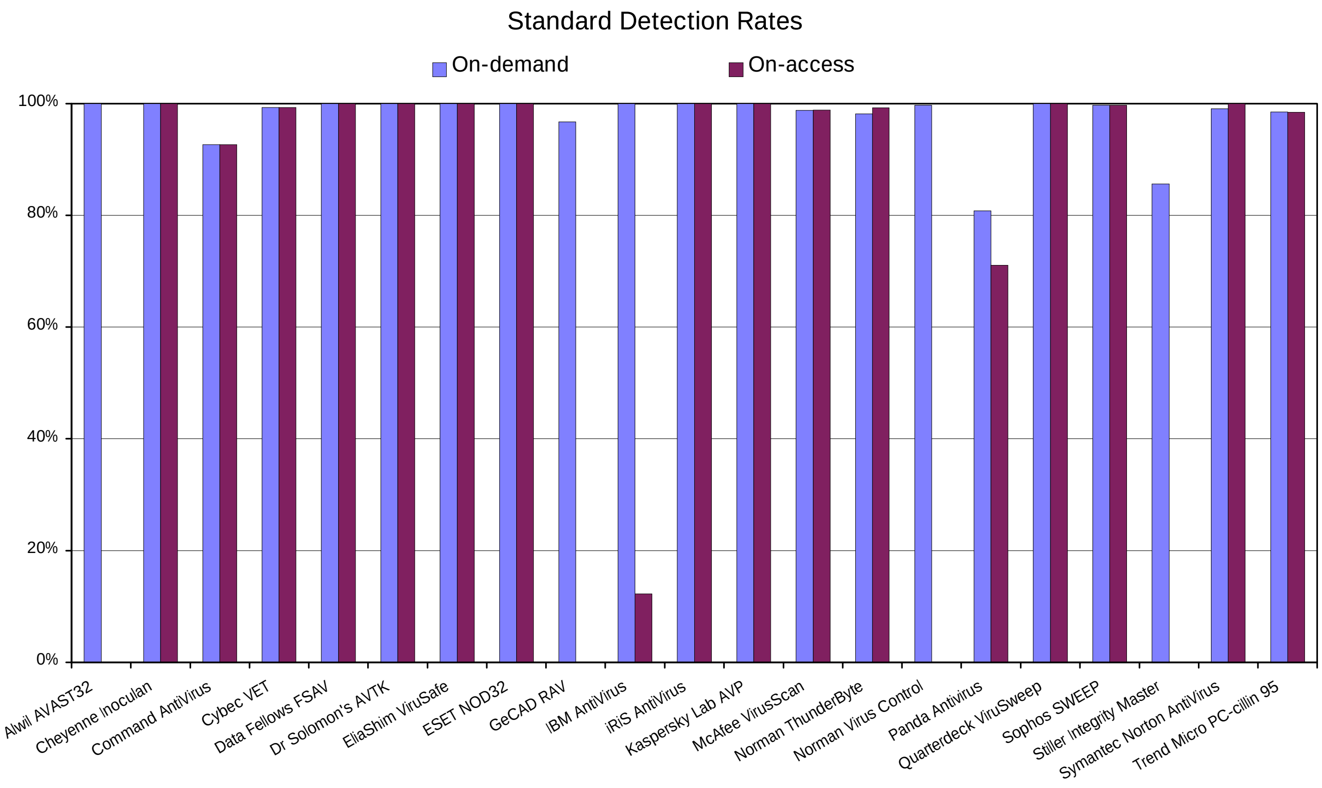
IBM's product proved trickily unstable in the on-demand file tests, which were prone to lock ups when scanning any sizeable number of files whilst logging. The convoluted method in which these log files must be confirmed as to action, in as many as a dozen passes, was not a little distressing.

Worse was to come in the on-demand boot sector scan, where although no viruses were missed, the process of confirming actions took four mouse clicks to perform for each virus. On-access, the boot sector viruses were detected poorly, and some way through testing the dialog box became hidden behind Explorer and was replaced by a blue screen alert. This alert, however, took some five seconds or more to appear and made no friends at all.

iRiS AntiVirus v22.06

ItW Boot	98.9%	Macro	92.1%
ItW File	99.9%	Macro on-access	92.1%
ItW File on-access	99.9%	Polymorphic	94.0%
ItW Overall	99.5%	Standard	100.0%

As stable as a sandcastle submerged at high tide, the degree to which quality assurance has been applied to this product would appear to be negligible. Anti-virus software which



cannot scan a clean *Windows* directory successfully is beyond this reviewer's comprehension. Despite having a pretty interface, all was lost by the contortions required to perform any successful action, though admittedly some of the crashes did produce impressive visual pyrotechnics. The clean scan crashed, a scan of C: drive crashed – the contents being only *Windows 95* and *iRiSAV* itself, a total of 72 MB. Still, *VB* persevered. Experimenting with the use of the sig files (provided with an older and more stable front end) failed to aid matters, as the two were incompatible.

The boot sector tests too, proved far from ideal. On-demand scanning reproducibly failed to detect infections at the first attempt, though a second attempt would often make *iRiSAV* aware that a problem existed. This was highlighted by the virus Baboon – detected once during fifteen accesses.

Kaspersky Lab AVP v3.0.119

ItW Boot	100.0%	Macro	99.7%
ItW File	100.0%	Macro on-access	99.7%
ItW File on-access	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	100.0%

With a review of this very same product elsewhere in *VB* this month, there is little but a summary that can be added to the words there. *AVP* behaves as it should under the test conditions, and easily detects sufficient viruses to qualify for a VB 100%. *Kaspersky Lab* will no doubt be aiming for complete detection in all categories in the next comparitive, with a good chance of success.

McAfee VirusScan v3.15.3103

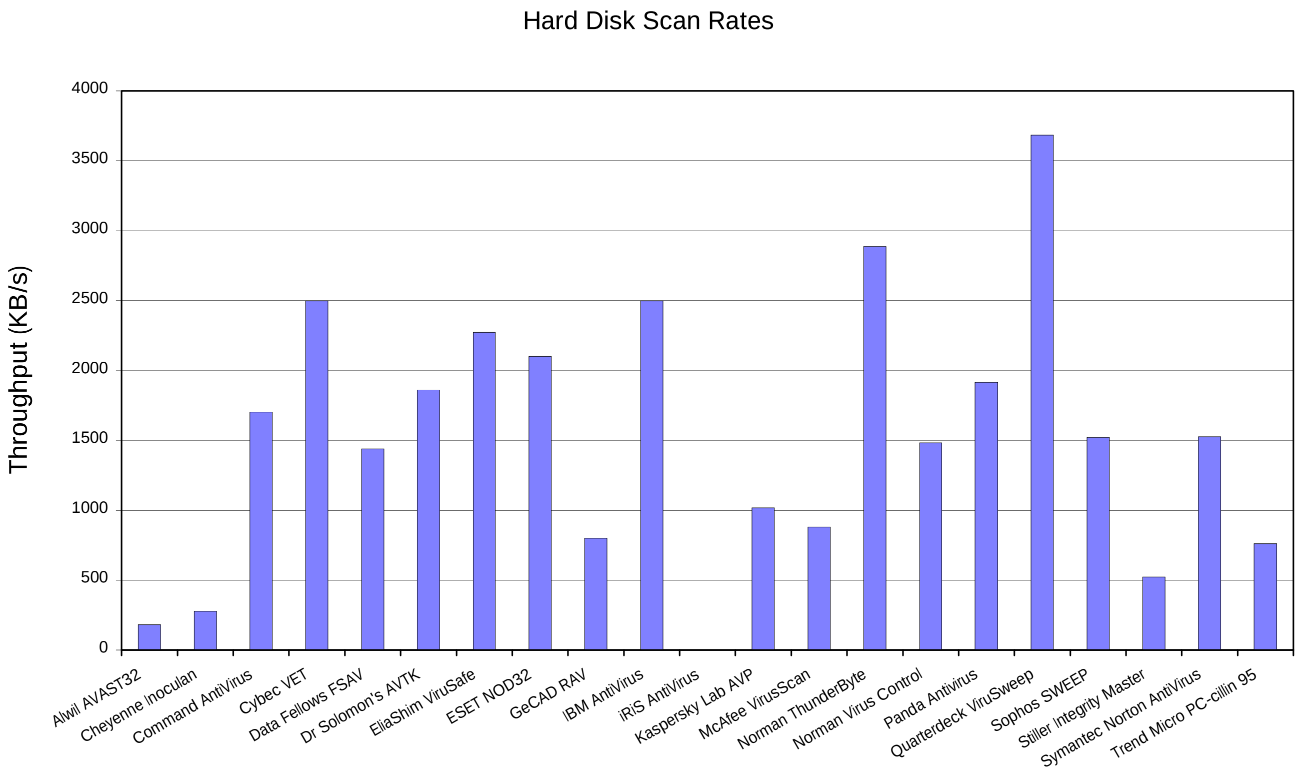
ItW Boot	100.0%	Macro	98.3%
ItW File	100.0%	Macro on-access	92.9%
ItW File on-access	100.0%	Polymorphic	98.7%
ItW Overall	100.0%	Standard	98.8%

The problems encountered by *VirusScan* in the last boot tests seem to have been swiftly overcome, and on-demand scanning of boot sector diskettes was comprehensive, though not always at the first attempt. On-access, however, boot sector viruses proved elusive, with over one third remaining undetected. The *NT* stability problems seemed to a great degree banished.

Norman ThunderByte AntiVirus v8.05

ItW Boot	100.0%	Macro	97.0%
ItW File	100.0%	Macro on-access	75.0%
ItW File on-access	90.8%	Polymorphic	98.1%
ItW Overall	100.0%	Standard	98.1%

TBAV is stable, and its only faults lie in areas irrelevant to the average user, but still caused some problems in the review process. More relevant is the time taken to install *TBAV*. The installation process begins by a scan of all local drives, followed by a checksum of those drives. On the *VB* test machine with a moderately laden drive this two pass process took over an hour. This, however, is unlikely to be a problem except on the busiest or most vital of workstations.



Similarly, the lack of a quiet mode on the active i/o monitor made testing problematic. It was noteworthy that the production of a modal blue screen or modal information box seemed to occur almost completely at random.

These niggles are slight – *TBAV* was the speediest product to check multiple disks, as it was placed in a mode where the A: drive was constantly accessed, and scans any disk inserted. As new disks are always scanned, this makes scanning a matter where no keyboard input is required.

Norman Virus Control v4.35.4.6

ItW Boot	100.0%	Macro	97.4%
ItW File	99.7%	Macro on-access	99.4%
ItW File on-access	n/a	Polymorphic	99.0%
ItW Overall	99.8%	Standard	99.7%

Another program with admirable stability, though the usual comments about the on-access component still apply. The *Norman* on-access system consists of a behaviour blocker (operational on file execution) and Cats Claw, which screens for macro viruses. The former of these proved impossible to test against anything but the Boot Sector test-set, where it discovered all but five samples, declaring the others to have been detected ‘by statistical tests’.

The file scan options were tested for stability more than for overhead ratings and showed no problems on this front. Of note was the behaviour blocker in ‘strict’ mode, which considered even the simple copying of executables to be a possible sign of viral infection.

On-demand in the boot sector tests a score of 100% detection was achieved with no glitches or irritations.

Panda Antivirus v5.0

ItW Boot	87.0%	Macro	72.4%
ItW File	96.2%	Macro on-access	72.7%
ItW File on-access	87.5%	Polymorphic	68.6%
ItW Overall	97.5%	Standard	80.8%

Another first-time appearance, this Spanish product should not be confused with the *Dr Panda Utilities* from (distant) past *Virus Bulletins*. The readme file contains the usual hyperbole (in this case, somewhat more outrageous). A built-in list of 38 potential target file extensions seemed a little paranoid (although the default ‘active’ extensions from this list is little different from most other products).

Interestingly, in the boot sector virus tests, *Panda* proclaimed merrily that there were two viruses present on each of five of the single sample diskettes. The Jumper.B sample topped this, however, apparently being host to three infected boot sectors. Most of these multiple reports were common aliases for the virus actually present, but if this is *Panda’s* mechanism for conveying that information, this should be made clearer. If not, it would seem that some duplicate virus signatures are present in *Panda’s* library.

As the on-access scanner had no discernible silent mode, the on-access tests were only run through the In the Wild Boot, File, Macro and Standard test-sets, by which time the tester’s wrists were glad of a change of scene.

Quarterdeck ViruSweep v1.00

ItW Boot	98.9%	Macro	86.9%
ItW File	99.9%	Macro on-access	86.9%
ItW File on-access	99.9%	Polymorphic	95.4%
ItW Overall	99.5%	Standard	100.0%

A new product for review, which is clearly having a few teething troubles. Rather unusually for a *Windows 95*-only product, the CD-ROM does not have an autorun feature. Upon starting the installation process manually, an error dialog popped open, due to the linking of a DLL to a non-existent OLE file. Things were not looking good at this point, and indeed, this did not bode well for the testing process itself.

On rebooting the system after installation, the QSM (presumably the Quarterdeck Service Manager) produced errors due to illegal operations. This fault was not fixed following installation of the supplied update, so QSM was removed from the Startup group on the test machine. An annoying quirk during installation was that, despite disabling the 'make a rescue disk' option early on, this effort seemed to have been ignored later in the process, when a prompt appeared asking if one should be made.

Peculiarity was the order of the day during the on-access boot sector virus tests. Re-testing of those viruses not detected produced, on occasion, a report of a completely different virus detection, although the virus detected was (usually) that from the immediately previous diskette. This was followed by a selection of other possible infections being logged, and eventually a blue screen was the result.

On-demand boot sector detection was also not without problems. The VxD screen appeared some, yet not all, of the time – an oddity that initially seemed related to some of the scanner's settings, but reappeared after a confusing spurt of reliability and then could not be vanquished.

Overhead tests further proved the lack of consistency in *ViruSweep*, since XCOPY was labelled at random as showing virus-like behaviour – 'ViruSweep Important Interrupts have been changed by command.com' being the rather strange warning. This annoyance was removed by deactivation of interrupt checking.

Sophos SWEEP v3.07

ItW Boot	100.0%	Macro	96.4%
ItW File	99.4%	Macro on-access	96.4%
ItW File on-access	99.4%	Polymorphic	99.0%
ItW Overall	99.6%	Standard	99.7%

Another of the non-crashing achievers of this comparative, we are back to minor niggles with *SWEEP*. The on-access scanner, *InterCheck*, is proclaimed in the manual to be non-removable under *Windows 95*, but this proved to be possible using the very *NT* configuration commands the manual specifically declared were unsupported under *Windows 95*. On the other hand, the 'deny access' option of this scanner did indeed do just that during the In the Wild Boot tests, where all viruses were detected. Were Explorer human, it would probably have been puzzled by the number of apparently unformatted diskettes it was seeing.

On-demand, the boot sector viruses were all discovered, although there was a peculiarity in the change of focus after virus detection. Combined with the inability to use Alt-F to produce a file menu, this slowed the rate of scanning diskettes considerably.

Stiller Research Integrity Master v4.01

ItW Boot	97.7%	Macro	74.8%
ItW File	96.6%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	32.7%
ItW Overall	97.0%	Standard	85.6%

Stiller Research's product is a little out of place in this review, and suffers a fair amount as a result. The primary protection method offered by *Integrity Master* is that of checksumming, and the detection of illicit changes to files – whether viral in origin or the actions of unauthorized personnel. As a result, the security and checksumming portions of the program are considered more important than the scanning portions. *Stiller Research* goes so far as to suggest that another scanner be used in conjunction with *Integrity Master*. The theory behind this is that a scanner will pick up known viruses, while *Integrity Master* prevents data damage caused by any that slip through the net.

Sumi AspVIRin AntiVirus

The developers of this Romanian product were keen to introduce it to *Virus Bulletin* testing. The supplied product installed quickly and apparently efficiently, but all attempts to run the main executable failed with a series of page faults. The trial version was downloaded from their web site, but it performed in exactly the same way. Installing Eastern European language support on the test machine did not resolve the matter either. Email to the developers went unanswered, so we abandoned trying to test the product.

Symantec Norton AntiVirus v4.04

ItW Boot	100.0%	Macro	97.4%
ItW File	100.0%	Macro on-access	98.0%
ItW File on-access	100.0%	Polymorphic	88.0%
ItW Overall	100.0%	Standard	99.1%

Yet another program where stability *and* predictability were to be found, though here it was fairly localized. After by far the prettiest of the splash screens (involving spaceships, sound effects and a rolling graphics show), the standard CD offered the option to watch four videos, ranging in content and style from mildly informative to cheesy. If these are used as a guide, the *Symantec* corporate image is that of a sideburnless Elvis in a fetching gold lamé suit.

Unlike so many other products, most scanning was performed without distress, though boot sectors proved something of a fly in the ointment. On-access scanning of floppies was wont to hang the test machines irretrievably should the diskette be removed too soon. In this context, 'too soon' includes a period of time after which all visible and audible disk access had finished! When a virus was detected, *Norton Antivirus* proclaimed that access had been denied, yet after a short period of time Explorer was apparently allowed enough access to decide that the sample diskettes were devoid of files, rather than not formatted. Despite these peculiarities, the only boot sector virus missed during on-access testing was Moloch.

On-demand boot sector tests produced no misses, though strange events occurred when faced with Michelangelo.A, Michelangelo.S, and MISiS. These samples have strange BPBs (for a diskette in a high-density 3.5-inch drive), which triggered the message 'Unable to access drive A:. The drive is locked with a disk utility. Scan again later when the disk is no longer locked'. Contrary to general intuition, at this point selecting 'skip disk' allowed *Norton Antivirus* to detect the infections upon these media.

The lack of a 'proper' silent mode made on-access testing slow, if not interesting.

Trend Micro PC-cillin 95 v3.0

ItW Boot	95.4%	Macro	97.4%
ItW File	98.7%	Macro on-access	90.2%
ItW File on-access	97.2%	Polymorphic	94.2%
ItW Overall	97.6%	Standard	98.5%

The product *Trend* submitted for review sat comfortably with the illustrious company inhabiting the 'non-functional' end of this comparative review. Things started nicely, as while installing the application, no problems were apparent. However, once installed almost any attempt to use any part of the product resulted in a message to the effect that this was an 'unsupported option'.

As scanning was amongst these unsupported options the future looked far from rosy. For the purposes of having at least some test results, an evaluation copy of *PC-cillin* was downloaded from the WWW and the signature file supplied with the review copy implanted into the evaluation product's installation. The result was a program with some limitations in functionality, though none of these related to tested actions (several of the Internet-related functions – including on-line updating and registration – and the disinfection wizards were not available).

Even after these steps had been taken there were still gripes aplenty to be addressed. As an *entré*, the button to start an on-demand scan was without an accelerator key. This is immensely frustrating when having to scan more than half a dozen or so diskettes. In an attempt to ease testing the 87 diskettes in the Boot test-set, the focus was tabbed to this button in the hope that a cycle of keypresses could be discovered to speed the testing. However, once this button was visually selected, pressing the Enter key caused the program to terminate completely. On-demand boot testing was not a pretty experience…

Having devised a process that seemed to work, boot sector viruses were not the most impressively dealt with. Despite having *ICSA* and *Secure Computing* certifications that the product detects all In the Wild viruses, a handful of misses in the ItW Boot tests seems to be all but expected in *Virus Bulletin* tests – it would be a pity if this had been fixed in the version sent for testing. Somewhat surprisingly, the option 'deny access to infected files and continue' seems to have been taken too literally – boot sectors are not, technically, files and thus Explorer was not prevented access to the rest of boot sector virus-infected diskettes. Added to this was an idiosyncratic method of detecting disk changes, which made more mistakes than it should have.

On access scanning also proved problematic when reasonably large numbers of files were passed through *PC-cillin's* gaze. The attemps to test on-access detection of the whole *Virus Bulletin* test set resulted in reliable crashing of the system, and more disturbingly this was reproduced when merely perusing an uninfected installation of *Windows 95*.

Conclusion

While congratulations are due to those nine products which acheived VB 100% awards, this is not to say that they were by any means perfect. More than one of these exhibited such grievous imperfections in either user interface or general stability as to be barely serviceable. On the other hand, some products, despite being a pleasure to use, displayed significant faults in their detection capabilities.

As mentioned at the beginning of the review, brute force detection is not the 'be all and end all' of an anti-virus product. If only to maintain the sanity of testers, it is to be hoped that quality assurance may become a more prominent part of product development.

Technical Details

Test Environment: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, running *Windows NT v4.0 (SP3)*. The workstations could be rebuilt from disk images and the test-sets were held in a read-only directory on the server. All timed tests were run on one workstation.

Speed and Overhead Test-sets: Clean Hard Disk: 5500 COM and EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win95/199805/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

Errata

Two errors from the May comparative review need correcting. The Technical Details box at the end of the review incorrectly claimed the test machines were running *NT*, rather than *Windows 95 (SP1)*.

Further, *Sophos* queried *VB's* Avispa.D samples – the virus that caused *SWEEP* to miss a VB 100% award. It transpires that the samples *SWEEP* missed are not Avispa.D. They are viral and replicate, and all other products in the review detected them as some form of Avispa, as *SWEEP* itself has done in the past. However, they are not samples of the same virus as the Avispa.D in the *WildList Organization's* 'reference set'. Genuine Avispa.D replicants have been generated from a reference sample supplied by the *WildList Organization* and these will replace the Avispa samples in our In the Wild File test-set. In re-testing, the reviewed version of *SWEEP* detected these samples, thus *Sophos* has been granted a May VB 100% award. No other results are affected ■