COMPARATIVE REVIEW

Opening Windows 98

Once more into the jungle that is today's anti-virus world, for a spot of behavioural observation. Here, however, extinctions occur with rather more rapaciousness than the Dodo's demise upon Mauritius.

Of the products reviewed this month yet another, the *Intel* species, was declared extinct during testing, swallowed by a large *Symantec*, while *Dr Solomon's Anti-Virus Toolkit* is destined to undergo significant evolutionary changes. However, preambles of this kind will only serve to keep the eager reader from the real purpose of the review and so the introduction ends here.

Test Procedures

The platform used for these tests was *Windows 98*, the same setup as that in the review of *Sophos Anti-Virus* last month. FAT32 disks were not used, because the sizes of the partitions employed for testing were too small. There are plans to alter this in future reviews.

The same machine was used for all the timing tests, while two other hardware-identical machines were used in conjunction for the on-demand and on-access scanning processes. In all cases the software was deployed in its standard configuration, unless this removed such useful features as on-access scanning or the ability to alter configuration of the scanners.

The August WildList was used in conjunction with the ever expanding Macro, Polymorphic and Standard test-sets, against products dated 1 September at the latest. Where possible, scan tests were run from a CD, thus removing the need to restore files after each scan as a precautionary measure against overkeen deletion or disinfection. Several products, however, produced useless report files or none at all. In these cases deletion or quarantining was used in order to obtain meaningful results.

On-access scanning overheads were tested using XCOPY to move large numbers of executables, the results being compared against a baseline with that component inactive. Floppy disk speed tests were performed upon two almost identical disks, differing only in that the files on one were all infected with Natas.4744. The hard disk scanning test, combining speed with false positives on 5500 executables, is the standard *VB* test, and comparable with results in the last *NT* comparative in September.

The complete detection tests are reported in the main tables. The results reported in the summaries are only the on-demand variety, plus the on-access result for the combined In the Wild test-sets and the Macro test-set.

Alwil AVAST32 v7.70 (Build 725)

ItW Boot	100.0%	Macro	98.2%
ItW File	100.0%	Macro o/a	n/t
ItW Overall	100.0%	Polymorphic	98.3%
ItW Overall o/a	n/a	Standard	99.7%

Still emblazoned with a horde of beetles, *Avast32* continues to sit with the better class of on-demand detectors, but remains untestable by *VB's* on-access scanning methodology.

This is not the problem it might seem – the on-access detection of viruses is dependent on an attempt to execute, which makes the testing of this function a task too epic to undertake in one lifetime. Nevertheless, *Alwil's* product remains reliable and stable, giving little cause for anything but pleasant comment.

CA Cheyenne Inoculan AntiVirus v5.0.4.13

ItW Boot	100.0%	Macro	98.2%
ItW File	100.0%	Macro o/a	98.2%
ItW Overall	100.0%	Polymorphic	99.1%
ItW Overall o/a	99.6%	Standard	100.0%

As ever *Inoculan* was frustrating to the degree that it endangered the reviewer's mortal soul as he invented new curses to lay upon *Cheyenne* programmers. The log file problem remained the greatest single obstacle – by all appearances, the program creates log files in memory which causes it to become ever more hungry for resources as scans of large numbers of viruses progress.

The act of attempting to print the log to file is enough to crash *Inoculan*. On-access scanning, meanwhile, is beset by a similar problem of resource leakage, which resulted in frequent hangs and the speed of the machine degenerating to that of an arthritic sloth.

With all of this laggardly behaviour *Inoculan* also manages to throw in a streak of capricious disobedience too. No amount of changing instructions could provide a setting where the on-demand boot infector tests did not produce a choice of actions to take. Such obvious settings as 'log only' had some mystical significance quite at odds with their literal meanings. There was also an impressive ability for the program to report a virus in memory when scanning of boot disks had just occurred – only likely to be true if *Inoculan* has masochistic code designed to activate boot viruses if detected.

Nevertheless, *Inoculan* was able to detect well in all categories which were testable – on-access polymorphic testing could not be completed without inducing catatonia

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	84	100.0%	738	100.0%	100.0%	1685	98.2%	14385	98.3%	1017	99.7%
CA Cheyenne Inoculan	84	100.0%	738	100.0%	100.0%	1684	98.2%	14433	99.1%	1026	100.0%
Command AntiVirus	84	100.0%	726	99.6%	99.6%	1715	99.5%	14176	97.3%	1017	99.7%
Cybec Vet NetSurfer 98	84	100.0%	726	99.6%	99.6%	1686	98.1%	14086	96.6%	1008	98.9%
Data Fellows FSAV	84	100.0%	738	100.0%	100.0%	1700	99.1%	14415	99.8%	1017	99.7%
DialogueScience Dr Web	0	0.0%	738	100.0%	89.8%	1683	98.1%	14394	99.7%	1017	99.7%
eSafe Protect	83	98.8%	708	98.2%	98.3%	1518	90.4%	13456	91.5%	1007	99.1%
ESET NOD32	84	100.0%	738	100.0%	100.0%	1711	99.1%	14381	99.5%	1026	100.0%
GeCAD RAV	82	97.6%	738	100.0%	99.8%	1706	99.4%	13865	95.4%	980	95.7%
Grisoft AVG	83	98.8%	686	94.8%	95.2%	1337	79.5%	12796	88.5%	883	87.0%
H+BEDV AntiVir	82	97.6%	659	95.5%	95.7%	1545	92.3%	11558	79.1%	980	96.9%
Intel LANDesk Virus Protect	81	96.4%	716	99.2%	98.9%	1578	94.0%	13611	94.0%	1013	99.5%
iRiS AntiVirus	84	100.0%	738	100.0%	100.0%	1688	98.4%	14433	99.1%	1026	100.0%
Kaspersky Lab AVP	84	100.0%	738	100.0%	100.0%	1700	99.1%	14415	99.8%	1026	100.0%
NAI Dr Solomon AVTK	84	100.0%	738	100.0%	100.0%	1692	98.6%	14287	97.6%	1026	100.0%
Norman TBAV	84	100.0%	730	99.7%	99.7%	1607	95.4%	14083	94.8%	997	98.2%
Norman Virus Control	84	100.0%	738	100.0%	100.0%	1617	96.0%	14294	99.0%	1017	99.7%
Sophos Anti-Virus	84	100.0%	738	100.0%	100.0%	1640	97.2%	14273	98.8%	1015	99.5%
Stiller Integrity Master	82	97.6%	559	86.1%	87.3%	1050	63.7%	5081	30.7%	769	81.9%
Symantec Norton AntiVirus	84	100.0%	738	100.0%	100.0%	1719	99.8%	14443	98.7%	1017	99.7%

upon the test machine. This detection rate is the only saving grace for *Inoculan* and the only part of the program which is not produced by *CA* programmers.

Command AntiVirus for Windows 95 v4.52

ItW Boot	100.0%	Macro	99.5%
ItW File	99.6%	Macro o/a	99.5%
ItW Overall	99.6%	Polymorphic	97.3%
ItW Overall o/a	99.6%	Standard	99.7%

The monitor lizard is a particularly close relative to *Command AntiVirus* (*CSAV*), both being slow lumbering creatures yet very effective in their respective hunting niches. No false positives were recorded during the scan of the Clean test-set – a 'suspicious' warning was the limit.

This conclusion was reached at a lethargic rate – only two products were slower. On-access overheads were of a more strolling nature, slowing affairs by a factor of four or more. Floppy disk speeds alone were an area where *CSAV* approached the median in terms of velocity.

On-demand tests resulted in good levels of detection – against the ItW test-set only Marburg and TVPO.3783.A were missed, the former being a worrisome creature given its current wide domain. It was also the sole virus missed in the Polymorphic test-set. Macro misses were due to AccessiV.A and B, which are not scanned in the default setting due to the large extra overhead incurred by default scanning of MDB files. Against the Standard test-set, Navrhar falls into the same category of unscanned files but here VxDs are ignored by default – a precaution particularly necessary in this less than swift scanner.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	84	100.0%		n/t	n/a		n/t		n/t		n/t
CA Cheyenne Inoculan	81	96.4%	738	100.0%	99.6%	1684	98.2%		n/t	1026	100.0%
Command AntiVirus	84	100.0%	726	99.6%	99.6%	1715	99.5%	14170	96.4%	1017	99.7%
Cybec Vet NetSurfer 98	83	98.8%	738	100.0%	99.9%	1691	98.2%	14340	98.0%	1008	98.9%
Data Fellows FSAV	84	100.0%	738	100.0%	100.0%	1701	99.1%	14444	100.0%	1026	100.0%
eSafe Protect		n/a	703	97.4%	n/a	1511	90.0%	13456	91.5%	1026	100.0%
ESET NOD32	84	100.0%	738	100.0%	100.0%	1711	99.1%	14381	99.5%	1026	100.0%
Grisoft AVG	49	58.3%	416	61.6%	61.2%	1140	68.8%	1102	7.5%	614	68.1%
H+BEDV AntiVir	24	28.6%	685	96.6%	89.7%	1548	92.5%	12178	84.1%	994	98.0%
Intel LANDesk Virus Protect	78	92.9%	366	56.4%	60.1%	180	9.9%	515	3.5%	608	68.4%
iRiS AntiVirus	81	96.4%	738	100.0%	99.6%	1688	98.4%	14419	95.5%	1026	100.0%
Kaspersky Lab AVP	84	100.0%	738	100.0%	100.0%	1700	99.1%	14415	99.8%	1026	100.0%
NAI Dr Solomon AVTK	83	98.8%	738	100.0%	99.9%	1688	98.4%	14287	97.6%	1024	99.7%
Norman TBAV	60	71.4%	657	89.3%	87.5%	1242	73.9%	14444	100.0%	1008	99.0%
Norman Virus Control	82	97.6%		n/t	n/a	1628	96.2%		n/t		n/t
Sophos Anti-Virus	84	100.0%	738	100.0%	100.0%	1636	96.9%	14273	98.8%	1015	99.5%
Symantec Norton AntiVirus	84	100.0%	714	97.7%	98.0%	1646	97.7%	13500	93.5%	1017	99.7%

On-access scanning was much the same, though a handful of Cryptor samples evaded the snapping jaws of *CAV* in addition to those already noted. The status of the on-access scanner was rather difficult to ascertain at first – what appeared to be a tray icon for on-access scanning was in fact connected with the management console.

Cybec Vet NetSurfer 98 v9.8.5.0

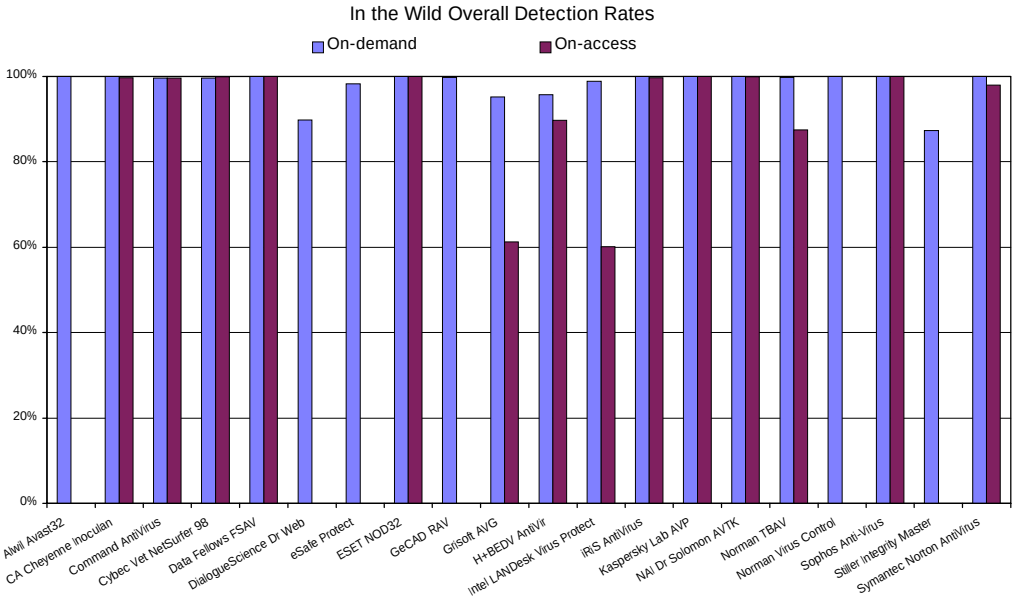
ItW Boot	100.0%	Macro	98.1%
ItW File	99.6%	Macro o/a	98.2%
ItW Overall	99.6%	Polymorphic	96.6%
ItW Overall o/a	99.9%	Standard	98.9%

Vet remains devoted to aardvarks in its manual and were an aardvark's tongue a little swifter in motion there might be some useful comparison to be made. Combining the buzzwords 'net', 'surfer' and '98' it might be expected that this product will appeal to the more gullible of middle management, who would on this occasion at least have purchased a reasonably effective and stable product. *Vet* also remains the speediest of the products reviewed here, with low overheads from its on-access component as well as impressive throughput in both the hard disk and diskette speed tests.

The main disappointment will therefore be the lack of detection of all In the Wild viruses, especially because there is a simple method of overcoming this failing. In the on-access tests *Vet* achieved a full detection rate, on-demand it missed only the screen savers infected with Marburg; the problem clearly being a simple omission from the default scanned extensions (SCR) or fixed programmatically with automatic file type detection. Users of *Vet* would be well advised to add SCR to the list of scanned files – especially if Marburg has been detected elsewhere or is making unexplained returns after disinfection.

Data Fellows F-Secure Anti-Virus v4.02

ItW Boot	100.0%	Macro	99.1%
ItW File	100.0%	Macro o/a	99.1%
ItW Overall	100.0%	Polymorphic	99.8%
ItW Overall o/a	100.0%	Standard	99.7%



with the Clean set. Coaxed through several partial runs, it produced two false positives, but could not be made to scan all of the test-set.

Elsewhere, however, results were good and there was a noticeable speed increase when scanning files on both floppy and hard disks in comparison with the *NT* testing. Detection, too, reached admirable levels, with all file categories recording detection percentages in the high nineties – in the wild files topping this at full detection. All in all, the results can be considered to represent a two-headed calf and act as an extreme example of the perils facing companies when they submit a new, superficially improved, but not quite fully tested, product for review.

eSafe Protect v2.0

ItW Boot	98.8%	Macro	90.4%
ItW File	98.2%	Macro o/a	90.0%
ItW Overall	98.3%	Polymorphic	91.5%
ItW Overall o/a	n/a	Standard	99.1%

The trickiest part of dealing with this product is its serpentine user interface. Once mastered, detection is respectable, though poor against the Macro set and especially on-access. During the overhead tests the inbuilt heuristics were sufficiently oversensitive to trigger upon the execution of XCOPY32. The overhead ratings thus do not include this particular part of the standard protection regime.

It is unlikely that any user would opt for virus protection which prevented any file copies due to their suspicious nature, and considered, as *eSafe Protect* did, that COMMAND.COM should be prevented from executing. The controls for the scanning methods to be used on-access and on-demand are praise-worthily comprehensive, allowing this niggle to be disabled simply.

ESET NOD32 v1.09

ItW Boot	100.0%	Macro	99.1%
ItW File	100.0%	Macro o/a	99.1%
ItW Overall	100.0%	Polymorphic	99.5%
ItW Overall o/a	100.0%	Standard	100.0%

Sadly the pulsating alien heart motif has departed *NOD32* but the rest of the program continues to please. Detection remains at an impressive level, with the sole problem area

Past reviews of the 4.*x* version of *FSAV* have shown it to be fearsomely painful to reviewers due to its instability and an initial problem when faced with on-access boot viruses did nothing to inspire confidence. On this occasion scanning halted after the first sample, giving an apparent detection rate of one. This turned out, happily, to be akin to a bee sting attack – once and once only – the program behaving impeccably thereafter and gaining a detection rate of one hundred percent for both boot sector tests.

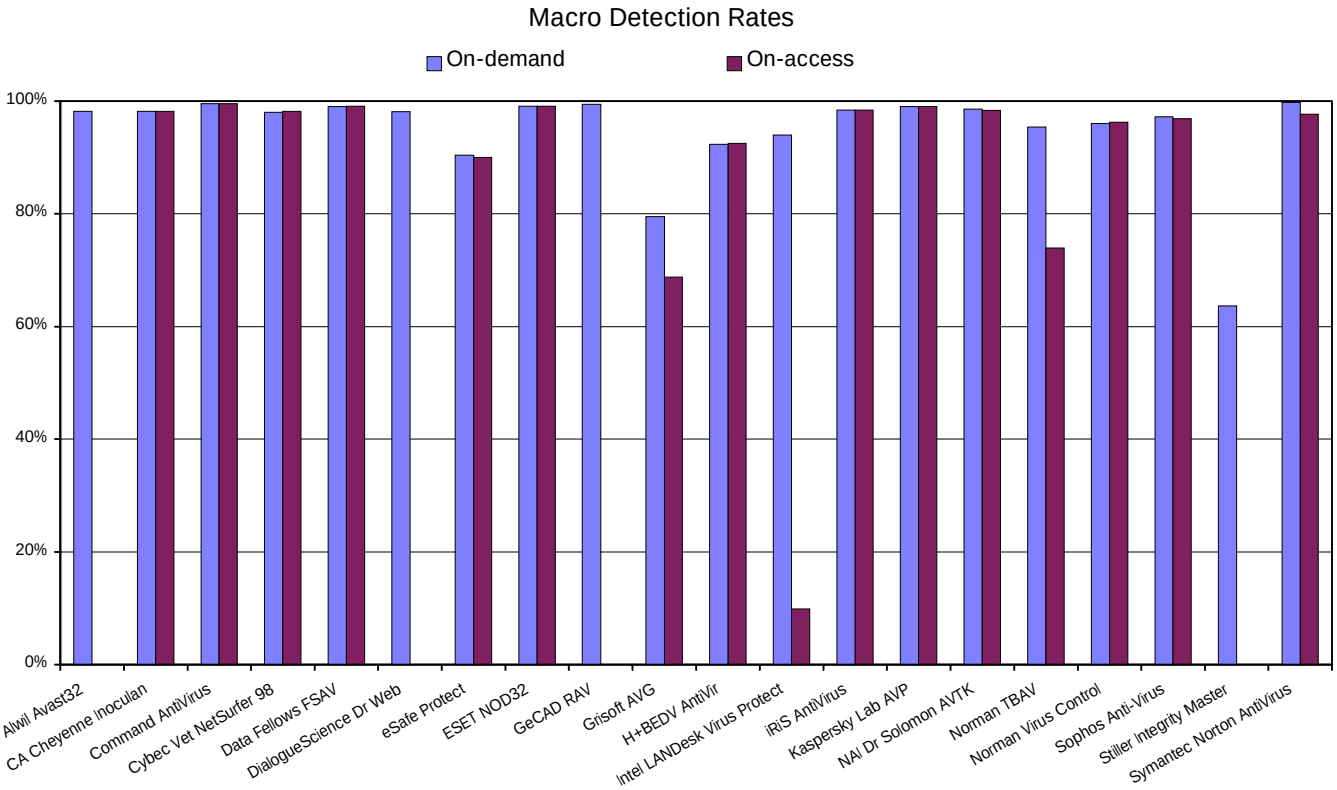
Detection in other areas was admirable too – MDB and VxD files undetected for reasons of speed, and macro viruses, including the almost universally problematical XM/Compat.A, provided the remainder of the misses. It was a notable feature of this test that macro viruses were by and large the greatest bane of the scanners involved, due, perhaps, to the problems involved in dealing effectively with the new generation of polymorphic macro viruses.

DialogueScience Dr Web for Win32 v4.02b

ItW Boot	0.0%	Macro	98.1%
ItW File	100.0%	Macro o/a	n/a
ItW Overall	89.8%	Polymorphic	99.7%
ItW Overall o/a	n/a	Standard	99.7%

In the *NT* comparative two months ago *Dr Web* proved a worthy, though rather slow, program. This slightly different version has no cosmetic changes but something under the skin has been drastically altered, and not all for the better.

The program supplied was admittedly a beta version and the suspicion must be that any release version could not be as flawed as this particular edition proved to be. Most disturbingly, detection of boot viruses dropped from near perfect to none whatsoever, a result which smacks of a botched build. The program repeatedly crashed when faced



being the treatment of the W97M/Splash.A virus. Splash is polymorphic by dint of adding random comments to itself, increasing in size with every generation. Here detection of samples in the lower range of size was perfect, but larger documents remained unflagged as infected. Whether this is a problem which will easily be rectified remains to be seen.

Under *Windows 98* it was also apparent that the 'odd boot sector' viruses had changed compared to those in previous reviews. On-demand *NOD32* declared that the directory path was not valid for ExeBug.Hooker, Michelangelo.A and Quox.A, though the viruses were detected both on-access and on-demand. In products which could not handle such oddities these three proved a particular problem.

GeCAD RAV v6.08

ItW Boot	97.6%	Macro	99.4%
ItW File	100.0%	Macro o/a	n/a
ItW Overall	99.8%	Polymorphic	95.4%
ItW Overall o/a	n/a	Standard	95.7%

Looking distinctly less attractive than its competitors, and without an on-access component, *RAV* is also relatively tortoise-like. This is particularly true of the boot sector tests, where the same age-old system of labyrinthine clicks and keypresses is required for each disk scanned. Seven false positives, similar to those noted in the *NT* test, were also thrown up against the Clean test-set.

All this said, *RAV* remains effective in the prime area of concern – that of detection. Though missing more than it should, *RAV* firmly occupies that middle ground.

Grisoft AVG v5.0 (database 20)

ItW Boot	98.8%	Macro	79.5%
ItW File	94.8%	Macro o/a	68.8%
ItW Overall	95.2%	Polymorphic	88.5%
ItW Overall o/a	61.2%	Standard	87.0%

AVG showed a variety of problems coupled with a readme file containing less than inspiring revelations. On-demand testing comprised a number of options, making the choice of scan a not entirely intuitive one.

The Complete test was chosen, and the on-demand tests performed fairly smoothly, though with a distinctly uninspiring set of detection statistics. Macro viruses proved the greatest challenge to detection, a sign of *AVG's* team being behind the times in their addition of new viruses. To this was added the scenario, drifting in the wake of the scan procedure, whereby *Explorer* refused to perform changes in the current directory – not a pleasing side-effect. Boot sector testing was almost perfect, though the inability to spot Natas.4744, an elder statesman of the virus world, must be considered disturbing.

If on-demand tests were unsatisfactory, on-access ones posed fewer problems for the operating system, but were more disappointing in terms of detection. A host of boot sector viruses passed unnoticed, those which were detected once were missed next time during a sequence of scans, a problem more common under *NT*. Detection of file viruses was similarly poor. Over 14,000 of the 17,000 samples were missed, making for a level of protection which might be considered worse than useless.

With such a low detection capability it is perhaps to be expected that no false positives were encountered, and that scanning proceeded speedily. It was surprising the readme file referred to the new addition of Laroux disinfection, but not that directories with long filenames were still unsupported in the scanning exclusion list.

H+BEDV AntiVir v5.14.0.7

ItW Boot	97.6%	Macro	92.3%
ItW File	95.5%	Macro o/a	92.5%
ItW Overall	95.7%	Polymorphic	79.1%
ItW Overall o/a	89.7%	Standard	96.9%

Whimsically fronted by a turn-of-the-century bathing photograph, *AntiVir* continues to be educational inasmuch as learning German benefits the review process. The on-access scanner was a new addition to this product in *VB* reviews, though these changes were not without concomitant changes in program stability. These manifested themselves in fatal exceptions during both on-demand boot and on-access file tests, and warped GUI antics at other times. *AntiVir* also takes the rabbit prize for timidity, finding 62 false positives in the Clean test-set.

The on-access scanner was all but useless on the boot sector tests, discovering fewer than a quarter of the virus-infected diskettes thrown at it as worthy of concern. Strangely enough, on-access scanning of files was marginally more effective than the on-demand scanner, though here detection was at least at a level which might be considered to provide adequate protection.

Disturbingly, for those folk who disapprove of macro virus upconversion, an option in the scanner triggered on occasion stating, in German, that the document scanned was of unknown format and offering to convert it to one which was known. Quite what the result of this would be is unknown, lest the wrath of the one known as Bontchev fall upon *Virus Bulletin's* unworthy collective pate.

Intel LANDesk Virus Protect v5.02

ItW Boot	96.4%	Macro	94.0%
ItW File	99.2%	Macro o/a	9.9%
ItW Overall	98.9%	Polymorphic	94.0%
ItW Overall o/a	60.1%	Standard	99.5%

Comparisons with the animal world fail with *Intel's* latest offering, since no creature as unsuited to its intended environment as *LANDesk* would ever have survived. The most heinous problem was encountered during the detection of certain boot viruses. When presented with Hare.7786, Hare.7610 or Moloch, the *LANDesk Virus Protect* simply crashed on-demand.

On-access, affairs were far worse. Scanning of these viruses turned off the on-access portion of the scanner completely, both for boot and file operations. This problem was occasionally noted at reboot with a message produced concerning debug errors but was not obvious from the actions of *LANDesk* either during or after the scan process. Since these viruses remained undetected by either on-access or on-demand scanning, this is a very serious flaw indeed.

Other problems were minor in comparison. Since *LANDesk* has no way of creating log records after scanning, infected files were simply deleted. This was fraught with problems, since it proved impossible to persuade *LANDesk* to delete read-only files. Having set all file attributes to allow deletion, there were still problems in that Cruncher was detected but the samples were not deleted.

iRiS AntiVirus v22.13

ItW Boot	100.0%	Macro	98.4%
ItW File	100.0%	Macro o/a	98.4%
ItW Overall	100.0%	Polymorphic	99.1%
ItW Overall o/a	99.6%	Standard	100.0%

A relatively little-known dark horse, *iRiS* supplies the scanning engine for *Cheyenne*, and the results of the two are unsurprisingly in accordance on-demand. Speed tests also show the expected similarities of a shared lineage and false positives are identical. On-access, however, very slight differences creep in with *iRiSAV* detecting WM/Leveller.A where *Inoculan* did not. The greatest difference is of a much more telling nature though, and is related to the stability and utility of the product.

Despite sporting some of the ugliest graphics around, *iRiSAV* produces good useful log files and no crashes occurred in these tests. This added stability is an anticipated side-effect of the *iRiS* team's use of their own virus detection code, as opposed to *Cheyenne's* aim of integrating *Inoculan* into many *CA* products.

Kaspersky Lab AVP v3.0 (build 124)

ItW Boot	100.0%	Macro	99.1%
ItW File	100.0%	Macro o/a	99.1%
ItW Overall	100.0%	Polymorphic	99.8%
ItW Overall o/a	100.0%	Standard	100.0%

Very much the pet beast of the newsgroup alt.comp.virus at the moment, *AVP* did not quite live up to its house-trained reputation in this showing. In general, detection was as good as ever, though macro viruses in general and XM/Compat.A in particular caused more problems than in the past. Boot virus testing resulted in the usual clean sweep of detection in both on-access and on-demand scanning modes.

On-access scans of the non-boot viruses were slightly more fraught. The first scan run produced a major seizure for the test machine, caused directly by an *AVP*-associated DLL. Retrying this gave no problems during the scan, yet directly

afterwards *Windows* hung when *Explorer* was run. Overheads on copy time with the *AVP* monitor were also a noticeable effect, running at close to 100%. Despite these problems detection remained exactly on a par with that shown on-demand and the possibility remains, as with other products, that some on-access problems are magnified by the sheer volume of infected files processed.

NAI Dr Solomon AVTK v7.87

ItW Boot	100.0%	Macro	98.6%
ItW File	100.0%	Macro o/a	98.4%
ItW Overall	100.0%	Polymorphic	97.6%
ItW Overall o/a	99.9%	Standard	100.0%

Rejoicing in possibly the longest name to be associated with anti-virus merchandise, this product was in fact the *Dr Solomon's* component, devoid of any *Network Associates* input. The aim of *NAI* being the selective breeding of a chimera of *McAfee* looks and *Dr Solomon's* detection, the choice of test subject comes as no surprise. Unhappily for those concerned, the slight stability worries which were apparent during boot sector testing in the past have become no better.

The first problems appeared upon installation, the screen outside the program window being transformed to a veritable kaleidoscope. The setup was its usual irksome self – the smallest changes to the on-access scanner still required a full reboot – a problem which one hopes will be not insuperable in the new generation of *NAI* scanner.

Previous problems with on-demand boot testing were in evidence again. Flame and Michelangelo.A both caused a complete hang of the test machine, offering no alternative to a potentially infecting reboot. With problems such as these appearing just as the tricky graft procedure for *NAI* and *Dr Solomon's* is occurring, there must be some doubt as to the stability of the combined program.

Norman Thunderbyte AntiVirus v4.10

ItW Boot	100.0%	Macro	95.4%
ItW File	99.7%	Macro o/a	73.9%
ItW Overall	99.7%	Polymorphic	94.8%
ItW Overall o/a	87.5%	Standard	98.2%

A product of evolution in action, *TBAV* now possesses an on-access scanner, though further changes are necessary before this new feature can be fully trusted. As ever, the prime feature of *Thunderbyte's* offering is its cheetah-like speed, though this was marred somewhat by the presence of nine false positives. These were all claimed to contain the HLLC.14795 virus. Being a high-level language virus, it seems more than likely that the part chosen to identify this virus is part of code commonly produced by the virus writer's compiler. Floppy scan rates were similarly speedy and with the new on-access scanner having minimal overheads there can be no complaints on this front.

On-demand scanning remains at the usual, reasonable level for *TBAV*, though a sprinkling of CIH misses is an area where improvements are a priority, and the detection of Marburg was far from perfect. Macro viruses too proved a particular weakness. *TBAV* does, in its defence, include an integrity checking component which might lessen the impact of these misses.

The on-access portion, however, exhibited instability and a bizarre detection pattern with DOT and DOC files. The first of each three DOC samples of most macro viruses was not detected. Viruses missed on-demand were again missed completely, and these should have been fully detected due either to age or simplicity.

There was also a number of spontaneous reboots and crashes during attempts to instigate on-access scanning. The on-access boot scans also proved a little unsatisfactory, with a significant number of misses, and poor detection of disk changes. In other areas on-access detection was very similar to that achieved with on-demand scanning, a few extra misses being in accordance with most other such scanners' performances.

Norman Virus Control v4.52

ItW Boot	100.0%	Macro	96.0%
ItW File	100.0%	Macro o/a	96.2%
ItW Overall	100.0%	Polymorphic	99.0%
ItW Overall o/a	n/a	Standard	99.7%

Norman Virus Control (*NVC*) remains its usual stable self, a beast which has found its habitat and stays there. The on-access part of the program remains something of a nonesuch, consisting of a standard macro virus detector, combined with an entirely heuristics-based, pre-execution 'behaviour blocker' for other file viruses. Boot viruses are also detected by pattern-based methods. For this reason only Boot and Macro test-sets were employed for on-access testing – attempting to execute all the samples would have been infeasible.

As ever, *NVC* was on its best behaviour, and testing was without any mishaps or adventures. The largest number of misses came in the macro virus collection, the polymorphic varieties proving problematical. Oddly, XM/Compat.A was detected on-access but not on-demand, possibly reflecting a difference in the databases used by both functions. Boot virus detection showed a couple of misses on-access but none on-demand, and time tests showed *NVC* to be just faster than average.

Sophos Anti-Virus v3.13

ItW Boot	100.0%	Macro	97.2%
ItW File	100.0%	Macro o/a	96.9%
ItW Overall	100.0%	Polymorphic	98.8%
ItW Overall o/a	100.0%	Standard	99.5%

Sophos already stables a selection of corporate beasts – a zebra, a rabbit and a penguin. Following an established tradition the *Sophos Anti-Virus* (*SAV*) tests were performed with no crashes or untoward happenings, log files being produced with no great stress on the reviewer's part. The same version of this program was featured in last month's review and, as might be expected, the only real difference was in the non-detection of some of the newer macros added to the test-set in the intervening month.

Stiller Integrity Master v4.01a

ItW Boot	97.6%	Macro	63.7%
ItW File	86.1%	Macro o/a	n/a
ItW Overall	87.3%	Polymorphic	30.7%
ItW Overall o/a	n/a	Standard	81.9%

Stiller Integrity Master (*IM*) is something of an oddity in these tests and reviewing it here is akin to comparing an elm tree to a variety of marsupial. As the name suggests, *IM* is primarily an integrity checker – in some ways not unlike *In-Defense* (see p.20). There is little point in having an integrity checker which is installed upon an already infected machine, however, and to this end *IM* pre-scans for known viruses before it produces its first integrity checksum database for a machine.

The scanner may also be utilized on-demand. However, *Stiller Research* clearly considers this scan to be of far from vital importance, providing updates to the virus list relatively infrequently, and trusting in its integrity checking to detect viral activity.

This lack of regular updates shows in the scan results, with polymorphic viruses proving a particularly problematical area for *IM*, code emulation presumably not being present in its repertoire of detection tricks. Against the In the Wild test-sets matters were better, though clearly date-related – the more recent samples remaining mostly undetected. Detection of boot viruses gave the best performance, not a surprise as this is an area where new viruses appear with much less frequency and the *Virus Bulletin* test-set is limited to those in the wild.

Speed-wise *IM* proved in the faster portion of the middle running, producing only one false positive in detecting a boot virus in a file (culled from an ancient virus scanner) that contains unencrypted scan strings. One of *IM's* companion virus detection heuristics is somewhat problematic when *Windows 98* itself installs both SCANDISK.COM and SCANDISK.EXE in the same directory.

Symantec Norton AntiVirus v5.00.01

ItW Boot	100.0%	Macro	99.8%
ItW File	100.0%	Macro o/a	97.7%
ItW Overall	100.0%	Polymorphic	98.7%
ItW Overall o/a	98.0%	Standard	99.7%

Resplendent in fine scarlet plumage and replete from the devouring of *Intel*, the question is whether *NAV 5's* image is the only difference. *NAV 5* is usually bundled with a host of nest-fellows but, possibly for legal reasons, the review copy arrived without them. This isolation may or may not explain the presence of a warning upon installation that *NAV* was 'unable to load auto-protect agent, logging… will not be available'.

This was not an ill omen, however, since the logging options available had, in fact, increased from those notable by their absence in the 4.*x* versions. On the whole, *NAV 5* showed improvement, with detection more worthy of *Symantec's* market share. One Marburg sample, the Navrhar VxDs and the macro virus W97M/Encr.A were the only samples missed on-demand.

On-access these joined a motley collection of mostly polymorphic macro viruses and the complete set of Marburgs. The macro virus misses here are presumably a result of the quest for low overheads, currently standing at about one hundred percent. However, the missing of Marburg is more of a disappointment, since it is not unlikely to be 'supplied' in archived material on CDs. In such cases on-access detection is of great importance.

Conclusion

The half-expected rash of new problems associated with *Windows 98* failed to materialize, though some differences in behaviour were apparent in comparison with the previously used operating systems. More disturbing, however, were the persistent problems remaining in an environment now several years old. Stability remains difficult to find in some well-established programs – this is becoming worse rather than better in more than one of the products tested.

The recent rise in polymorphic macro viruses caused by far the greatest percentage of misses. So far the polymorphism seen in macro viruses is quite simple, yet, for many products, dealing with it adequately will require some major redesign of internal macro handling functions. What the future holds is presumably more complexity in the viruses and perhaps a drop in detection while anti-virus companies get to the root of the problem.

Technical Details

Test Environment: Three 166 MHz Pentium-MMX PCs with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, running *Windows 98*. The workstations could be rebuilt from disk images and the master copy of the test-set was held on a CD-ROM. 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-set: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199811/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.