COMPARATIVE REVIEW

What's up, DOS?

The last *Virus Bulletin* DOS comparative was in July 1997. Of the eighteen products up for testing this time around, sixteen of them featured in that last review. The two newcomers this month are both Eastern European – *AVG* from the Czech company *Grisoft*, and *NOD-iCE* from the Slovak Republic's *ESET*. This is also the first *VB* review to feature the revamped *Data Fellows F-Secure Anti-Virus*.

As with other recent *VB* DOS comparatives, the focus of this review is on detection rate and speed. This review does introduce a change, however. Over the last few years, *VB* has run DOS comparatives approximately six-monthly, but this is the only such comparative for 1998. With the Win32 platforms (*Windows 95* and *NT*) firmly in the ascendancy, and their increasing importance throughout the business and personal computing sectors, we have decided to focus our attention more on these platforms, providing two comparatives for each, every year.

There were no limitations on the software we asked the vendors to submit, other than that they had to run as DOS applications. Some developers still ship a separate macro virus scanning program with their 'normal' scanner as the only (or most reliable) way of detecting these increasingly important viruses

Including separate scanning components can be seen as a positive or a negative thing. Whilst a macro-only scanner could be a useful option in some circumstances, most computer users seem to want a complete anti-virus solution. Reflecting this, we tested the most appropriate component of multi-scanner packages against each test-set. As the In the Wild File set contains both parasitic executable infectors and macro viruses, this means that some otherwise good packages cannot score a 'perfect' 100%. These products are thus precluded from attaining the coveted VB 100% award through a design decision.

The Tests

The speed tests in this review were carried out on a Pentium machine with 64 MB of RAM. When speed was not an issue, a variety of other machines were also used – the aim being to produce the results in a reasonable period of time by sheer weight of numbers.

For the detection test, the virus test-sets were stored in a read-only directory on a *NetWare* server and the samples were tested one by one. This required more than 15,000 file copies and scanner launches per product test. For those products that did not have an 'append to an existing file' logging option, a similar number of file copy operations were needed to preserve the report file. This testing procedure provides a more accurate indication of 'real world' detection rates. Some products are known to boost their detection rate in test situations by increasing their level of heuristic analysis once a certain number of different viruses are detected. Our test is designed to circumvent this, whilst testing products with their default settings.

The default detection settings were used, and as far as possible, all other settings were optimized to our testing procedure. Thus, memory and boot sector scanning, program self-checks, and the like, were disabled. Report logs were made, complete with missed files where possible, and the whole process automated through a series of batch files and *NetWare* login scripts. Products with separate macro scanners presented a few minor complications to the procedure. Throw in a couple of server crashes during the actual testing run and a fine time was had by all!

The test-sets were updated so that the In the Wild Boot and File sets matched the October 1997 WildList as closely as possible. The product submission date for inclusion in this review was 31 October 1997. A Web location containing a complete listing of the test-sets is included in the technical summary box at the end of the review.

Speed tests were conducted against a selection of clean files on a local hard drive. This most closely reflects 'typical' operation in the real world. The Clean test-set consists of 5500 executables, comprising approximately 540 MB. The contents have been culled from common DOS and *Windows* applications, and from publicly accessible collections of freeware and shareware utilities. As well as being a speed test, this doubles as a false positive test – there are no viruses in this collection, so none should be found.

Alwil AVAST! v7.70.10 31 Oct 1997

ItW Boot	100.0%	Macro	97.7%
ItW File	95.9%	Polymorphic	100.0%
ItW Overall	97.3%	Standard	98.8%

Slipping a couple of percentage points on the In the Wild Overall and Standard test-set ratings, *AVAST!* has made up ground on the Macro test. It is always encouraging to see a product boost its score to 100% on the Polymorphic set, which is the most technically challenging. The viruses missed from the In the Wild File test-set were mainly *Word 8* and *Excel* macro viruses, though some samples of each kind were detected, so AVAST! can deal with viruses of these types.

Alwil's scanner placed half-way through the field on the speed test. Although not excitingly fast, this represents quite a respectable performance, and as would be hoped, it did not claim to find any viruses in the Clean set.

	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST!	91	100.0%	632	95.9%	97.3%	730	97.7%	13000	100.0%	806	98.8%
Command F-PROT Pro	91	100.0%	583	88.6%	92.5%	716	95.9%	7138	50.8%	730	92.2%
Cybec VET	91	100.0%	422	66.1%	77.6%	730	98.5%	12998	99.0%	804	98.4%
Data Fellows FSAV	91	100.0%	654	100.0%	100.0%	741	100.0%	12917	97.6%	819	100.0%
DialogueScience Dr Web	89	97.8%	648	99.2%	98.8%	741	100.0%	13000	100.0%	800	98.1%
Dr Solomon's AVTK	91	100.0%	654	100.0%	100.0%	741	100.0%	13000	100.0%	819	100.0%
Eliashim ViruSafe	88	96.7%	646	98.9%	98.1%	726	97.9%	12962	97.9%	810	99.4%
ESET NOD-iCE	91	100.0%	647	98.5%	99.0%	729	98.3%	13000	100.0%	816	99.7%
Grisoft AVG	86	94.5%	560	86.2%	89.0%	660	88.2%	10548	81.0%	572	78.4%
IBM AntiVirus	91	100.0%	654	100.0%	100.0%	741	100.0%	12500	96.2%	819	100.0%
iRiS AntiVirus	90	98.9%	645	98.8%	98.8%	699	94.5%	12103	91.9%	813	99.3%
KAMI AVP	91	100.0%	654	100.0%	100.0%	741	100.0%	12917	97.6%	819	100.0%
McAfee VirusScan	91	100.0%	654	100.0%	100.0%	741	100.0%	12797	93.1%	801	98.8%
Norman ThunderByte	91	100.0%	654	100.0%	100.0%	738	99.6%	13000	100.0%	799	98.5%
Norman Virus Control	91	100.0%	654	100.0%	100.0%	737	99.5%	13000	100.0%	813	99.4%
Sophos SWEEP	91	100.0%	654	100.0%	100.0%	741	100.0%	13000	100.0%	817	99.7%
Symantec Norton AntiVirus	91	100.0%	648	99.4%	99.6%	740	99.9%	11498	87.5%	773	97.0%
Trend Micro PC-cillin	84	92.3%	638	97.6%	95.8%	676	91.3%	12383	93.6%	790	97.4%

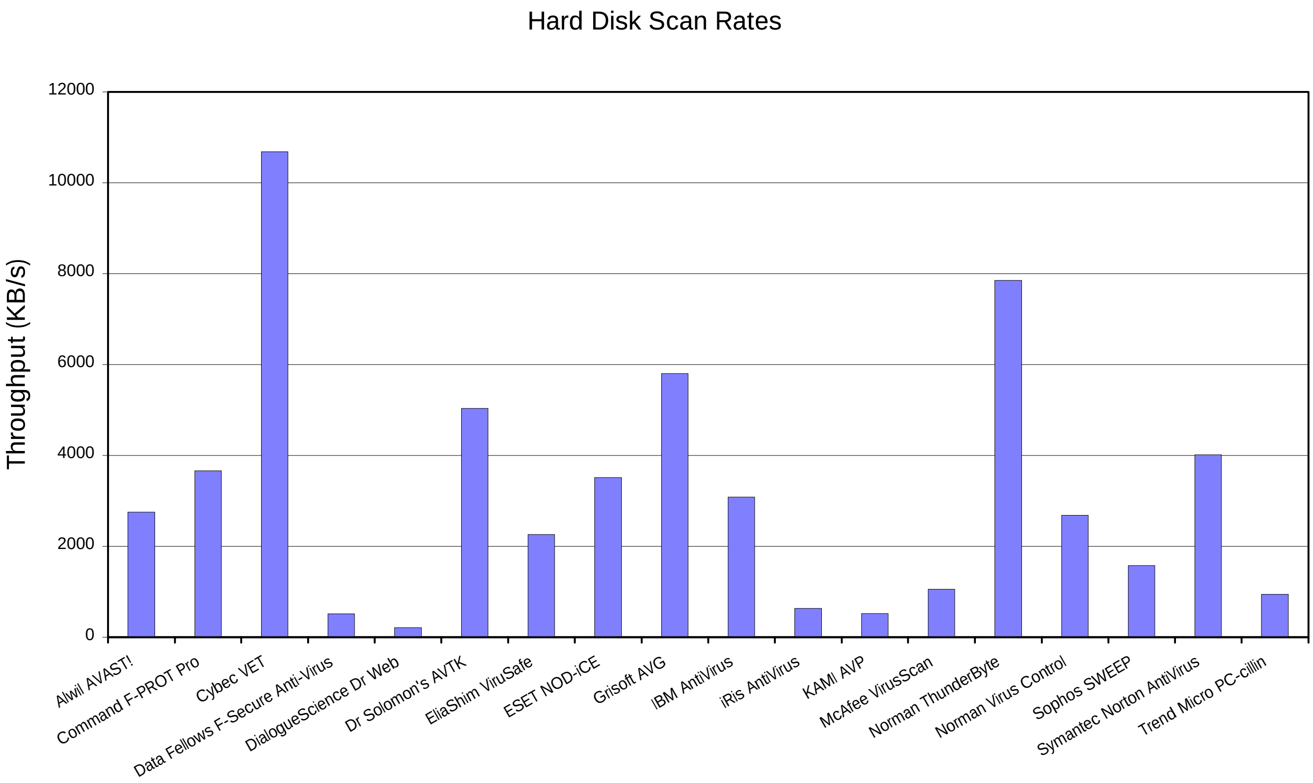
Command F-PROT Professional v2.27a

ItW Boot	100.0%	Macro	95.9%
ItW File	88.6%	Polymorphic	50.8%
ItW Overall	92.5%	Standard	92.2%

The *F-PROT* engine is currently bordering on a major upgrade, for which beta versions are in circulation. When finally released, that version should improve upon the somewhat disappointing performance seen here. *Command F-PROT Professional's* In the Wild File detection rate is depressed by the current lack of a built-in macro virus scanner, while polymorphic detection suffers from an aged emulator (an area the much-heralded v3.0 is claimed to improve significantly).

The main scanner detects many macro viruses, but does so using simple string scanning techniques. This is an unreliable approach, as the partial detection of the WM/NOP.A and WM/Pesan.B samples in the In the Wild set showed. The separate macro scanner provides much more reliable (and comprehensive) detection, although one cannot help feeling that the version supplied for review was possibly a little outdated. The v3.0 engine is also claimed to combine the macro and executable scanner. The next DOS comparative should show a marked improvement in this product.

Whilst not lightning fast, a hard disk scanning speed approaching 4000 KB/s throughput is quite nippy, placing *Command F-PROT* just in the top third of products tested. No false positives were reported.



Cybec VET v9.53

ItW Boot	100.0%	Macro	98.5%
ItW File	66.1%	Polymorphic	99.0%
ItW Overall	77.6%	Standard	98.4%

Cybec's VET traditionally rates well in *VB* tests. However, the lack of any form of macro virus detection in the main DOS scanner is starting to take its toll on *VET's* detection rate against the In the Wild File set, as the proportion of macro viruses in that test-set climbs. VETMACRO , the separate macro scanner turned in a slightly improved result over its last outing against the Macro test-set, but still missed all samples of the Delta, Legend and RoboCop Excel viruses. *Cybec* has informed *VB* that it will combine its DOS macro and executable scanners in version 9.6.

Following the speed tests, *VB* staff were left wondering what the Australian developers of *VET* eat for breakfast. Typically amongst the top three speedsters, *VET* blitzed the field in this test. In outpacing its nearest rival (the traditionally speedy *Norman ThunderByte*) by more than 20%, it registered an effective data throughput rate of 10682 KB/s. Reporting no false positives, *VET* displayed a good combination of speed and accuracy.

Data Fellows F-Secure v3.0 Build 115

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	97.6%
ItW Overall	100.0%	Standard	100.0%

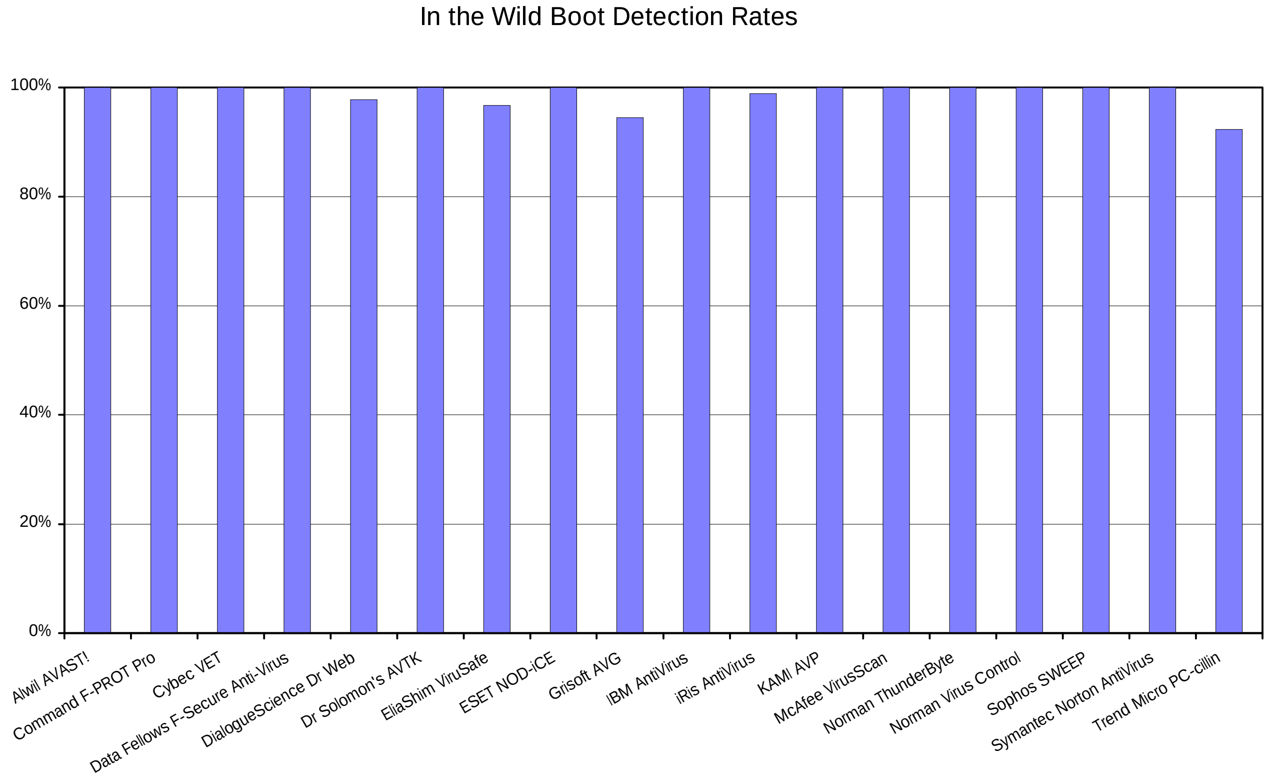
Data Fellows revamped its anti-virus software line late in 1997, combining the *F-PROT* and *AVP* scanning engines. The resulting product line goes by the name of *F-Secure Anti-Virus (FSAV)*, and this is its first appearance on any platform in a *VB* review. In the *FSAV* DOS scanner, *Data Fellows* has elected to include only the *AVP* engine. This accounts for the notable improvement over July's performance, resulting in a VB 100% award. Registering 100% against all but the Polymorphic test-set does not leave much room for further progress against the current *VB* test-sets.

This high detection rate comes at quite a price in terms of speed, however. At less than 5% of the scan speed of *Cybec's VET*, *FSAV* was in the slowest quarter of products, though still twice as fast as the slowest.

DialogueScience Dr Web v3.26 28 Oct 1997

ItW Boot	97.8%	Macro	100.0%
ItW File	99.2%	Polymorphic	100.0%
ItW Overall	98.8%	Standard	98.1%

DialogueScience specializes in detecting 'difficult' viruses, and *Dr Web* turns in another stalwart job in the trickier sets here. With perfect polymorphic and macro detection, the other holes in detection need only a little improvement. *Dr Web* depends heavily upon heuristic analysis, and while this often allows it to find new viruses other products miss, the performance overhead is very noticeable when scanning clean files. It seems that *Dr Web* runs some portion of most



program files through its emulator before 'rejecting' them as not infected. This results in remarkably different performance from the speed demons like *VET* and *Norman ThunderByte*. They seem to have optimized reaching the conclusion 'there is no point going further' and thus quickly move on when scanning clean files. *Dr Web* is quite the slowest of the packages tested, and recorded nineteen false positives in its cogitation upon the clean set.

The documentation states that the default settings are not good enough to detect some highly complex polymorphics, and suggests that extra time is needed for this on top of the standard. The *Dr Web* scanner is really designed to be used in conjunction with *DialogueScience's ADinf* integrity checker and, working in this combination, the slow but thorough scanning would not be a major problem.

Dr Solomon's AVTK v7.77 13 Oct 1997

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

At times like this it can be difficult to make reviews interesting reading. 100% against all test-sets! As for detection, what more can be said? This is the first time this has happened since we introduced the macro test-set in the July DOS comparative last year, and ony the second time in recent history that a product has swept the table in a *VB* test. The *AVTK*, of course, receives a VB 100% award!

With very little room for improvement from its last outing in a DOS comparative, this product still managed the feat. Although not the absolute fastest of scanners, *Dr Solomon's AVTK* combines very good scanning speed with excellent detection across the board.

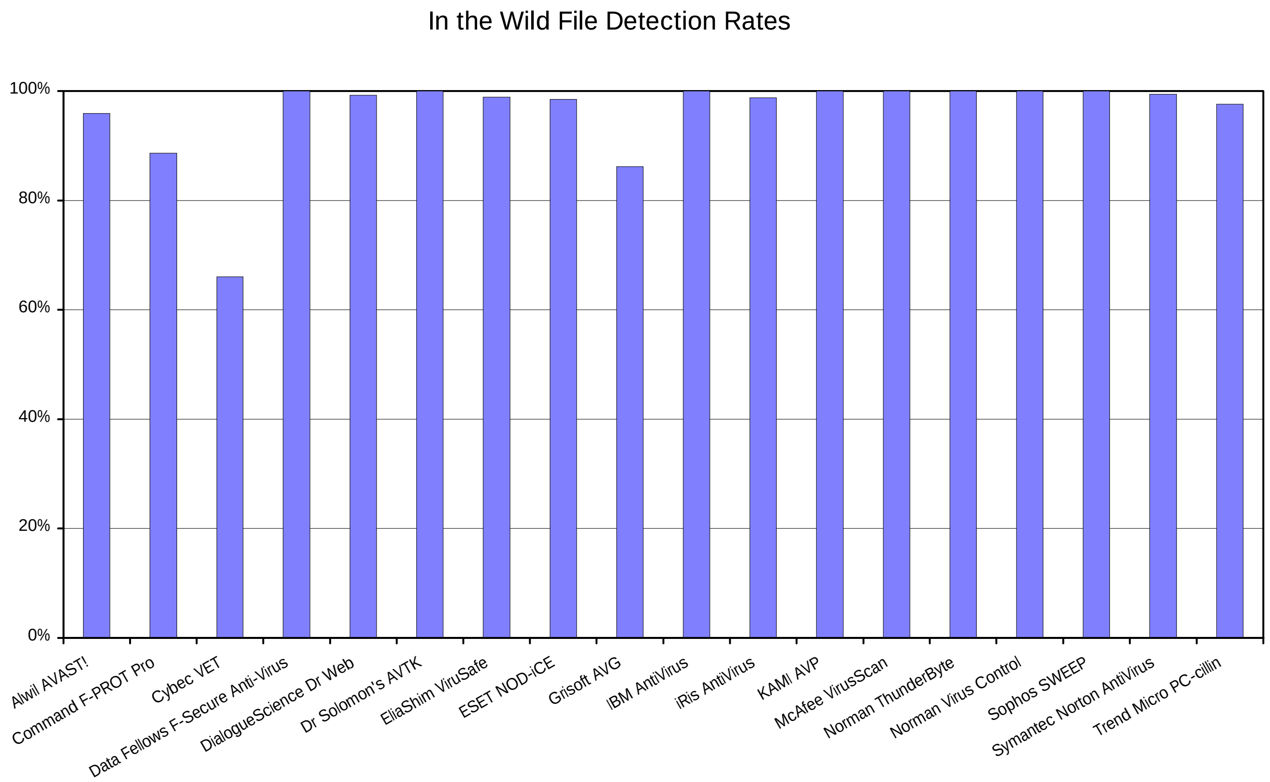
EliaShim ViruSafe v7.53

ItW Boot	96.7%	Macro	97.9%
ItW File	98.9%	Polymorphic	97.9%
ItW Overall	98.1%	Standard	99.4%

Showing a pleasing improvement against the Macro and Polymorphic test-sets since the last DOS comparative, overall*ViruSafe* still places just out of the top rankings. A couple of relatively new macro viruses (WM/Pesan.B and WM/Schumann.C:De) blocked a perfect In the Wild File score and the three Hare variants in the In the Wild Boot test-set upset that apple-cart. In the Macro test-set it was again the comparatively new viruses (like Header.A and Mess.A) that were missed.

A more immediate cause for concern is the false positive tally of twenty-five. *ViruSafe* claimed all of them to be Cruncher.4000, so perhaps a little more work needs to be done on its definition of this virus.

While not in the top 50% of performers as far as scanning speed is concerned, *ViruSafe's* 2263 KB/s throughput is at the respectable end of the slower half of scanners. Although noticeably slower than the real speedsters, this is probably still an acceptable scanning speed for most purposes.



ESET NOD-iCE v7.19

ItW Boot	100.0%	Macro	98.3%
ItW File	98.5%	Polymorphic	100.0%
ItW Overall	99.0%	Standard	99.7%

The first of the two new vendors to feature in this comparative review, *ESET* submitted a product that performed, perhaps surprisingly, well. We have noticed in the past how new products often take some settling in, but this has apparently already happened with *NOD-iCE*, which scored higher than some of the *Virus Bulletin* regulars. The version number presumably indicates a long development history and that the product is at least as well-established in its country of origin as any Western counterparts with similarly ‘advanced’ version numbers.

Missing some of the HLLP.5850.C, and the WM/Hiac.A and W97M/Wazzu.A samples from the In the Wild File test-set was all that stood between NOD-iCE and its first VB100% award. All are recent entrants to the top of the WildList. This must be a pleasing, if slightly frustrating, result for the product’s Czech developers. They have clearly got the fundamentals right, and we will be watching with interest to see how this product evolves over the course of future *Virus Bulletin* tests.

In terms of speed, *NOD-iCE* placed seventh fastest of the eighteen products tested, with a respectable 3514 KB/s throughput. Unfortunately, the excellent overall detection rate was offset somewhat by the detection of one ‘virus’ in the Clean test-set.

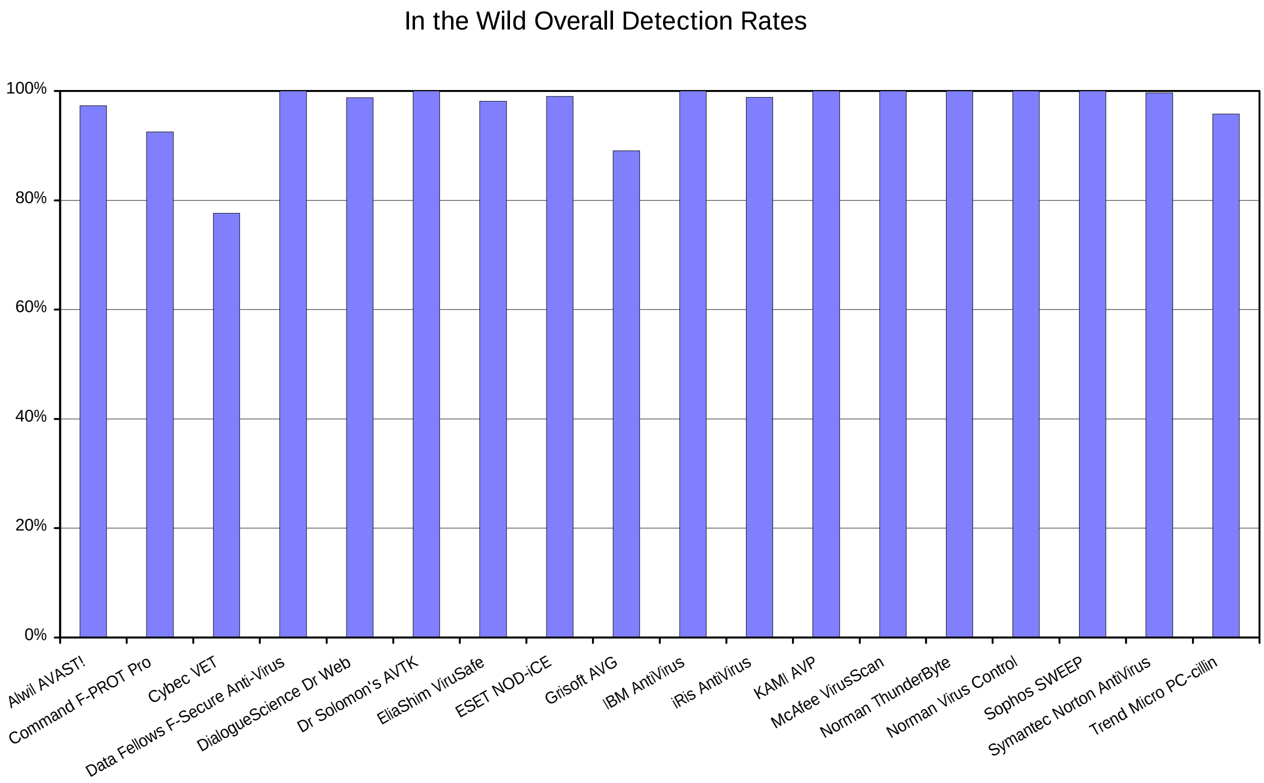
Grisoft AVG v5.0

ItW Boot	94.5%	Macro	88.2%
ItW File	86.2%	Polymorphic	81.0%
ItW Overall	89.0%	Standard	78.4%

The other new vendor to submit a product for this review is the Slovakian anti-virus company *Grisoft. AVG* is smartly-presented, and has a notably well-translated manual. Having said that, performance with out-of-the-box settings leaves quite some room for improvement. Careful selection of scanning options can certainly result in better detection than seen in our tests, but, as usual, we tested with the default settings.

AVG’s relatively poor showing on the ItW File test-set was initially a little disappointing. Most of the viruses it missed entered the WildList in the two months prior to the product submission date for this test, but as usual, we used the current WildList at submission date. This, coupled with its poorer showing on the Standard test-set, suggests the developers focus on detection of ‘in the wild’ viruses. The macro viruses missed in both the ItW File and Macro test-sets were mainly new, *Word 8*, or *Excel* viruses. Detection of polymorphic viruses tended to be an all-or-nothing affair. *AVG* missed all 500 samples of each of Baran.4968, Cryptor.2582, Mad.3544 and Neuroquila.A, 452 samples of DSCE.Demo, and detected all of the rest.

As you would hope, no false positives were registered against the Clean test-set. At just over 5800 KB/s throughput, *AVG* returned the third fastest hard disk scan time. This



result would likely be different should more thorough detection options be enabled by the user. *Virus Bulletin* did not formally test any of these options.

IBM AntiVirus v3.0w

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	96.2%
ItW Overall	100.0%	Standard	100.0%

IBM AntiVirus receives this month's third VB 100% award, their first to date. The product detected all samples of all viruses in the *Virus Bulletin* test-sets except for the 500 samples of Cryptor.2582 in the Polymorphic set.

IBM supplies a command-line scanner and a combined checksummer and scanner in a full-screen, menu-driven program. The command-line scanner was used for all tests in this review. The full-screen program traditionally returns very fast 'scan' speeds because it only virus-scans files whose checksums do not match those calculated on the checksummer's first run. Using the command-line scanner, *IBM AntiVirus'* scan speed was in the middle of the field. It is no surprise that no false positives were reported.

iRiS AntiVirus v22.02 30 Oct 1997

ItW Boot	98.9%	Macro	94.5%
ItW File	98.8%	Polymorphic	91.9%
ItW Overall	98.8%	Standard	99.3%

Hare.7610 from the In the Wild Boot test-set, some file replicants of its sibling, Hare.7786, and two of the macro viruses new to the WildList in October, were all iRiS AntiVirus missed from the In the Wild test-sets. This test shows a marked improvement in detection of viruses in the Macro test-set and a small improvement against the Polymorphic set, over last July's DOS comparative result. At 629 KB/s throughput, *iRiS AntiVirus* is the fourth slowest scanner on our Clean test.

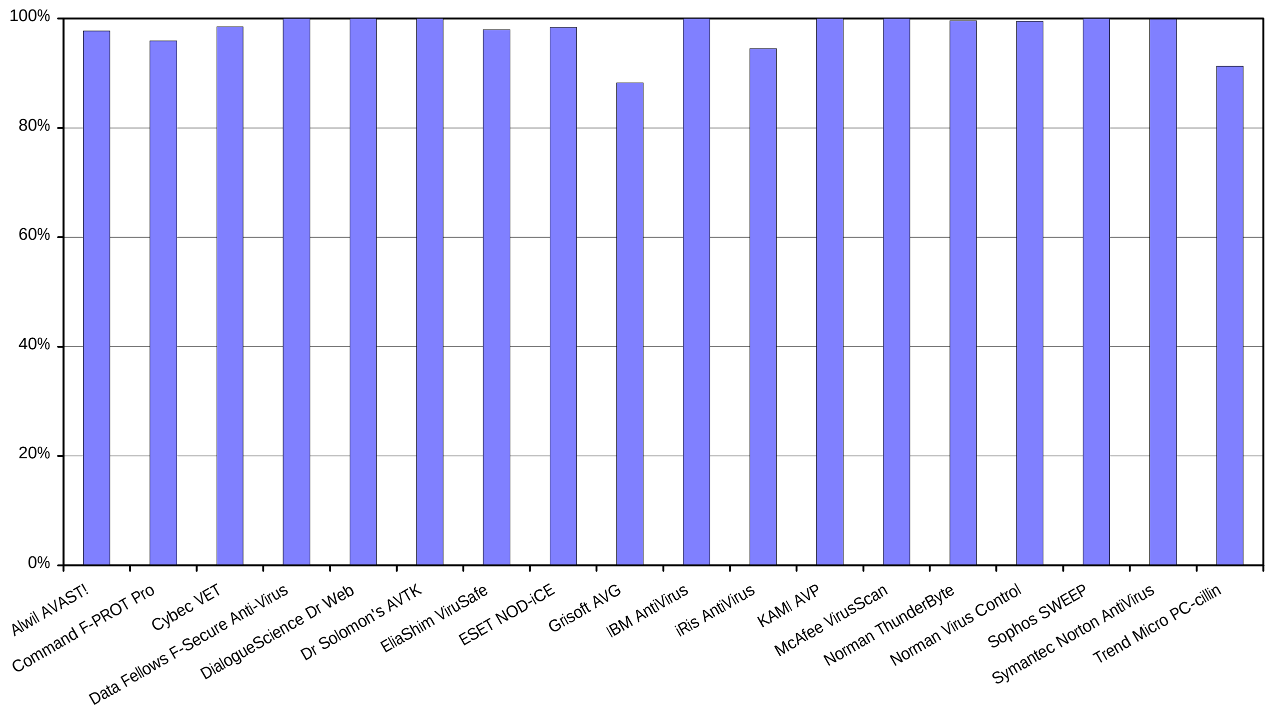
The slow speed was coupled with two false positives. Normally something to be concerned about, this represents progress compared to some of the false positive results *VB* has reported from *iRiS* in the past year.

KAMI AVP v3.0 Build 115

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	97.6%
ItW Overall	100.0%	Standard	100.0%

As already mentioned, the *AVP* scanning engine is now incorporated in *Data Fellows F-Secure AntiVirus*. It should not, therefore, be surprising that *KAMI*, *AVP's* Russian developers, received the fourth VB 100% award. The results are exactly the same as for the *Data Fellows* submission, reflecting the fact that the same engine version was used in each product. The only areas of any concern in these tests were the scanning speed, a handful of Cryptor.2582 replicants and one DSCE.Demo replicant.

Macro Detection Rates



McAfee VirusScan v3.1.2 13 Oct 1997

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	93.1%
ItW Overall	100.0%	Standard	98.8%

Receiving this review's fifth VB 100% award, *McAfee VirusScan* has improved slightly in both its In the Wild File and Macro test-set detection rates. This continues a trend of better detection seen over the last few *Virus Bulletin* comparatives.

VirusScan's progress has been associated with worsening speed, and this test shows no indication of this being reversed. Recording 1059 KB/s throughput, it was the sixth slowest scanner in the pack. It reported no false positives.

Norman ThunderByte v8.04 31 Oct 1997

ItW Boot	100.0%	Macro	99.6%
ItW File	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	98.5%

The first of three products to attain their second VB 100% award, *Norman ThunderByte* turned in a typically sterling performance on the In the Wild test-sets.

These results show an advance in detection of the polymorphic test-set, now fully detecting the stems it has only partially detected in previous tests. *VB's* repeated publication of test results reporting that *ThunderByte* did not fully detect SMEG_V0.3 spurred its developers in Holland to take a long, hard look at their handling of this virus. After several days work following publication of the previous DOS comparative, they reported to the *VB* editor that they had improved their SMEG detection and expected to get 100% on that stem in the next test.

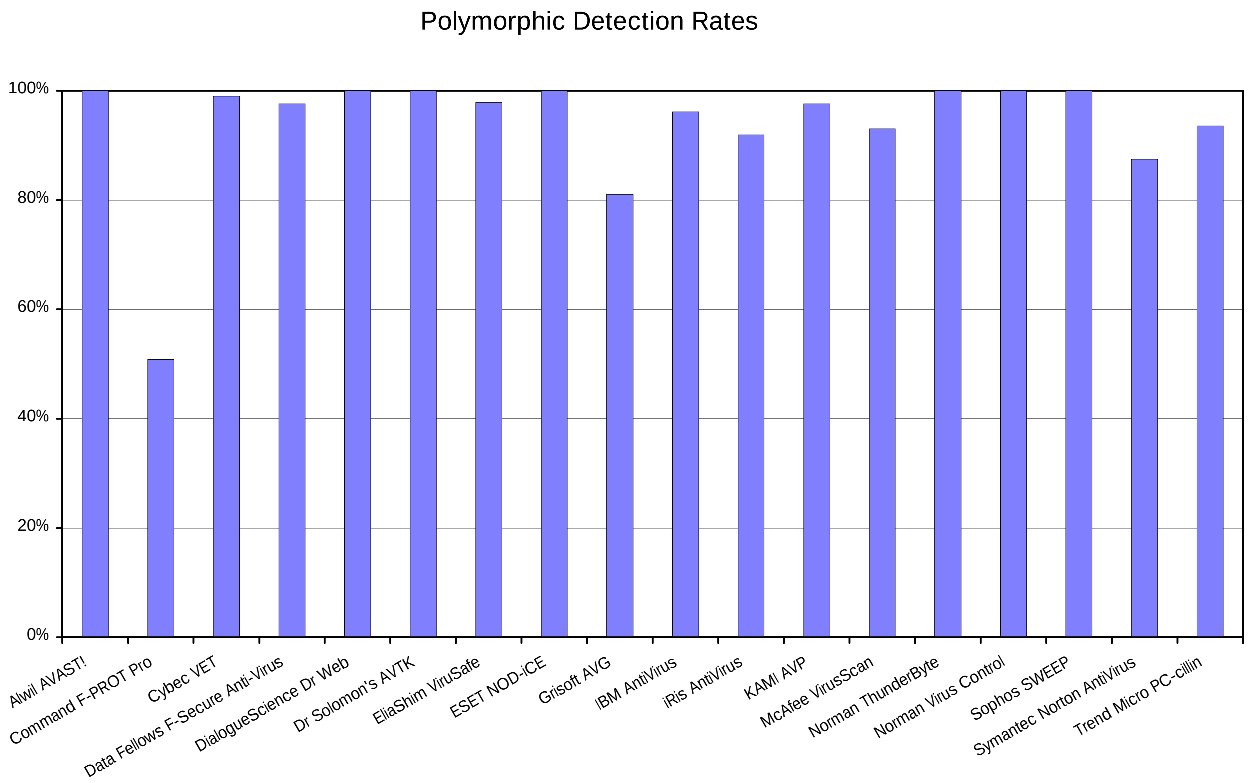
A good 30% ahead of the third fastest product, *ThunderByte* returned a scan speed of 7855 KB/s. This placed it second behind *Cybec's VET*. One false positive was reported, which marred an otherwise excellent performance.

Norman Virus Control v4.30

ItW Boot	100.0%	Macro	99.5%
ItW File	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	99.4%

This VB 100% award is the second attained by the Norwegian product, *Norman Virus Control*. Its performance was every bit as commendable as that of its stablemate. Despite returning outwardly similar results, the two products use quite different scanning engines.

There was only one virus in the Macro test-set that either of the *Normans* missed, and in fact both of them missed at least some samples of it. This was the *Excel* macro virus RoboCop.A – *Norman Virus Control* missed all four samples, whereas *ThunderByte* detected one of the four. Another indication of the scanning engines being different was that *Norman Virus Control*'s scanning speed was



substantially slower. In fact, it placed right in the middle of the field, with a throughput of 2684 KB/s. Yet another pointer to differences between the products was that *Norman Virus Control* correctly failed to detect any viruses in the Clean set.

Sophos SWEEP v3.03 3 Nov 1997

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	99.7%

Sophos has earned itself another VB 100% award in this review, turning in near-perfect detection across the test-sets. The only virus *SWEEP* missed was both samples of Positron in the Standard set. The developers point out that *SWEEP* detects this virus in 'full sweep' mode, and they do not intend to change this.

Not surprisingly, *SWEEP* did not report any false positives in the Clean test-set. Although not the fastest scanner in this review, placing seventh slowest, *SWEEP* is faster than several of its competitors which boast similarly impressive detection rates.

Symantec Norton AntiVirus v4.0 1 Nov 1997

ItW Boot	100.0%	Macro	99.9%
ItW File	99.4%	Polymorphic	87.5%
ItW Overall	99.6%	Standard	97.0%

Symantec missed out on a VB 100% award by missing all the samples of HLLP.5850.D from the In the Wild File test-set. A slight improvement was seen on the Macro and Polymorphic sets, and a marked improvement was noted against the Standard test-set as compared to the results of the last DOS review in July 1997.

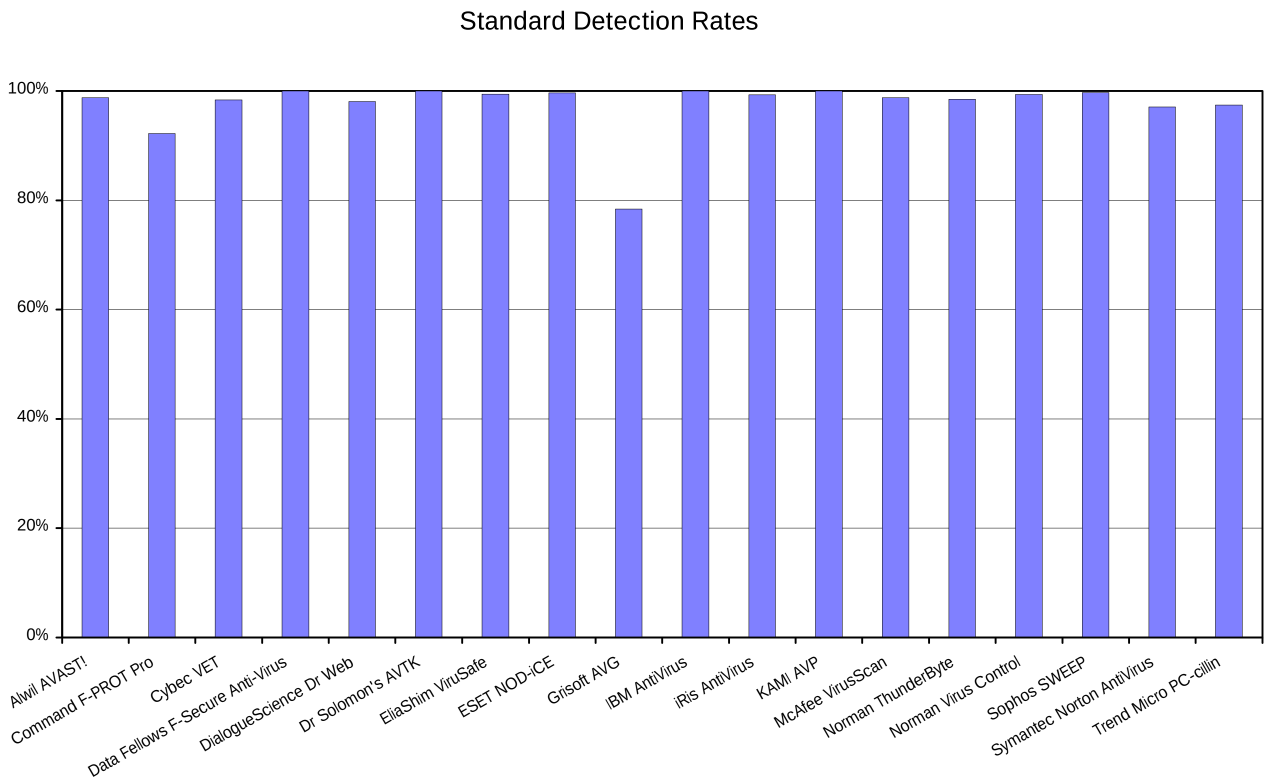
With a throughput of just over 4000 KB/s, *Norton AntiVirus* was the fourth fastest product on the scanning speed tests, notably faster than the next best performance. No false positives were reported when scanning the Clean test-set.

Trend Micro PC-cillin v6.01 VPN 332

ItW Boot	92.3%	Macro	91.3%
ItW File	97.6%	Polymorphic	93.6%
ItW Overall	95.8%	Standard	97.4%

The first problem encountered with *PC-cillin* was that without altering the BIOS settings, it was impossible to run the program. In fact, in our test machines default configuration, this was the largest system rebooter that we have seen. The problem was resolved by enabling the 'memory hole' at the 16 MB boundary, and appeared to be associated with the DOS extender used by the product.

This apart, the results were workman-like, but not exactly thrilling stuff. Having said that, *PC-cillin* has made notable progress against *VB's* Macro, Polymorphic and Standard test-sets. However, it has slipped slightly against both In the Wild test-sets, which is interesting given that the product is listed as currently maintaining both *ICSA Certification* and



the *Secure Computing Checkmark*. This discrepancy is not peculiar to *PC-cillin*, and is normally explained by the above certification bodies using more aged WildLists as the basis of their ‘current’ tests.

No speed leader, *PC-cillin* was sixth slowest in the scan speed tests, returning a throughput of 947 KB/s. Its performance in the Clean test-set was disappointing, claiming to have found four viruses there.

Conclusion

The relative stasis of the *Virus Bulletin* test-sets (other than the ItW Boot and File sets) over the last year is starting to show. This needs to be addressed by beefing up the non-ItW sets, which is now a priority. That said, all credit to the eight products that attained the VB 100% standard. This is as good a ‘common ground’ for required detection as the industry has. Short-listing products that consistently achieve 100% (or *very* close) detection of these viruses should be a good choice, then select based on other features.

To recap, the eight VB 100% award recipients from this review are *Data Fellows F-Secure Anti-Virus 3.0.115*, *Dr Solomon’s AVTK v7.77*, *IBM AntiVirus v3.0w*, *KAMI AVP v3.0.115*, *McAfee VirusScan v3.1.2.3010*, *Norman ThunderByte v8.04*, *Norman Virus Control v4.3* and *Sophos SWEEP v3.03*.

Special mention is due to those products scoring 100% on at least three of the four complete test-sets. These are *Data Fellows FSAV*, *IBM AntiVirus*, *KAMI AVP* and *Sophos SWEEP*. Of particular note is *Dr Solomon’s Anti-Virus Toolkit*, which scored 100% on all the *VB* test-sets – a first since adding the Macro set back in July 1997.

The days of DOS, and hence of DOS virus scanners, are probably limited now. As *Virus Bulletin’s* tests of products on other platforms have consistently shown, vendors whose DOS products score well do not necessarily score as well on other platforms. This is despite the much-repeated litany of ‘the exact same scan engine is used in all products’. Many low-level, OS technicalities complicate the issues for anti-virus software, so if you are looking for a cross-platform solution, you should choose looking at test results across all platforms of interest.

Technical Details

Test Environment: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12.* Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy; One *Compaq* DeskPro XE 466, 16 MB RAM, 207 MB disk, all running MS-DOS 6.22 and *NetWare* ODI/VLM drivers. 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 and it was not connected to the network for the duration of the timed tests.

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/DOS/199802/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW

Trend Micro Server Protect for Windows NT v4.50

Martyn Perry

Trend Micro's products have often featured in *Virus Bulletin's* comparative tests, but not in a standalone review. This month we rectify that by seeing how *Server Protect for Windows NT v4.50* performs under close scrutiny.

Presentation and Installation

To dispense with the preliminaries, a licence is required for each server on which the software is installed. *Server Protect* comes boxed with an Installation Guide, User's Guide and four diskettes. It requires a 486 or higher, with a recommended minimum of 32 MB RAM, 5 MB of disk space and *NT 3.51* or later.

The installation process has a familiar feel to it, due to the use of *Installshield*. Initially, the software scans the boot sector, and providing all is well, prompts for the licence number, which can be found on the first diskette. A destination directory is prompted for (the default is 'C:\Program Files\Trend\Sprotect'), and Select Program Group gives a choice between Create Personal Program Group and Create Common Program Group (the default). This determines whether only one person can access the *Server Protect* program group or if other users can access it. Program icons can be added now with Select Program Folder.

Server Protect is designed to work in a domain of servers, with one primary server that can be used to update all the others. Several options relating to these features are presented during installation. For this review I set up the test machine as an Information Server in the *Server Protect* domain TRENDTEST. The next set of options determines the scanner's initial configuration. For example, Configure Server Protect gives a choice of actions to take in the event of virus detection. There is also an option to set up the real-time scan direction (Incoming/Outgoing).

After answering all the configuration questions, program files are copied and registry entries changed. Before completing installation, it is necessary to logon to an account, either by default with Default System Account, or with a password to a specific account. At this stage, the program group shows the ISUtilty icon (for Information Server management) and the *Server Protect* icon.

The installation guide appears to have been created independently from the software, or perhaps for a different version, as there are obvious inconsistencies. Fortunately, this does not cause any problems since the installation options are fairly self-explanatory.

Server Protect for Windows NT v4.50

Server Protect can provide domain management for servers. These domains are grouped under specific 'Information Servers' (IS), which sit at the top of a control hierarchy. Each IS is responsible for storing the configuration of all the domains included in its group, and for validating the password, user name and any logon restrictions.

With so much of the domain management functionality focused on Information Servers, it is good to see that *Trend Micro* makes a safety provision whereby the IS can be backed up periodically and the time interval set to hours, minutes and seconds. In addition to this, there is a separate utility (ISUtility) for managing Information Server functions which include assigning a new IS, merging existing ones, backing them up, and rebuilding.

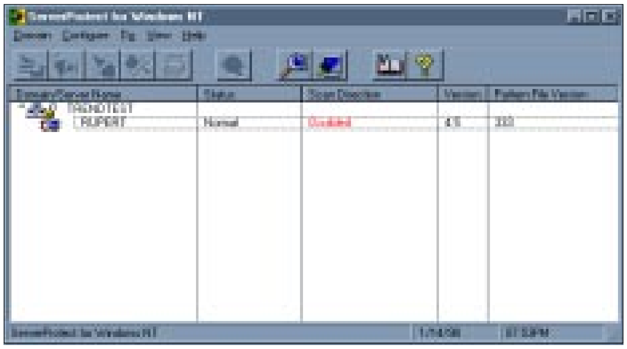
Scanning Options

The default file extensions are BIN, COM, DLL, DOC, DOT, DRV, EXE, OVL, SYS, XLS. Additional file selections can be made or all files checked. There are separate options for boot sector scans and archived files compressed with ZIP, LHA, ARJ, and MS-COMPRESS formats.

There are several actions available for infected program files. Leave Alone performs no action on the file, Clean allows the product to attempt to remove the virus, and Rename changes the file extension to VIR, or to a user-defined one. Further options include Delete, which erases the infected file, and Move, which moves it to the directory (default 'C:\ Program Files\Trend\Sprotect\SUSPECT')

You must select Manual Scan from the Do menu in order to choose a particular directory to scan. You can then browse, choosing from Selected Drives and Directories. It is also possible to make configuration changes at this point, if required. The scan is then started.

There was a problem with the test software in that if it was required to scan only selected drives or directories, this did not seem to work as it would only check the hidden system files and the last directory on drives C and A.



Domain/Server Name	Status	Scan Direction	Version	Pattern File Version
TRENDTEST				
RUPERT	Normal	Disabled	4.5	333

ServerProtect for Windows NT 1/14/98 07:53PM

When running, the scan display keeps incrementing totals of files scanned and infections found. Further to this, the current directory and file name under investigation are shown with an elapsed time display and progress bar. I think this is a very good set of feedback data, since it allows the supervisor to monitor, pause or curtail the scan progress if need be. Another good control feature is the option to select actions (Clean, Delete, Rename and Move) at scan time. If this is not required, then the action can be automated by selecting the appropriate action on the Manual Scan Configuration screen.

The frequency of scheduled scans can be set to Daily, Weekly or Monthly. Multiple scheduled scans can be configured and set to run concurrently, while the status of any pending scheduled scans can be viewed in the server status window. The file type and action settings available here are the same as for on-demand scanning.

Real-time scanning is available with incoming, outgoing, or incoming and outgoing scan checks. The default file extensions are the same as for Immediate scanning. In addition to using pattern file comparison for virus detection, there is an option to select behaviour monitoring. On the evidence of timing tests, this added a further 10% to the real-time scanning overhead.

Administration

Server Protect's configuration utility is password-protected. Unless the correct password is entered, no configuration is enabled. The same password facility must be used each time *Server Protect* is started, even if the user is logged in with Administrator rights. This provides an additional security layer.

The configuration of each server can be defined separately, or migrated from an existing server configuration. Main menu options deal with domain management, configuration of the three scanner modes, Immediate scanning, pattern updates, and viewing the server status and log files. There is also an on-line Virus Encyclopædia.

Reports and Activity Logs

The Manual Scan Monitor displays scan activity, showing individual files as they are scanned, along with the elapsed time and a progress bar. A log file records infections, scan summaries and pattern updates. To help filter the volume of data produced, selections can be disabled and the start and end event times are selectable. The results may be displayed on-screen, printed, or exported to a CSV file, suitable for importing into a spreadsheet, database or other report generator. This log file is quite separate from *NT's* Application Event log which can be viewed independently from within the software.

There are several methods of posting notifications of a virus incident – Message box, Printer, Pager and Internet email. Any or all can be selected and configured. The Message box option notifies selected Server(s) with a dialog box on the console. Numeric Pager support can be configured to run through a particular COM port and modem. In the case of Printer notification, text messages can be sent to designated printers, while the Internet email option sends a predefined warning message to selected users across the Internet. With this last option, there is a connectivity test facility to send the warning message as configured. The text of Message Box, Printer, and Internet email messages can be combined with special abbreviations to display virus name, user name, PC and so on.

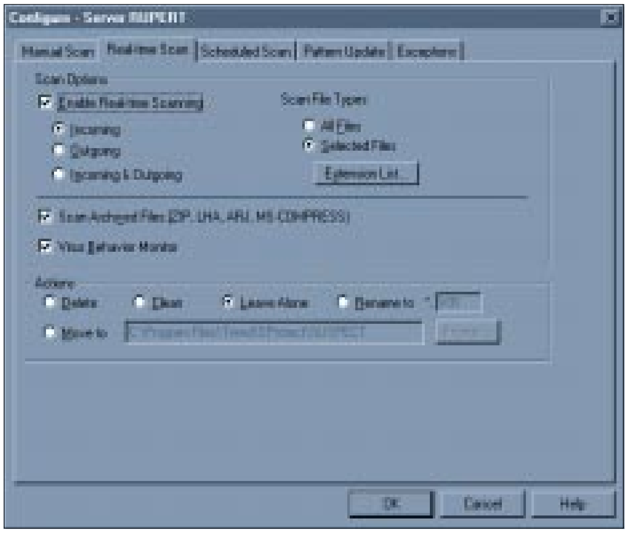
Detection and Speed Tests

The Virus Pattern File used for testing purposes was LPT$VPN.333. Pattern files can be obtained from *Trend Micro's* BBS or FTP sites, on floppy disk or from another *Server Protect* server.

It took *Server Protect* 248 seconds to scan a floppy disk comprising 26 EXE and 17 COM files. When the test was repeated with the same files infected with Natas.4744, it took 292 seconds. The overhead was 17.7%.

It took 11 minutes and 8 seconds to scan the 5500 files of the *Virus Bulletin* Clean test-set. Unfortunately seven false positives were reported in this test. *Trend Micro* has included in their software a feature called Exception Lists, ostensibly to help overcome problems with false positives. This facility enables users to catalogue files which are not to be monitored for viruses. Normally this list is empty, but in some circumstances, as in the case of false positives, files added to this will not be monitored. There are two types of Exception List – Exception File List and Exception Pattern List. Patterns listed in the latter are not used when scanning for viruses.

The scanner was tested against the *VB* In the Wild Boot, In the Wild File, Macro, Polymorphic and Standard test-sets. Details can be found in the product summary box. The various tests were conducted using the default scanner file



Configure - Server RUPERT

Scan Options

☒ Enable Real-time Scanning

● Incoming
○ Outgoing
○ Incoming & Outgoing

Scan File Types

○ All Files
● Selected Files

☒ Scan Archived Files (ZIP, LHA, ARJ, MS-COMPRESS)

☒ Virus Behavior Monitor

Actions

○ Delete ○ Clean ● Leave Alone ○ Rename to *.
○ Move to

extensions, and the scan action was set to delete infected files. The residual file count was then used to determine the detection rate. Results on the In the Wild Boot tests were the most disappointing, with seven out of the ninety viruses missed –15_Years, Cruel, Hare.7750, Moloch, Neuroquila, QRoy and Satria.A.

The scanner also suffered in the Polymorphic tests, missing all 500 samples of Cryptor.2582, 116 samples of Gripe.1985 plus three other samples. Seven samples from four viruses were missed in the In the Wild File test-set (the viruses were Hare.7610, Hare.7750, Scitzo, Tentacle.II). A further 31 samples were missed in the Standard test-set. *Server Protect's* detection in the Macro test-set was much better, at 100%.

Real-time Scanning Overhead

To determine the impact of the real-time scanner on the server's performance, the following test was performed. Two hundred COM and EXE files (totalling 20.6 MB) were copied from one folder to another using XCOPY. The folders used for the source and target were excluded from the virus scan so as to avoid the risk of a file being scanned while waiting to be copied.

The default *NT* setting of Maximum Boost for Foreground Application was used for consistency in all cases. Due to the different processes which occur within the server, the time tests were run ten times for each setting and an average taken. See the table for detailed results.

The test conditions were:

- Program not loaded. This establishes the baseline time for copying the files on the server.
- *Server Protect* service only. This shows the impact of the Domain service on its own.
- Program loaded but not scanning and Resident Protection not enabled. This tests the impact of the application in a quiescent state.
- Program loaded and Resident Protection enabled. Incoming Opening Files and Closing Files both set to 'off'. This tests the impact of having the monitor software loaded with no monitoring.
- Program loaded and Resident Protection enabled for Incoming Files only. This tests the impact of the scan on incoming files.
- Program loaded and Resident Protection enabled for Outgoing files only. This tests the impact of the scan on outgoing files.
- Program loaded and Resident Protection enabled for Incoming and Outgoing Files. This tests the impact of the scan for incoming and outgoing files.
- Program loaded and Resident Protection enabled for Incoming and Outgoing Files. Manual scan running. This tests the full impact of the scan for incoming and outgoing files as well as the normal scanning of files.
- Program unloaded. This is run after the server tests to check how well the server is returned to its former state except for the Domain service.

Activating the real-time scanner enables the behaviour monitor. The impact of the *Server Protect* service is due to the domain management software running as a service. From the results, it looks as if the on-demand scan takes over from the real-time scan, when selected.

Summary

Server Protect's scanning results, apart from macro detection, need a little attention. Also, the number of false positives it detected seems worse than average. However, scanning speed is good and the configuration options are comprehensive and easy to set up. The User's Guide is concise, making it quick to locate required information . Overall, the product has a good set of facilities for managing a domain of servers in a *Windows NT* environment.

Trend Micro Server Protect for NT

Detection Results

Test-set[1]	Viruses Detected	Score
ItW File	639/646	98.9%
ItW Boot	83/90	92.2%
Standard	769/799	96.2%
Macro	741/741	100.0%
Polymorphic	12381/13000	95.2%

Overhead of On-access Scanning:

Time in seconds to copy 200 COM and EXE files (20.6 MB), averaged over ten runs.

	Time	Overhead
SPNT not loaded	19.8	–
SPNT Domain service only	20.3	2.5%
— + inactive resident scanner	20.8	5.1%
— + resident scan, incoming	21.3	7.6%
— + resident scan, outgoing	21.6	9.1%
— + resident scan, both	21.8	10.1%
— + — + on-demand scan	20.9	5.6%
SPNT unloaded	20.6	4.0%

Technical Details

Product: *Trend Micro Server Protect for Windows NT v4.50.*

Developer/Vendor: *Trend Micro Inc*, 10101 De Anza Blvd,
4th Floor, Cupertino, California 95014, USA.
Tel 1 800 228 5651, fax +1 408 257 2003,
email: trend@trendmicro.com, WWW http//www.antivirus.com/.

Price: List price for 50 users, $1150.

Hardware Used: *Compaq* Prolinea 590 with 80 MB RAM, 2 GB hard disk, *NT* server 4.0 with service pack 3.

[1] **Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/DOS/199802/test_sets.html.