COMPARATIVE REVIEW

Faster, Stronger, Swifter

Once again, *VB* steps into the mysterious world of the DOS anti-virus product – the core technology of most anti-virus companies is to be found in their product for good old *MS-DOS*, so this review, as ever, will be concentrating very much on the scanners' technical ability.

To this end, it largely ignores going into detail on the user interface and the resulting usability of the product, and gets straight to the nitty-gritty: how quick; how reliable.

Tried and Tested

In this review, as in the last DOS comparative (July 1996), the tests were arranged so that each product was run on each sample in turn (i.e. each time it is run, the scanner is allowed to see only one infected file). Whilst this does vastly increase the time taken to run the scan tests, it is not really a problem, as each product is run automatically from batch files – human interaction is not required.

Consequently, a network of old 386 and 486 machines connected to a Pentium running a *Windows NT* server was used. The test-set was written to CD, and the *NT* server was configured to make the CD available to clients via *NT* drive-sharing. Hence, all the client machines had direct access to the samples, but there was no way that anything could modify the set.

Each sample on the CD was copied to the hard disk of the client PC, where it was scanned by the product being tested by that client. The results of the scan were recorded, and the sample deleted before the next one was copied. The log file created by each product for each sample was copied to the server as it was created.

This system, whilst not described in complete detail here, has several advantages. It allows many products to be run simultaneously against a centralised 'sample server', it minimises the opportunities for mistakes to creep in, and, for the vast majority of the time, it does not require the presence of the tester.

How the Test was Run

The In the Wild Boot Sector test-set continues to expand: for this test, it contained 86 viruses, each a live infection on its own 3.5-inch diskette.

In the last comparative review in July, an automated approach was taken to testing against boot sector viruses (an image was dropped onto a diskette, the diskette was scanned, the next image dropped, etc). This time around, the procedure has been abandoned due to the complexity of ensuring that the data gathered from such a test is accurate. Although swapping disks over 1800 times is tedious and painful, it is at least reliable.

The clean set, as always, does double duty as both a false positive and a speed test. For these, the clean files (which now number 5500 COM and EXE files spread across 121 directories and occupying 546,932,175 bytes) are placed onto a hard disk, and each product is run in turn against that disk. Clearly each product must be run under the same conditions, or the results are invalid.

One change has been introduced, to take account of the fact that a couple of products have default modes that create checksum databases of checked files. They do this so that next time they scan, they can simply compute a checksum of each file and compare it to that stored. This way, they need only scan a file if the checksum has changed since last time. Each product is therefore run twice against the clean set – both figures are given here.

The other speed tests remain unchanged: two 3.5-inch 1.44MB diskettes are used; one of which contained 43 uninfected COM/EXE files (997,023 bytes), the other containing the same 43 files, but infected with Natas (1,201,015 bytes).

Virus Test-sets

The basis for the viruses which have been designated 'in the wild' is, as usual, is Joe Wells' WildList (available at http://www.virusbtn.com/WildLists/). As the deadline for submission of products was mid-October, the WildList which was used was that dated 22 September 1996. The bid to create valid, working, checked replicants of everything on the WildList continues: this time we miss out by only four viruses which could not, for various reasons, be replicated for the test-set.

The Standard and Polymorphic sets have continued to grow over the last few months; they now number 532 and 11,000 samples respectively.

One concession in the testing methodology has been made since July: as was done in the last *NT* comparative review in March 1996, products are now explicitly asked to scan all files. This is due both to the rapid growth in the number of macro viruses in the wild, and also to the fact that scanner manufacturers do not yet agree on which file extensions should be scanned by default.

At present, there are eight *Word* viruses in the ItW test-set, each of which is represented by four samples. One of these samples is always a copy of the infected NORMAL.DOT, and the others are standard infected documents. In addition, there are four samples of the *Excel* virus Laroux.

	ItW Boot		ItW File		ItW Overall	Standard		Polymorphic	
	Number	Percent	Number	Percent	Percent	Number	Percent	Number	Percent
Alwil AVAST!	86	100.0%	431	99.0%	99.4%	532	100.0%	11000	100.0%
Cheyenne InocuLAN	83	96.5%	389	92.2%	93.9%	508	97.1%	10354	91.1%
Command F-PROT	86	100.0%	419	96.8%	98.1%	481	93.6%	6053	50.4%
Cybec VET	85	98.8%	409	94.5%	96.2%	520	98.8%	10999	98.9%
DialogueScience DrWeb	81	94.2%	425	97.8%	96.3%	519	97.8%	11000	100.0%
Dr Solomon's AVTK	86	100.0%	418	97.7%	98.7%	530	99.6%	10997	98.8%
ESaSS ThunderBYTE	84	97.7%	433	99.5%	98.8%	527	99.6%	10997	97.7%
H+BEDV AVScan	83	96.5%	409	94.2%	95.1%	509	97.1%	9636	82.7%
IBM AntiVirus	86	100.0%	425	98.6%	99.2%	527	99.2%	10998	97.7%
Intel LANDesk Virus Protect	82	95.3%	415	96.9%	96.3%	359	79.0%	10054	84.5%
Iris AntiVirus Plus	86	100.0%	428	98.4%	99.1%	517	98.3%	10366	90.0%
KAMI AVP	86	100.0%	431	99.2%	99.5%	531	99.8%	11000	100.0%
Look Software Virus ALERT	85	98.8%	431	99.0%	98.9%	532	100.0%	11000	100.0%
McAfee Scan	83	96.5%	423	97.9%	97.3%	473	93.1%	9078	77.8%
Microsoft AntiVirus	15	17.4%	94	24.0%	21.3%	189	53.4%	975	7.8%
Norman Virus Control	86	100.0%	435	100.0%	100.0%	532	100.0%	11000	100.0%
RG Software Vi-Spy	85	98.8%	416	95.2%	96.7%	484	93.9%	7731	62.9%
Sophos SWEEP	86	100.0%	431	99.2%	99.5%	526	99.2%	10998	98.9%
Stiller Integrity Master	81	94.2%	369	87.8%	90.4%	416	86.4%	3479	26.0%
Symantec Norton AntiVirus	86	100.0%	434	99.6%	99.8%	441	89.8%	10500	95.5%
Trend PC-cillin	82	95.3%	407	95.0%	95.1%	355	78.6%	9723	82.2%

Extra Tests and Scoring

As always, the workload imposed by the so-called 'extra tests' is completely out of proportion to the rest of the testing. These tests incorporate limited testing of the ability of the products to detect viruses live in memory, and their disinfection capabilities. For this review, the viruses used in these tests were:

- Boot: AntiEXE, Empire.Monkey.B, Form.A, NYB, Parity_Boot.B, Quandary
- File: Burglar, Manzon, One_Half.3544
- Multi-partite: Junkie

All of these tests were performed on a selection of old *Amstrad* 386 portables, with a mere 1MB of RAM [*Those were the days... Ed.*].

Disinfection of both Burglar and One_Half is considered 'successful' even if the file is not repaired to be completely identical to the original file. The byte at offset 12 within the EXE header is part of the checksum word – this byte is often irreparable, and is usually left by anti-virus products. However, this has no effect on the validity of the final executable file, and so is ignored here.

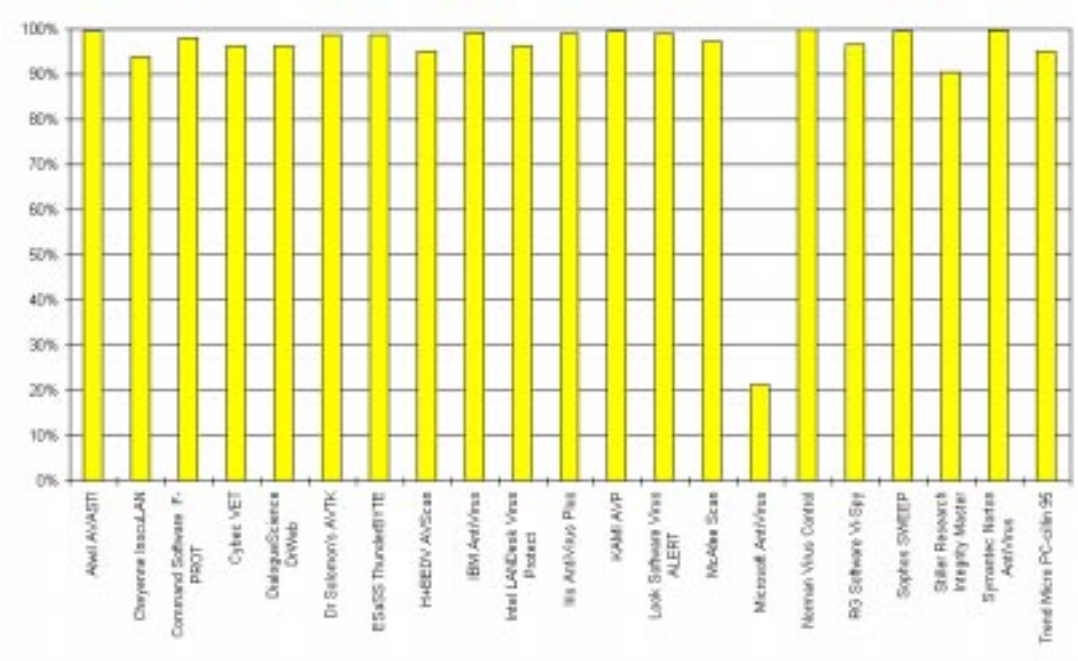
The calculation system is unchanged from the *Windows NT* comparative of October 1995 – for more information on this area, readers are advised to point the WWW browser at the document whose address is given in the Technical Details panel at the end of the article.

It is, needless to say, not possible to score the extra tests.

Alwil AVAST! v7.50-11

ItW Boot	100.0%	Standard	100.0%
ItW File	99.0%	Polymorphic	100.0%
ItW Overall	99.4%		

Results Against the In the Wild Test-set



The only samples with which *AVAST!* had trouble in this review were of Hare – two each of Hare.7610 and Hare.7750 were missed. This tiny omission drops the product to fifth in the In the Wild Overall section. Both the other test-sets were detected flawlessly. Readers may have noticed that in recent reviews, versions of *AVAST!* for other operating systems have produced 100% detection rates against all test-sets: the slight drop in the percentage score here reflects the increasing difficulty of the In the Wild set.

In the other tests, the product missed Manzon in memory, finding the other viruses without difficulty and advising the user on an appropriate course of action. As previously, *AVAST!* does not remove EXE/COM infectors, and handles boot sector virus removal by replacing the offending sector with a new, custom, boot sector (on floppies), or with a previously-saved copy of the original (on the hard disk).

Cheyenne InocuLAN v4.0j, 3.23

ItW Boot	96.5%	Standard	97.1%
ItW File	92.2%	Polymorphic	91.1%
ItW Overall	93.9%		

Notable improvement is seen here in the Standard and Polymorphic sets – both of these scores are considerably up in the last six months. Unfortunately, In the Wild scores are down by a few percent. *InocuLAN* misses 49 of the 522 samples in the combined In the Wild sets; however, the more detailed results show that the product is in fact missing identification of only twelve viruses from these sets. This is sufficient to drop the product to nineteenth (of 21) in the ItW overall category. In other tests, one result stands out: the product managed to avoid detecting Form.A in the hard disk boot sector! Such a bizarre omission cannot go unremarked, especially as the same virus was detected in the boot sector of floppy disks and live in memory. The product also seemed to hang when Junkie was active in memory: everything else was detected and disinfected in memory.

InocuLAN was able to detect and remove the viruses in the extra tests in memory, and also remove them from the other objects without problems. However, this fact is masked by the problems described. The product as it stands needs more quality assurance on the part of the manufacturer, *Cheyenne*, particularly in view of the two false positives it suffered.

Command Software F-PROT v2.24c

ItW Boot	100.0%	Standard	93.6%
ItW File	96.8%	Polymorphic	50.4%
ItW Overall	98.1%		

F-PROT again comes fairly close to attaining faultless In the Wild detection, but doesn't quite make it this time. There are several reasons for this failing: the only standard DOS viruses it misses are Digi.3547 and One_Half.3570.

However, the command-line scanner seems to have considerable trouble with *Word* macro viruses; consequently, a second executable called *F-MACRO* is provided (though not installed by default): this component performs admirably against *Word* and *Excel* viruses. One hopes that the functionalities of the two programs are combined as soon as possible, as, although users do have the capability to protect themselves against macro viruses with the current distribution, it is not obvious how to do so. The continued decline in the Polymorphic score gives cause for concern. Can it be true that *F-PROT* is third from bottom in this category?

In the extra tests, all the viruses were correctly detected in memory (in this area, a distinct improvement over performance in the last review), and all bar Manzon were removed correctly from their respective infected objects.

	Clean Floppy		Infected Floppy		Clean Hard Drive 1		Clean Hard Drive 2	
	Scan Time (min:sec)	Data Rate (KB/s)	Scan Time (min:sec)	Data Rate (KB/s)	Scan Time (min:sec)	Data Rate (KB/s)	Scan Time (min:sec)	Data Rate (KB/s)
Alwil AVAST!	0:43	22.6	1:01	19.2	3:53	2292.3	3:53	2292.3
Cheyenne InocuLAN	0:41	23.7	0:39	30.1	8:29	1049.3	8:29	1049.3
Command F-PROT	0:35	27.8	0:45	26.1	4:07	2162.4	4:07	2162.4
Cybec VET	0:39	25.0	0:45	26.1	1:44	5135.7	1:44	5135.7
DialogueScience DrWeb	1:28	11.1	1:45	11.2	55:28	160.5	2:10	4108.6
Dr Solomon's AVTK	0:42	23.2	0:55	21.3	2:47	3198.3	2:47	3198.3
ESaSS ThunderBYTE	0:32	30.4	0:33	35.5	1:44	5135.7	1:44	5135.7
H+BEDV AVScan	0:49	19.9	1:11	16.5	7:01	1268.7	7:01	1268.7
IBM AntiVirus	0:50	19.5	0:55	21.3	6:56	1283.9	1:10	7630.2
Intel LANDesk Virus Protect	0:48	20.3	0:48	24.4	10:08	878.5	10:08	878.5
Iris AntiVirus Plus	0:39	25.0	0:53	22.1	11:36	767.4	11:36	767.4
KAMI AVP	0:59	16.5	0:41	28.6	24:17	366.6	24:17	366.6
Look Software Virus ALERT	0:46	21.2	1:09	17.0	3:58	2244.2	3:58	2244.2
McAfee Scan	0:38	25.6	0:35	33.5	8:46	1015.4	8:46	1015.4
Microsoft AntiVirus	0:27	36.1	0:42	27.9	3:12	2781.8	3:12	2781.8
Norman Virus Control	0:41	23.7	0:45	26.1	5:43	1557.2	5:43	1557.2
RG Software Vi-Spy	0:45	21.6	0:48	24.4	3:30	2543.4	3:30	2543.4
Sophos SWEEP	0:42	23.2	0:29	40.4	8:16	1076.8	8:16	1076.8
Stiller Integrity Master	0:50	19.5	1:26	13.6	8:57	994.6	5:45	1548.2
Symantec Norton AntiVirus	0:44	22.1	0:55	21.3	3:10	2811.1	3:10	2811.1
Trend PC-cillin	0:48	20.3	0:56	20.9	6:43	1325.3	6:43	1325.3

Cybec VET v9.13

ItW Boot	98.8%	Standard	98.8%
ItW File	94.5%	Polymorphic	98.9%
ItW Overall	96.2%		

The results against the In the Wild test-set for *VET* in this comparative are comparable, in many ways, to *F-PROT*'s. *VET* too has imperfect detection of *Word* macro viruses, so ships with a second executable (*VETMACRO*) designed specifically for detection and removal of this virus type. The job is performed very well, but like *F-MACRO*, it should be integrated into the main command-line scanner. Other than macro viruses, only Karnivali.1971, the two variants of Tentacle, and Pasta were missed in the In the Wild sets.

As far as the other test-sets are concerned, *VET* performed very well, missing just one sample in the Polymorphic test-set (PeaceKeeper.B), and twelve samples of three viruses (PS-MPC.545, XQC.133, and Warchild.886) in the Standard test-set. The product is also exceptionally fast for a non-checksumming scanner, clocking in at the same speed as *ThunderBYTE*: startling by any standards.

The extra tests were handled well: all viruses were detected in memory, and all bar One_Half.3544 and Manzon were disinfected. The same is true of the infected objects: all were correctly disinfected except Manzon and One_Half.3544, where disinfection was not attempted.

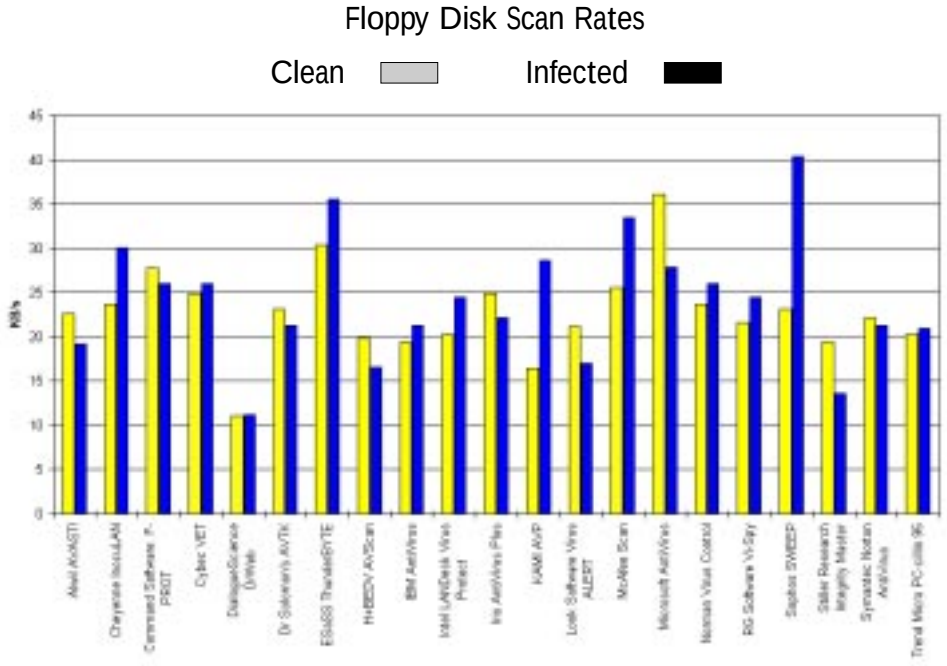
DialogueScience DrWeb v3.16

ItW Boot	94.2%	Standard	97.8%
ItW File	97.8%	Polymorphic	100.0%
ItW Overall	96.3%		

DrWeb is one of the comparatively few products whose speed figure when scanning a clean hard disk is different second time around. When the product is run as advised, a checksummer

validates files to determine if they need to be checked again. This helps its otherwise incredibly sluggish performance: it goes from being by far the slowest product first time around to amongst the fastest on subsequent scans.

As for detection, the story is the opposite of that in the more conventional products: very good detection of the supposedly more difficult polymorphic set, but middling scores against the In the Wild sets: curious. Performance in the extra tests was excellent: all the viruses were detected and removed from all infected objects and memory. Perhaps more importantly, two false positives were encountered.



Dr Solomon's AVTK v7.63

ItW Boot	100.0%	Standard	99.6%
ItW File	97.7%	Polymorphic	98.8%
ItW Overall	98.7%		

Curiously, the distribution department at the newly-renamed *Dr Solomon's Software* shipped an outdated version of their software for this review – however, the policy is to review what is sent, which is exactly what *VB* did.

Detection in the In the Wild sets was, despite the slip-up, very good: the *Toolkit* only missed three viruses (17 samples in total, of Hare.7786, Laroux, and Xuxa.1984) in these groups. Standard (two samples of Positron were missed) and Polymorphic (three of Anarchy.6503) detection was similarly good.

On top of this, the product continues to perform well above average in the speed tests, and extremely well in the extra tests. Here, all viruses were found in memory, and disinfected from all on-disk objects.

ESaSS ThunderBYTE v7.06

ItW Boot	97.7%	Standard	99.6%
ItW File	99.5%	Polymorphic	97.7%
ItW Overall	98.8%		

TB's speed is undiminished (it seems that *Cybec's VET* has been getting faster, rather than *ThunderBYTE* getting slower…), and the detection rate is on the way up in all but the In the Wild sets. That last result is slightly unfortunate, and must surely be a measure of the ever-increasing difficulty of detecting everything out there in the real world. Only four were missed in this case: one each of Date, Hare.7750, Moloch and Werewolf.1500.B.

All viruses except Burglar were detected in memory, and all boot sector viruses correctly removed from floppy and hard disks. The product takes a somewhat unusual approach to parasitic virus disinfection, using checksum and header data on each file to aid in the attempted reconstruction of the file in question. The technique enabled it to repair successfully infections by Burglar, Junkie, and Manzon, although the disinfected Burglar file had more differences from its original than that of other products.

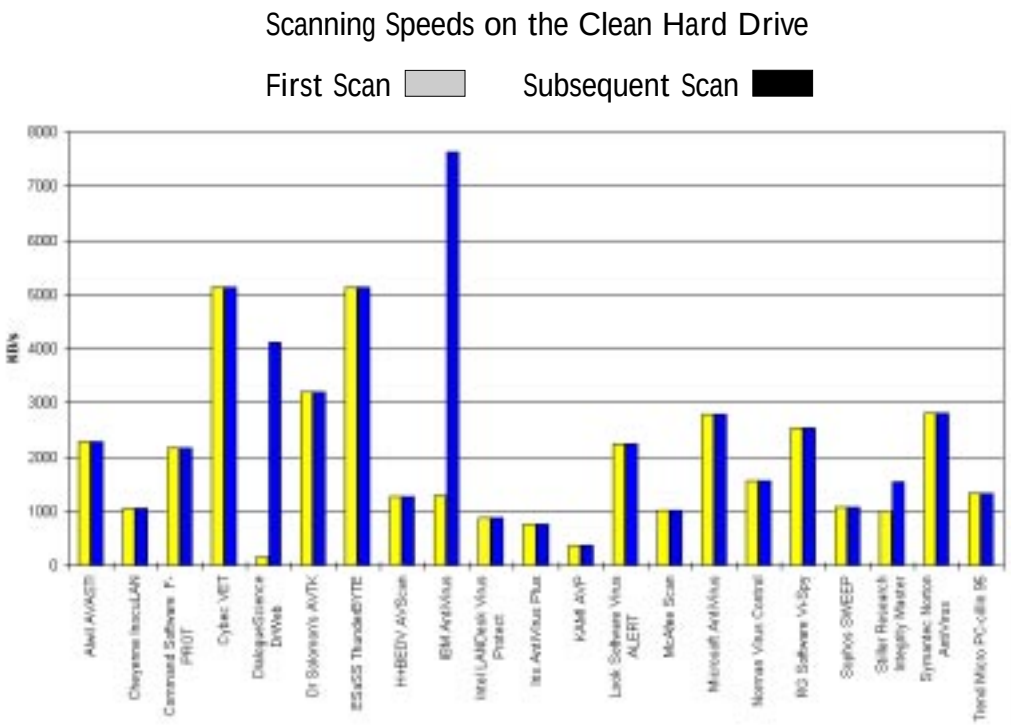
H+BEDV AVScan v3.06

ItW Boot	96.5%	Standard	97.1%
ItW File	94.2%	Polymorphic	82.7%
ItW Overall	95.1%		

Another improved performance from the German company *H+BEDV's AVScan* – scores are up again from the last comparative. Nonetheless, whilst it is improving, performance on the In the Wild sets is still weak, and there were two false positives. In the extra tests, *AVScan* detected all the test viruses in memory, but once again a version capable of disinfection was not submitted for review.

IBM AntiVirus v2.5.1

ItW Boot	100.0%	Standard	99.2%
ItW File	98.6%	Polymorphic	97.7%
ItW Overall	99.2%		



improving for a while now, but still has a little way to go, missing as it does some variants of Hare, in addition to the samples of Pieck.4444 and Xuxa.1984.

In the extra tests, *LANDesk Virus Protect* missed One_Half.3544 and Manzon in memory. All of the boot sector viruses were correctly disinfected from floppy and from hard disks, and disinfection was attempted for all file samples, but Burglar could not be run after disinfection.

Despite being a product that (at least in the UK) gets little marketing push, *IBM AntiVirus* has performed consistently over the years, and still manages to maintain the best and most far-sighted research department in the business. That department has been busy in recent months: Hare.7750 and Tentacle.10634 were the only viruses in the In the Wild test-sets for which detection was lacking.

The scores in the other test-sets are up on last time as well: the Polymorphic score, for example, is marred only by two missed samples – one each of One_Half.3544 and SMEG_v0.3. The product's speed figures are also greatly helped by being given a second shot at the clean hard drive: the checksum database built up the first time around means that the product suddenly becomes the fastest in this, more realistic, test.

In the extra tests, all viruses were detected in memory without difficulty, and all the boot sector viruses were removed from both hard and floppy disks. As for infected files, only Junkie could be cleaned.

Intel LANDesk Virus Protect v193

ItW Boot	95.3%	Standard	79.0%
ItW File	96.9%	Polymorphic	84.5%
ItW Overall	96.3%		

These tests, which were performed on the DOS component of *Intel's* essentially network-oriented solution, reveal scores which are generally unremarkable in most aspects: the detection rate against the In the Wild test-set has been

Iris AntiVirus Plus v21.24

ItW Boot	100.0%	Standard	98.3%
ItW File	98.4%	Polymorphic	90.0%
ItW Overall	99.1%		

Iris' scores continue to rise as time progresses – for a largely unknown product, it is doing well. It missed Goldbug and Tentacle.10634 in the In the Wild test-sets, and various samples from the other two groupings.

In the extra tests, all viruses were detected and disinfected from their respective objects, and from memory – a fine performance. Although thirty-two bytes were left at the end of the Manzon sample, its file header was correctly repaired.

KAMI AVP v2.2 (13/10/96)

ItW Boot	100.0%	Standard	99.8%
ItW File	99.2%	Polymorphic	100.0%
ItW Overall	99.5%		

AVP, once unbeatable in terms of detection, does not attain that level of perfection in this review. However, the product only missed the four Laroux samples in both of the In the Wild test-sets, and one of Positron in the Standard set – everything else was detected. This places the product joint third in the In the Wild rankings.

In the extra tests, all viruses except Manzon were detected and disinfected in memory, and everything was correctly removed from all infected objects on disk.

In terms of speed, *AVP* still reigns supreme: in its default configuration, *AVP* was the slowest product to run across the clean hard disk. Still, the detection rates it offers are such that under some circumstances this would be acceptable, were it not for the six false positives.

Look Software Virus ALERT v4.10 (29/09/96)

ItW Boot	98.8%	Standard	100.0%
ItW File	99.0%	Polymorphic	100.0%
ItW Overall	98.9%		

It is only in the ItW test-sets that *Look's* product does not get 100% – this mars an otherwise excellent performance. Having said that, the only samples missed in these sets were those of Hare; an omission which appears eminently fixable.

Virus ALERT detected all viruses used in the extra tests in memory, with the exception of Manzon. The boot sector samples could be removed from hard disks with the help of a recovery diskette, and the boot sectors of infected floppy disks were replaced without problems.

McAfee Scan v2.5.2, 9610

ItW Boot	96.5%	Standard	93.1%
ItW File	97.9%	Polymorphic	77.8%
ItW Overall	97.3%		

McAfee's In the Wild detection score is down since the last comparative. The fact that it missed samples of Laroux, One_Half.3570 and Xuxa.1984 in these groups is sufficient to drop it to the middle of the field. Detection in other sets is up, however, and the situation is far from irretrievable. In the extra tests, *Scan* detected all viruses used in memory, and disinfected them from all infected objects. A pleasing result.

Microsoft AntiVirus v6.22

ItW Boot	17.4%	Standard	53.4%
ItW File	24.0%	Polymorphic	7.8%
ItW Overall	21.3%		

This product is really only included to give a little light relief during testing – besides, it's nice to have a product which can be criticised for every aspect of its operation, and no one minds… Please, home users who have DOS-based machines: there are plenty of freeware/shareware products (not to mention evaluation versions) to be found on the Internet. There's no need to rely on this sort of thing.

Norman Virus Control v3.53, 2.32

ItW Boot	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%
ItW Overall	100.0%		

Norman Virus Control has improved in all areas since the last test, and this time around is the only product to score 100% In the Wild detection. As well as perfect scores in all test-sets, it encountered no false positives.

Material for complaint is also reasonably scarce in the extra tests, although *Norman Virus Control* failed to detect both Junkie and Manzon in memory. Manzon and One_Half.3544 could not be removed from infected files, but everything else was handled admirably. If one had to criticise, one could always mention that it's not the fastest product around, but then the same is true for almost all the other products under test…

RG Software Vi-Spy v14.3

ItW Boot	98.8%	Standard	93.9%
ItW File	95.2%	Polymorphic	62.9%
ItW Overall	96.7%		

An all-round rise in detection rates for *Vi-Spy*, which is gratifying to see. Detection in the In the Wild set is somewhat disappointing, but this is easily remedied – as with many other products, it is basically only the more recent samples which are missed. In the other test-sets the scores are generally unremarkable.

All the viruses tested for in memory were found and identified by the product, which then advised on an appropriate course of action for each one. The boot sector viruses were correctly removed from hard and floppy disks, and Junkie and One_Half from files.

Sophos SWEEP v2.90

ItW Boot	100.0%	Standard	99.2%
ItW File	99.2%	Polymorphic	98.9%
ItW Overall	99.5%		

A good improvement against the In the Wild test-set over the results in the last comparative help to raise *SWEEP's* all-round performance: this time it only missed the samples of Tentacle.10634. In the Polymorphic test-set, the simple omission of two samples of Code.3952:VICE.05 knocks 1.1% off the score.

In the extra tests, *SWEEP* successfully disinfected all of the boot sector viruses from hard and floppy disks, with the sole exception of Junkie. As with the last comparative review, this product encountered memory problems when attempting to disinfect Empire.Monkey.B – *SWEEP* could, however, accomplish the task when copied to a write-enabled floppy disk and run from there.

The problem has to do with the minimal amount of memory on the *Amstrad* machines which were used for testing. On any more modern machine there will be no problem, as much more memory is usually available.

Stiller Research Integrity Master v3.02a

ItW Boot	94.2%	Standard	86.4%
ItW File	87.8%	Polymorphic	26.0%
ItW Overall	90.4%		

As in the last review, *Integrity Master's* In the Wild score is still too low for comfort: indeed, detection rates overall are down on last time. Users should, of course, bear in mind that *Integrity Master* is much more than just a scanner; however, the fact that a scanner is provided should stand for something.

In the extra testing, all viruses used were found in memory, and appropriate advice offered to the user. Also, all boot sector viruses were correctly removed from hard and floppy disks. Disinfection of parasitic viruses is not supported.

Symantec Norton AntiVirus v3.10

ItW Boot	100.0%	Standard	89.8%
ItW File	99.6%	Polymorphic	95.5%
ItW Overall	99.8%		

Somewhat of an ugly-duckling-to-swan transformation for this product, it would seem: in this review, it clocks very close to the top of the heap in terms of the In the Wild detection rates; a very impressive performance. Indeed, the only sample missed in either ItW set was one of the two samples of Desperado.1403.C.

Scores in the other test-sets are perhaps a little less inspiring: it is clear that *Symantec* is concentrating on the immediate threat, and dealing with In the Wild viruses as a priority.

Trend Micro PC-cillin 95 v5.02, 181

ItW Boot	95.3%	Standard	78.6%
ItW File	95.0%	Polymorphic	82.2%
ItW Overall	95.1%		

Trend's scores stay very much the same this time around. The In the Wild score is clearly the one requiring the most attention, as it places the product joint seventeenth. Missing a Jerusalem variant, for example, is not particularly good.

Extra testing provided interesting results as well: the Burglar sample, like that of *Intel*, could not be run after disinfection (this is unsurprising, as the two products use the same engine). In addition, Manzon was missed in memory, though everything else was detected while active. Everything but Burglar was disinfected correctly.

Conclusions

As usual, the frankly startling amount of data generated by this type of comparative has, of necessity, been compressed for publication. No magazine is big enough to contain the complete, detailed results for every product – and no reader interested enough to read them all anyway. The access database used to store and modify the data, and perform the complex and time-consuming calculations involved, has expanded beyond belief.

However, out of all this information there comes a pleasing general picture of the current state of anti-virus product performance. This, at the very highest level, shows us that detection of In the Wild viruses is improving, and appreciably so. For every product (*MSAV* does not count!) to score over 90% in this category is a fine sight to see, all the more so after the considerable difficulty of introducing detection for *Word* macro viruses.

Having said that, for only one product to get 100% is not quite so inspiring – it is noticeable that many products are certified by one or other (often both) of the two certification schemes out there that only pass the product if it gets 100% on In the Wild viruses. These products do not pass the same test in this review.

False Positives

Overall, the false positive results are improved since the last comparative – the complete results in this area were:

DialogueScience DrWeb	19
RG Software Vi-Spy	9
KAMI AVP	6
Cheyenne InocuLAN	2
H+BEDV AVScan	2
Intel LANDesk	1
Stiller Integrity Master	1
Trend PC-cillin 95	1

Products not listed did not encounter false positives on the collection of clean files used.

Speed

As always, the speed figures invite a variety of different interpretations; however, in terms of raw hard disk scanning speed, it is clear that *Cybec's VET* and *ESaSS' ThunderBYTE* tie for the lead. Once the second scan is taken into account, *IBM AntiVirus* streaks into the lead thanks to an extremely fast checksumming system.

The floppy scan speeds offer the usual intriguing split between those products that run faster on a clean disk, and those that run faster when the disk is infected.

In Closing

One product stands alone in this version of the DOS scanner comparative – *Norman Virus Control* was the only one to score 100% over the In the Wild sets, and it even managed it in the other sets as well. The only slight gripe is the apparent reluctance to detect Junkie and Manzon in memory, but the other test results were very good indeed.

In the Wild Boot Sector Test-set. 86 samples of 86 viruses, one sample each of:

15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot.437, Brasil, BootEXE.451, Bye, Chance.B, Chinese Fish, Crazy_Boot, Da_Boys, DelCMOS.B, Den_Zuko.2.A, Diablo_Boot, Disk_Killer, DiskWasher.A, Empire.Int_10.B, Empire.Monkey.A, Empire.Monkey.B, EXEBug.A, EXEBug.C, EXEBug.Hooker, Flame, Finnish_Sprayer, Form.A, Form.C, Form.D, Frankenstein, FAT Avenger, Galicia, Hare.7750, Ibex, Int40, J&M, Joshi.A, Jumper.A, Jumper.B, Junkie, Kampana.A, Leandro, Michelangelo.A, Mongolian_Boot, Moloch, Music_Bug, Neuroquila, Natas.4744, NYB, Parity_Boot.A, Parity_Boot.B, Pasta, Peter, QRry, Quiver, Quandary, Quox.A, Ripper, Russian_Flag, Sampo, Satria.A, She_Has, Stealth_Boot.B, Stealth_Boot.C, Stoned.16.A, Stoned.Angelina.A, Stoned.Azusa.A, Stoned.Bunny.A, Stoned.Bravo, Stoned.Dinamo, Stoned.Daniela, Stoned.No_Int.A, Stoned.June_4th.A, Stoned.Kiev, Stoned.LZR, Stoned.Manitoba, Stoned.NOP, Stoned.Spirit, Stoned.Standard.A, Stoned.Swedish_Disaster, Stoned.W-Boot.A, Swiss_Boot, Unashamed, Urkel, V-Sign, WelcomB, Wxyc.

In the Wild File Test-set. 435 samples of 125 viruses, made up of:

Anticad.4096.Mozart (4), Alfons.1344 (5), Arianna.3375 (4), Avispa.D (2), Barrotes.1310.A (2), Backformat.2000.A (1), Bad_Sectors.3428 (5), BootEXE.451 (3), Burglar.1150.A (3), Byway.A (1), Byway.B (1), Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Chaos.1241 (6), Chill (1), Changsa.A (5), Concept (4), Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Date (4), Delta.1163 (6), Desperado.1403.C (2), Digi.3547 (5), Die_Hard (2), Dir_II.A (1), DR&ET.1710 (3), DelWin.1759 (3), Fairz (6), Fichv.2_1 (3), Flip.2153 (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.Frodo.A (4), Green_Caterpillar.1575.A (3), Ginger.2774 (2), Goldbug (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Hot (4), Imposter (4), Istanbul.1349 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.1364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian.A (3), Jos.1000 (3), Junkie (1), Kaos4 (6), Karnivali.1971 (3), Keypress.1232.A (2), Laroux (4), Liberty.2857.A (2), Lemming.2160 (5), Little_Red.1465 (2), Macgyver.2803 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon (2), MDMA (4), Mirea.1788 (2), Major.1644 (3), Markt.1533 (3), Nightfall.4518.B (2), Necros.1164 (2), No_Frills.No_Frills.843 (2), No_Frills.Dudley (2), Nomenklatura.A (6), Nop (4), Npox.963.A (2), Natas.4744 (5), Nuclear.B (4), November_17th.800.A (2), November_17th.855.A (2), One_Half.3544 (5), One_Half.3570 (3), Ontario.1024 (3), Pathogen:SMEG.0_1 (5), Ph33r.1332 (5), Phx.965 (3), Pieck.4444 (3), Predator.2448 (2), Quicksilver.1376 (1), Reverse.948 (3), Sarampo.1371 (6), SatanBug.5000.A (2), Sayha (5), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tanpro.524 (6), Tentacle (3), Tentacle.10634 (4), Tequila.A (3), Teraz.2717 (5), Trojector.1463 (6), Trojector.1561 (3), Tai-Pan.438 (3), Tai-Pan.666 (2), Tremor.4000.A (6), Trakia.653 (3), Three_Tunes.1784 (6), Unsnared.814 (3), Vampiro (2), Vacsina.TP-16.A (1), Vacsina.TP-05.A (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Wazzu (4), Werewolf.1500.B (3), Xeram.1664 (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), Yankee_Doodle.XPEH.4928 (2).

Standard Test-set. 532 samples of 257 viruses, made up of:

Anticad.4096.A (4), Abbas.5660 (5), Accept.3773 (5), AIDS (1), AIDS-II (1), Alabama (1), Alexe.1287 (2), Algerian.1400 (3), Amazon.500 (2), Ambulance (1), Amoeba (2), Anarchy.6503 (5), Andreew.932 (3), Angels.1571 (3), Annihilator.673 (2), Another_World.707 (3), Anston.1960 (5), AntiGus.1570 (3), Anthrax (1), Anti-Pascal (5), Argyle (1), Armagedon.1079.A (1), Assassin.4834 (3), Attention.A (1), Auspar.990 (3), Baba.356 (2), Barrotes.840 (3), Backfont.905 (1), Bebe.1004 (1), Big_Bang.346 (1), Billy.836 (3), BlackAdder.1015 (6), Black_Monday.1055 (2), Blood (1), Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger.405.A (1), Burger (3), Butterfly.302.A (1), BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cascade.1704.D (3), Cantando.857 (3), Casper (1), Catherine.1365 (3), CeCe.1998 (6), Cascade.1701.Jo-Jo.A (1), Cliff.1313 (3), CLI&HLT.1345 (6), Coffeeshop (2), Continua.502.B (3), Cosenza.3205 (2), Coyote.1103 (3), Cruncher (2), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cybercide.2299 (3), Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Danish_Tiny.163.A (1), Danish_Tiny.333.A (1), Datacrime_II (2), Datacrime (2), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Diamond.1024.B (1), Dir.691 (1), DOSHunter.483 (1), DotEater.A (1), Dark_Revenge.1024 (3), Destructor.A (1), Datalock.920.A (3), Ear.405 (3), Eddie-2.651.A (3), Enola Gay.1883 (4), Eight_Tunes.1971.A (1), Fellowship (1), Fax_Free.1536.Topo.A (1), Finnish.357 (2), Flash.688.A (1), Feltan.565 (3), Four Seasons.1534 (3), Frodo.3584.A (2), Fisher.1100 (1), Fumble.867.A (1), F-You.417.A (1), Genesis.226 (1), Green.1036 (6), Greets.3000 (3), Greetings.297 (2), HLLC.Halley (1), Hamme.1203 (6), HDZZ.566 (3), Helga.666 (2), HLLC.Even_Beeper.A (1), HLLP.5000 (5), HLLP.7000 (5), Halloechen.2011.A (3), Horsa.1185 (3), Happy_New_Year.1600.A (1), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A (1), Immortal.2185 (2), Invisible.2926 (2), Internal.1381 (1), Itavir.3443 (1), Jerusalem.1607 (3), John.1962 (3), Joker (1), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), July_13th.1201 (1), June_16th.879 (1), Kamikaze (1), Kela.b.2018 (3), Kemerovo.257.A (1), Kranz.255 (3), Kukac.488 (1), Keypress.1280 (6), Leda.820 (3), Lehigh.555.A (1), Leapfrog.A (1), Liberty.2857.A (5), Liberty.2857.D (2), Loren.1387 (2), LoveChild.488 (1), Little_Brother.307 (1), Lutil.591 (3), Maresme.1062 (3), Metabolis.1173 (3), Mickie.1100 (3), Necropolis.1963.A (1), Nina.A (1), NRLG.1038 (3), NutCracker.3500.D (5), November_17th.768.A (2), Omud.512 (1), On_64 (1), Oropax.A (1), Parity.A (1), Peanut (1), Perfume.765.A (1), Phantom1 (2), Pitch.593 (1), Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Phoenix.800 (1), Pojer.4028 (2), Poison.2436 (1), Positron (2), Prudents.1205.A (1), PS-MPC.227 (3), PS-MPC.545 (6), Power_Pump.1 (1), Quark.A (1), Red_Diavolyata.830.A (1), Revenge.1127 (1), Riihi.132 (1), Rmc.1551 (4), Rogue.1208 (6), Saturday_14th.669.A (1), SVC.1689.A (2), Screaming_Fist.927 (4), SillyCR.710 (3), Screen+1.948.A (1), Stardot.789.A (6), Stardot.789.D (2), Semtex.1000.B (1), Senorita.885 (3), Shake.476.A (1), ShineAway.620 (3), SI.A (1), SillyC.226 (3), SillyCR.303 (3), Sofia.432 (3), Spanz.639 (2), Starship (5), Subliminal (1), Suomi.1008.A (1), Suriv_2.B (1), Suriv_1.April_1st.A (1), Surprise.1318 (1), Svir.512 (1), Svin.252 (3), SysLock.3551.H (2), Sylvia.1332.A (1), TenBytes.1451.A (1), Terror.1085 (1), Thanksgiving.1253 (1), The_Rat (1), Tiny.133 (1), Tiny.134 (1), Tiny.138 (1), Tiny.143 (1), Tiny.154 (1), Tiny.156 (1), Tiny.159 (1), Tiny.160 (1), Tiny.167 (1), Tiny.188 (1), Tiny.198 (1), Todor.1993 (2), Traceback.3066.A (2), TUQ.453 (1), Untimely.666 (3), V2P6 (1), Vbasic.5120.A (1), VCS1077.M (1), Vacsina.1212 (1), Vacsina.1269 (1), Vacsina.1753 (1), Vacsina.1760 (1), Vacsina.1805 (1), Vacsina.2568 (1), Vacsina.634 (1), Vacsina.700 (2), Vcomm.637.A (2), VFSI (1), Vienna.583.A (1), Vienna.623.A (1), Vienna.648.Lisbon.A (1), Victor (1), Vienna.Bua (3), Vienna.Monxla.A (1), Virus-101 (1), Virus-90 (1), Virogen.Pinworm (6), Vienna.W-13.507.B (1), Vienna.W-13.534.A (1), Vienna.W-13.600 (3), Voronezh.600.A (1), Voronezh.1600.A (2), VP (1), V2Px.1260 (1), Warchild.886 (3), Warrior.1024 (1), Whale (1), Willow.1870 (1), WinVir (1), WW.217.A (1), XQG.133 (3), Yankee_Doodle.1049 (1), Yankee_Doodle.2756 (1), Yankee_Doodle.2901 (1), Yankee_Doodle.2932 (1), Yankee_Doodle.2981 (1), Yankee_Doodle.2997 (1), Zherkov.1023.A (1), Zero_Bug.1536.A (1).

Polymorphic Test-set. 11,000 samples; 500 each of the following 22 viruses:

Alive.4000, Anarchy.6503, Code.3952:VICE.05, Cordobes.3334, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove and Coffee_Shop, MTZ.4510, Natas.4744, Neuroquila.A, Nightfall.4559.B, One_Half.3544, Pathogen:SMEG.0_1, PeaceKeeper.B, Russel.3072.A, SatanBug.5000.A, Sepultura:MtE-Small, SMEG_v0.3, Tequila.A, Uruguay.4.

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**