COMPARATIVE REVIEW

Slipping through the NetWare

Matt Ham

In the last Comparative of *NetWare* products (July 1999) it was noted that although *NetWare 5* was the current version of that operating system, the tests were performed on an older version, since few products had active support for the new features of version 5. Time rolls on and not only would it be expected that these features might by now be supported to a greater extent, but also *VB* could be considered to be living in the past if *NetWare 4.x* were to be used again.

These reasons were very nearly ignored at the sight of *NetWare 5.1's* 240 MB Service Pack waiting to be installed in all its vast glory. The trials and tribulations of *NetWare* installation duly followed, though with these being familiar to all those who have had contact with *Novell's* products, the exact details can be glossed over. Of the products submitted for testing, two – the *RAV* beta and *VBuster VBShield* – proved unable to operate on the *VB NetWare 5.1* server. The former proved a casualty beyond help and will probably be featured in a standalone review soon. *VBuster* rallied eventually, and is included in the proceedings.

The Test-Sets

So, the operating system is all new, what about the test-sets? Detection tests were performed on a *VB* test-set aligned to the July WildList with, due to a reviewer holiday, no non-WildList additions to the other sections. Any reader who has not spent the last few months on the moon will realise that the .VBS extension is the big new appearance in the WildList since *NetWare's* last testing at *VB*, and the numbers of such malware in the WildList have soared since the last (*Windows 98*) Comparative.

The viruses and/or worms in question have also introduced into the *VB* test-set a number of dual-extensioned samples as well as the now notorious .SHS extension. Since the extensions included for default scanning have often been a bugbear for *NetWare* products, will these new additions cause upsets in the VB 100% awards for this month?

As it happens, there are a few problems along these lines as I write this introduction, with barely half the results in. The culprits are likely to be kicking themselves, or at least their extension-handling departments, but as to who these bumblers might be, the accusing finger is pointed below.

Test Procedures

The usual speed tests were performed – on-demand scanning speeds returned against executable and OLE2 file scanning plus the on-demand scanning speeds against archived executables and OLE2 files. The scanning speed tests double up as false positive tests and the VB 100% award can only be gained by those products having no false positives in addition to full detection of ItW viruses. This includes only 'full' false positives, and not files flagged as 'suspicious', very relevant to one product this month. These tests were performed either directly from the console or, where at all possible, from the console application designed for control of the product. The latter method of testing is assumed to add a little overhead in the use of a console and associated network transfers, though this reviewer suspects that given the added ease of use the console may be considered as a usual operating method. Some may disagree, in which case appropriate weighting should be applied to considerations of scanning rates.

CA InoculateIT v4.5

ItW File	100.0%	Macro	100.0%
ItW File (o/a)	100.0%	Macro (o/a)	100.0%
Standard	99.6%	Polymorphic	98.8%

This product, as befits *Computer Associates* whose stock in trade is central administration, had one of the more complete and smooth installation procedures encountered. It, among other procedures, offered to back up important disk information in case of emergency.

Scanning, however, was less of a pleasure if only due to the slowness of the procedure. It seems likely that this is related to logging, since the problem was at first minor, increasing as the scan progressed. As such it should not really be problem in real-world situations unless mass infestations are being scanned. No false positives were encountered and thus *InoculateIT* earned the first VB 100% award of the review.

CA Vet NetWare Anti-Virus v10.1.9.a

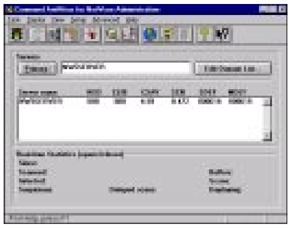
ItW File	100.0%	Macro	99.5%
ItW File (o/a)	100.0%	Macro (o/a)	99.5%
Standard	99.8%	Polymorphic	94.3%

Despite requiring a degree of manual installation twiddling, since appropriate users are not set by the installation routine, once in place *Vet* performed with no problems or difficulties. As far as detection was concerned *Vet* achieved good results in most areas, with the polymorphics, as for other products in this test, proving to be the sticking point. A full complement of ItW viruses were, however, detected both on-demand and on access which together with a zero false positive rating merited *Vet* with the second VB 100% award in as many products reviewed.

On-demand tests	File		Macro		Polymorphic		Standard	
	Missed	%	Missed	%	Missed	%	Missed	%
CA InoculateIT	0	100.00%	0	100.00%	9	98.87%	2	99.61%
CA Vet AntiVirus	0	100.00%	19	99.59%	266	94.36%	2	99.87%
Command AntiVirus	1	99.96%	3	99.70%	1	99.98%	9	99.20%
DialogScience DrWeb	0	100.00%	0	100.00%	2	99.95%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	1	99.90%
Kaspersky Lab AVP	6	99.19%	3	100.00%	0	100.00%	23	99.41%
NAI NetShield	1	99.96%	3	99.97%	6	99.25%	5	99.83%
Norman Virus Control	4	99.74%	4	99.89%	286	91.23%	5	99.83%
Sophos Anti-Virus	0	100.00%	13	99.66%	190	95.36%	15	99.54%
Symantec Norton AntiVirus	0	100.00%	17	99.53%	259	94.81%	16	99.46%
VBuster VBShield	79	92.61%	236	94.17%	2595	77.46%	72	95.54%

Command AntiVirus v4.59

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



Another application where control is exerted at a client machine, *Command's* product gained the 'security by obscurity' award for this Comparative. With very little tweaking it was possible to activate the NLM in such a way that only CPU usage was available as a check for whether a scan was progressing. The client also lacked communication ability, the actions on scan seeming to bear little if any relation to those selected at the client.

Having said that, solidly respectable detection rates were not good enough to gain *Command* a VB 100% award this month. Extensionless O97M/Tristate samples were not scanned and one such sample exists in the WildList.

Also lacking was any facility for the scanning of statically compressed archive files, which is reflected in the archive scan rates table. The slow rates of scan encountered for normal files, however, possibly explain this dearth of a feature which would potentially exacerbate the velocity problem yet further.

DialogueScience DrWeb v4.20

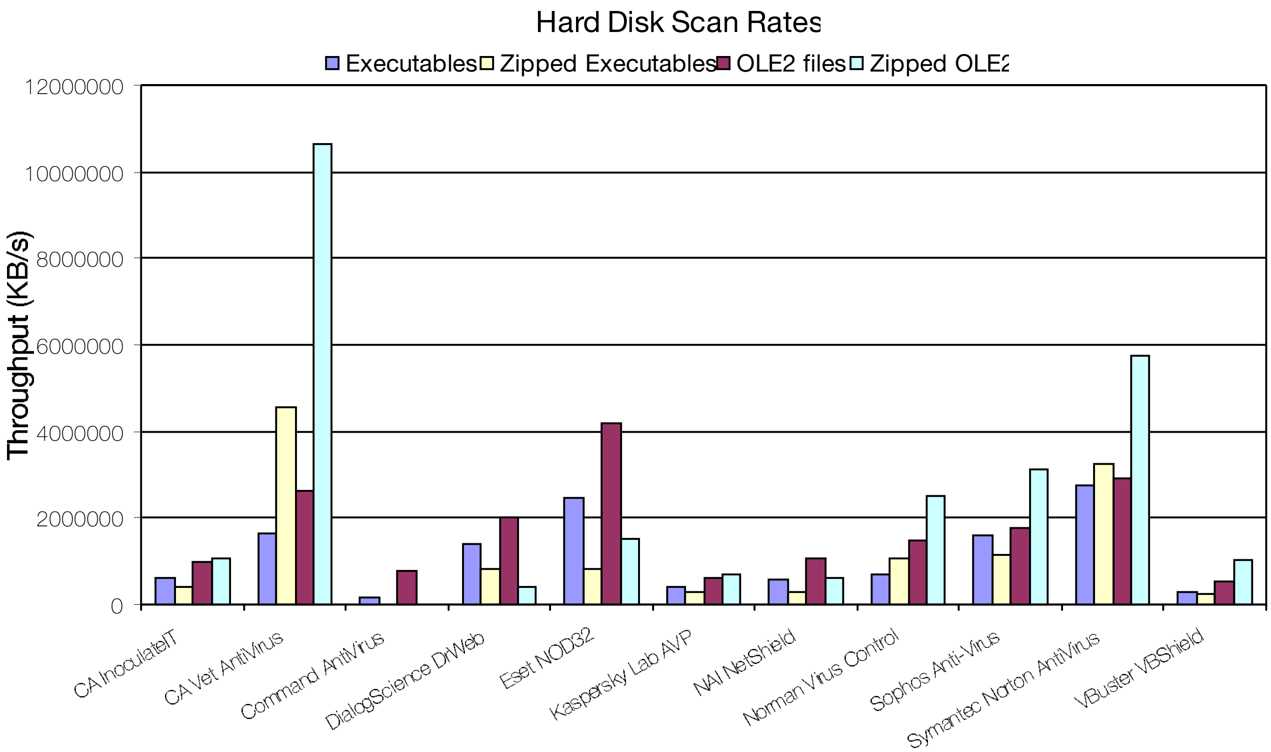
ItW File	100.0%	Macro	100.0%
ItW File (o/a)	100.0%	Macro (o/a)	100.0%
Standard	100.0%	Polymorphic	99.9%

For reasons unknown, almost all native *NetWare* GUIs in this test were of a standardised blue and white nature, a trend bucked by *DrWeb* which opts for a more ancient monitor-style green screen effect.

The scanning of files on-access does not occur on file opens, a trait which *Sophos SWEEP* for one shares, leading to the on-access testing being performed by moving the virus collection. Somewhat oddly, the copy was allowed to proceed despite the log file showing ample evidence of viral files.

There was also some confusion as to how on-demand scans are performed – the tests were all completed via scheduled jobs. The results for scanning proved to be speedy enough with all ItW viruses detected at a good rate of knots.

Despite numerous 'suspicious' flags, *DialogueScience's DrWeb* can be justifiably proud of its VB 100% award. These suspicious files have, on the other hand, remained constant, not only in the previous *NetWare* reviews but also in *DrWeb's* outings on other platforms and thus remain a tenacious thorn in the flank of *DialogueScience*.



Eset NOD32 v1.42

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

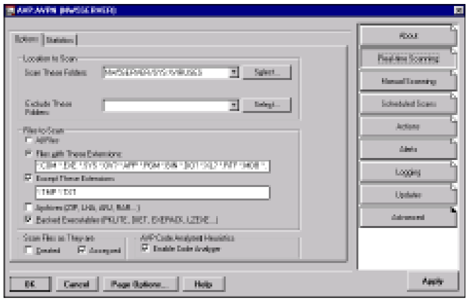
The pair of *NOD32* NLMs provided one of the more minimalist installs in this Comparative, the on-demand NLM being singularly limited to a command-line interface. This interface, however, did not prevent NOD32 from performing at its usual impressive level of detective skill – a level which gains it yet another VB 100% award. The rudimentary nature of control available in this product is a recurring feature in this review and is addressed in the conclusions.

Of all the test-sets scanned, *NOD32* missed only one sample in the Standard set, a feat difficult to improve upon and unique to this review. Coupled with good scanning speeds and no false positives, this is a gratifying result this time around for the Slovakian anti-virus company.

Kaspersky Lab AVP for NetWare v3.5

ItW File	99.1%	Macro	100.0%
ItW File (o/a)	99.1%	Macro (o/a)	100.0%
Standard	99.4%	Polymorphic	100.0%

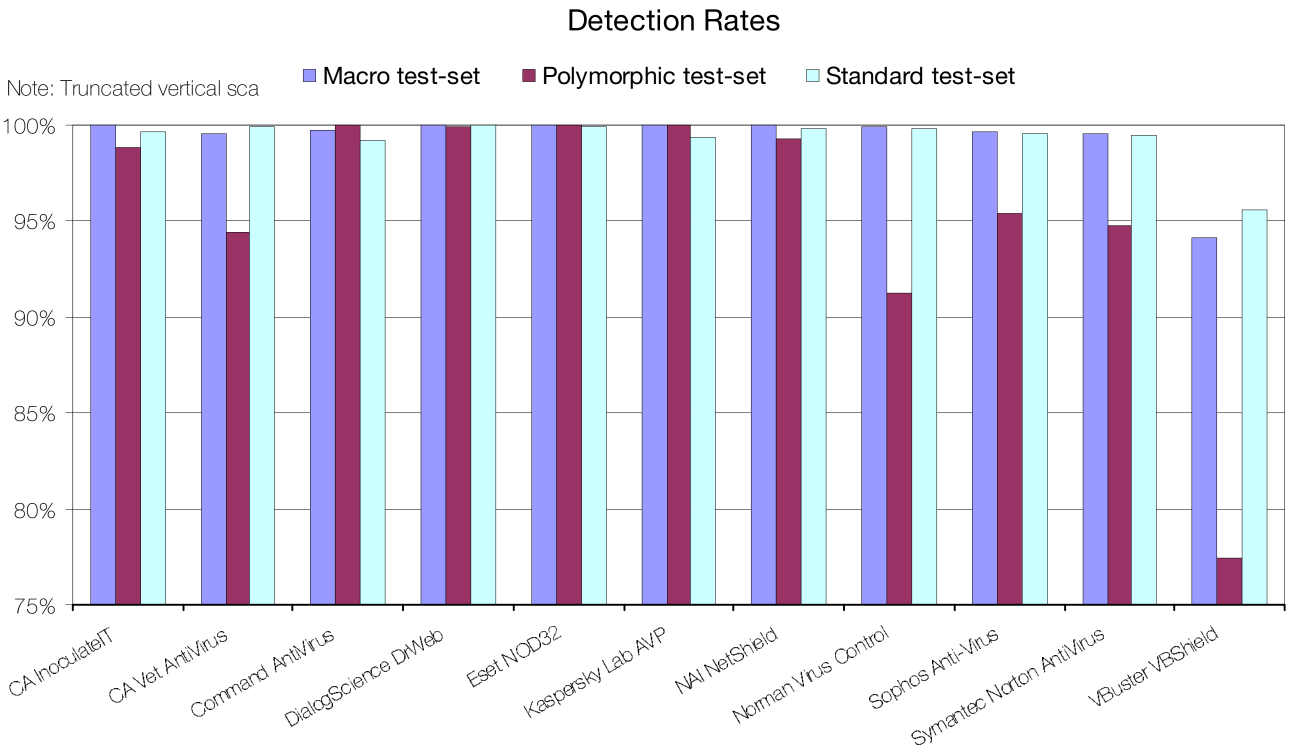
AVP for NetWare was the first product reviewed where administration was fully integrated within the NWADMN32 program within *Windows NT*. The ease and clarity of operation was thus much improved over the pure console-driven applications expected of *NetWare* and was the only console which could in fact load the NLM.



On the downside the application suffered from intermittent instability, requiring Dr Watson to be summoned on a couple of occasions. There were also oddities in the method used by *AVP* for counting files, as more were reported scanned than actually existed. Log files caused some confusion, primarily by the marking of files as 'OK' when in fact this referred to file structure rather than a lack of viral content.

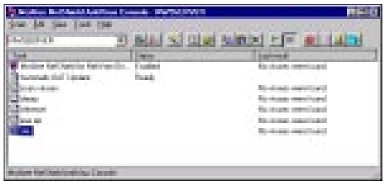
It was with *AVP* that the perils of extensions reared their heads once more with the problem areas being the major surprise since the new double extensions were all detected happily. Not alone in missing the extensionless sample of O97M/Tristate in the WildList, the chaps at *Kasperky Lab* will be joined by others in their reversion to problems with this file – problems long since banished on other platforms.

The nature of the console is also of note as a potential slowing factor, the scan rates here being very low indeed. There was a, certainly related, torrent of network activity present while scans were being performed. The console it seems is updated very regularly, rather too regularly perhaps since the scan rates 'felt' much slower than *AVP* operating on other systems. This would appear to be the one flaw in the console, which otherwise performed admirably and, not surprisingly, was always well informed of its NLM partner's status.



NAI NetShield for NetWare v4.5.0

ItW File	99.9%	Macro	99.9%
ItW File (o/a)	99.9%	Macro (o/a)	99.9%
Standard	99.8%	Polymorphic	99.2%



NetShield is supplied, as would be expected from a network-based company, with a client control program which is a welcome sight in such a review. Perhaps more welcome is that the client neither constantly polls for information, as *AVP* does, nor has information, as in the case of *Command's* submission. This allows information on scan status to be present at the client without overwhelming network activity.

All of this goodwill is, however, frittered away by the speed of scanning through the Polymorphic sets, which moved with a speed akin to the rate of evaporation of granite. Of particularly agonising note was the scanning of Splash, which took several minutes for many of the *VB* samples. This slowness was also reflected in the Clean set testing, where speed was not an *NAI* strong point.

It is lucky, therefore, that detection rates have something to show for all this effort, with good detection across the board except in one simple area. *NetShield* falls among those products which do not scan extensionless files by default and thus denies itself a VB 100% award by the slimmest of margins.

Norman Virus Control for NetWare v3.98b

ItW File	99.7%	Macro	99.8%
ItW File (o/a)	99.7%	Macro (o/a)	99.8%
Standard	99.8%	Polymorphic	91.2%

Norman's offering for this review achieved notability in the main by its having two names, '*FireBreak*' being the alternative, which were used interchangeably throughout the operation of the program.

It also succeeded in niggling as it was unable to fine-tune scanning within areas smaller than an entire volume. Short of creating a volume specifically for the investigation of viral suspects this makes checking individual files something of an onerous pursuit and leaves all scans on the SYS volume doomed to be extremely lengthy indeed.

The Polymorphic set was the great divider in this month's testing, with all but one product faring well in all other areas. The bane that is ACG.A flummoxed the *Norman* product completely, as it did more than one other scanner, leaving it with the highest aggregate total of missed files in the test. A lack of scanning for .HLP files prevented the detection of W95/Babylonia in the ItW set, which in turn denied the product a VB 100% award.

Sophos SWEEP for NetWare v3.36

ItW File	100.0%	Macro	99.6%
ItW File (o/a)	100.0%	Macro (o/a)	99.6%
Standard	99.5%	Polymorphic	95.3%

	Hard Disk Scanning Speed									
	Executables			OLE2 files			Zipped Executables		Zipped OLE2	
	Time (sec)	Throughput (kB/s)	FPs [susp]	Time (sec)	Throughput (kB/s)	FPs [susp]	Time (sec)	Throughput (kB/s)	Time (sec)	Throughput (kB/s)
CA InoculateIT	895	611097	0	79	1004224	0	375.0	425111	70.0	1065821
CA Vet AntiVirus	329	1662407	0	30	2644458	0	35.0	4554760	7.0	10658214
Command AntiVirus	3611	151462	0	101	785482	0	N/T	N/A	N/T	N/A
DialogScience DrWeb	395	1384638	[27]	39	2034199	[1]	196.0	813350	185.0	403284
Eset NOD32	223	2452610	0	19	4175461	0	196.0	813350	49.0	1522602
Kaspersky Lab AVP	1392	392911	0	130	610260	0	531.0	300220	110.0	678250
NAI NetShield	964	567357	0	75	1057784	0	540.0	295216	125.0	596860
Norman Virus Control	802	681960	0	53	1496864	0	150.0	1062777	30.0	2486917
Sophos Anti-Virus	200	1589919	0	27	1762973	0	49.0	1138690	13.0	3108646
Symantec Norton AntiVirus	344	2734660	0	45	2938288	0	140.0	3253400	24.0	5739038
VBuster VBShield	1787	306061	9	148	536039	2	687.0	232047	72.0	1036215

The *SWEEP* NLM falls firmly in the middle ground of control sophistication in this review, the greatest idiosyncrasy being in the area of scanned file selection where recursion is selected by the addition of a '>' to the path.

Irritating from *VB's* point of view is the inability to have logs greater than 999 KB in size, though, as with many *VB* niggles, this is less of a problem in the real world than in *VB* tests. Detection-wise affairs seem to be tightening up after the extension problems of the last Comparative, with a clean sweep in the wild. The NLM does not, admittedly, scan within some file types which might otherwise have upped percentages in the Standard and Macro sets, .MDB being an example.

The objective here is presumably to raise scan speeds at the expense of non-detection of perceived low-risk viral threats, since *Access* infectors are not famed for their rampant spread. This is also the assumed reason for the continued non-detection of W95/Navrhar and Positron, both mid-infectors requiring slower scanning methods for positive detection.

This 'need for speed' ethos proved possibly to be a success as *SWEEP* not only performed quickly on the Clean sets, but with a combination of full detection in the wild and no false positives, *Sophos* regains its position as a VB 100% award holder.

SWEEP was once rare in that it routinely detected the same viruses on-demand as on-access. This review was no different as far as *Sophos's* detection rates go, though the uniqueness is certainly a thing of the past – all products managed such detection, a fact reflected in the combined detection rate graphs and tables for on-demand and on-access scanning.

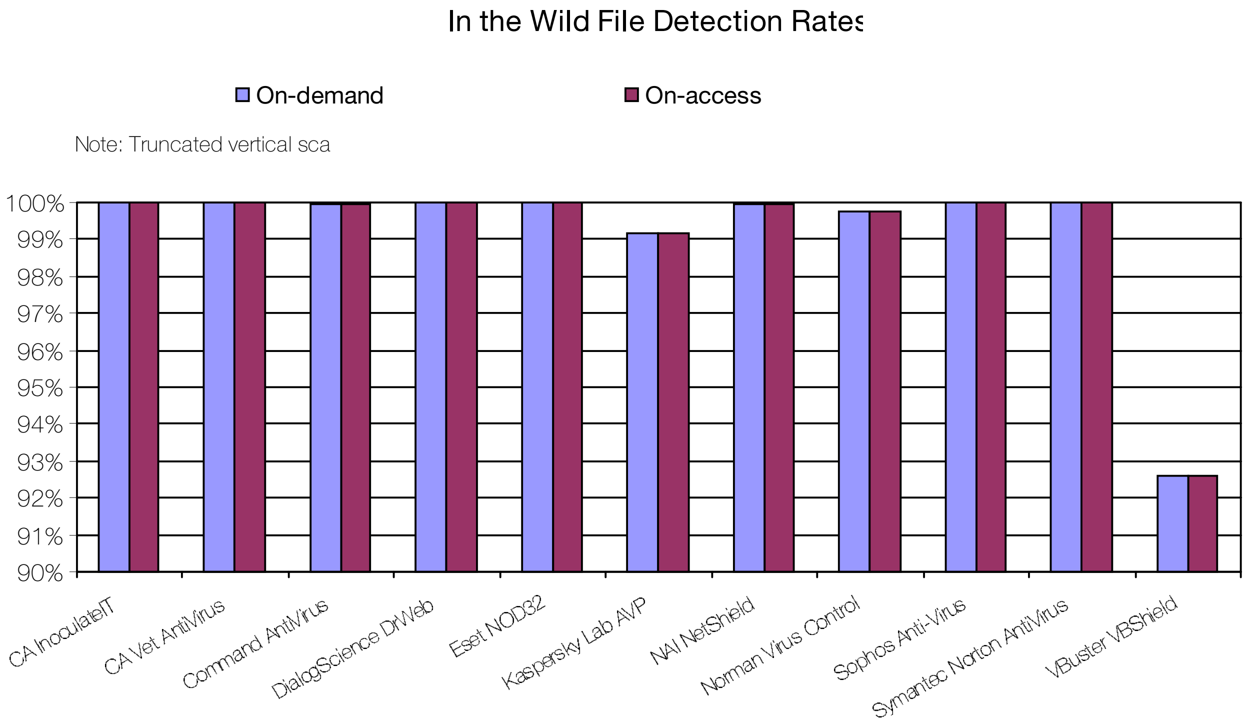
Symantec Norton AntiVirus for NetWare v4.04

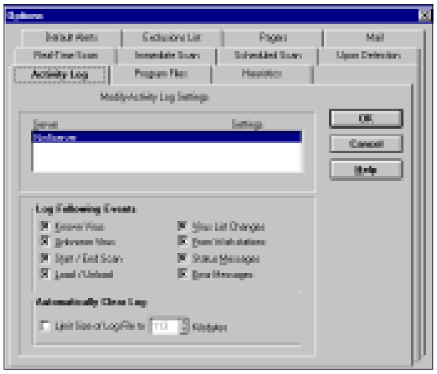
ItW File	100.0%	Macro	99.5%
ItW File (o/a)	100.0%	Macro (o/a)	99.5%
Standard	99.4%	Polymorphic	94.8%

Norton AntiVirus was one of the very few recipients of a VB 100% award in the last Comparative, at which juncture it was pointed out that such a distinction was perhaps not all it could be.

This month, however, surrounded by companies wilfully shooting themselves in the foot, the VB 100% award gained by *Symantec* will be more pleasing to them and is much more representative of a superior all-round performance.

The *NAV* program is one of those sporting a *Windows* front-end to the NLM and this operated with a near complete lack of problems. Admittedly, the viral scanning speed was a little sluggish in comparison with some of the faster scanners on show, though as with the other slightly slow entrant previously mentioned, this was coupled with a good detection rate. Much more impressive was the extremely fast Clean set scanning speed, which by and large put rivals to shame.





Log Following Events

☒ Known Virus
☒ Unknown Virus
☒ Start / End Scan
☒ Load / Unload
☒ Virus List Changes
☒ Errors/Initializations
☒ Status Messages
☒ Error Messages

Automatically Clear Log

□ Limit Size of Log File to [illegible] Kilobytes

Despite these sterling features *NAV* was in fact one of the products which missed the most samples overall, ACG.A being a culprit here as elsewhere. It seems odd that scanning of infected samples should be so slow with so many misses, while Clean set scanning was so fast. The likely explanation seems to be that false positives have been singled out for eradication, thus more checking is done than usual as to the validity of viral identities.

One extra niggle arose during false positive testing when the *Windows* front-end caused a general protection fault, though this was not reproduced on further testing.

VBuster VBShield for NetWare v1.02

ItW File	92.6%	Macro	94.1%
ItW File (o/a)	92.6%	Macro (o/a)	94.1%
Standard	95.5%	Polymorphic	77.4%

The only newcomer to the Comparative, as noted in the introduction, *VBuster's VBShield* proved unable to load successfully at the first attempt. It was also the last product scheduled to be reviewed and thus a great deal of frantic information exchange occurred between *Virus Bulletin* and the Hungarian developers at *VirusBuster*. The problem turned out to be a simple oversight on *Virus Bulletin's* part, though the expected activities of the installer were not noted in the documentation supplied, a fault which was not unique to this product. As a new entrant, therefore, somewhat more detail is supplied as regards *VBShield's* capabilities and limitations.

The *VBShield* NLM has a constant on-access thread running, which gives the options to disinfect, deny or quarantine, but gives no deletion option. The on-demand section provides the same options and in both cases the activity may be sent to a log. By keeping the log on screen a measure of information can be observed concerning ongoing scans. These logs are written to a single file which holds details of both on-access and on-demand detections. On-demand scans can be created in a scheduled mode and applied to chosen directories or volumes.

Scanning proved to be no problem, files denied on-access being determined easily by *VB's* in-house tools. With the treatment of the log files, however, problems arose in the parsing of the files. The logs are written to in such a way that detection notifications are logged across several lines and thus impenetrable to the usual *VB* methods. For the sake of reaching deadlines, the on-access results were used for both on-access and on-demand results, this being in accordance with trends across the other products.

VBShield is clearly somewhat outclassed in detection by the other products reviewed this month, though in fairness the best comparison is with *VBShield's* performance in previous reviews. From that point of view there is good news, since detection rates are up, most specifically in the Standard and ItW sets.

Speed remains something of a problem, but it is good to see that the important issue of detection is indeed being addressed by the developers.

Notes on Testing

As noted in the comments for *Sophos SWEEP* the results this month were unique in one aspect, this being the first time that this reviewer can recall all products rating the same for detection for the on-demand and on-access tests. This is attributable at least in part to the lack of boot sector virus testing in the *NetWare* test regime.

It also seems likely that the *NetWare* environment itself is one which makes this more likely, since the situation was very nearly the same on the last occasion that a *NetWare* Comparative took place. Although this reviewer would be much more happy performing only one set of tests for both on-access and on-demand testing, this does not seem likely in the future.

Furthermore, some products showed scan speed results far below those that would be acceptable in a corporate environment. The *VB* test machine is clearly at the extreme low end of performance for a *NetWare 5* server – a situation which might cause concern among readers.

The reason behind this apparent lack of server technology is not all due to *Virus Bulletin's* penury. By using a machine which is at the limits of performance a better understanding of scan rates under stress can be gained than on a machine running at one or two percent CPU usage. The scan throughput rates, like the other figures supplied, are not valuable in isolation but as a means of comparison between the scanners.

Conclusion

After the last Comparative's warping by the addition of VBS/Unicle.A to the WildList, this test did not hold as many potential pitfalls in the way of new viruses added to the Standard set, though many products managed to fall over on the detection of old favourites instead.

The age-old problem of extensionless samples fooled a disturbing number of the products in the line-up, a quirk more disturbing since the same samples caused problems in the *NetWare* Comparative of July 1999. The same story was repeated in the Polymorphic test-sets, where both the last Comparative and this one saw mass problems with ACG.A and to a lesser extent ACG.B for some products.

There have, however, been minor improvements on that last *NetWare* test in other areas – the overall detection rates are up and false positives on those products tested on both occasions are very marginally down. Major differences in manageability are, though, hard to come by in all but the case of *Kaspersky Lab's AVP*, the product (in this reviewer's opinion) which is most fully integrated with the *NetWare* operating system.

The manageability of some products in fact borders upon the arcane, with features absent which would be taken for granted on any other platform. Being unable to tell whether a scan is operating, to monitor a scan, to delete offending files or to be unable to run an on-demand scan would instantly consign a *Windows* or Mac product to exile, to the tune of alternating hails of derision or shrieks of laughter.

What lies behind the state of the *NetWare* market? *NetWare* as an operating system has certainly suffered from the rise of *Windows NT* as an, arguably, secure platform for large networks. In addition to this, the Console One interface of *NetWare 5.x* is sufficiently doddering that few could consider *NetWare* to be on a par with *Windows* systems as far as new-user friendliness goes.

For these reasons the anti-virus developer community may have decided that *NetWare* has had its day and that a *NetWare* scanner, although useful for the sake of completeness, should not be allocated a great deal of development time. It also seems, at a guess, possible that the aspects of security involved in remotely administering a *NetWare* product might well make this a task few would relish.

The reviewer's personal opinion, however (also a wild hypothesis), is that there has been no real call for improvements. *NetWare* users are used to obscure and Byzantine procedures for the simplest of tasks. Thus, the odd and obscure ways of some of the scanners tested are perfectly at one with the *NetWare* environment and likely to exist long after we are all safely tucked up in retirement homes.

Technical Details

Server: 500 MHz Athlon with 6 GB HD, 64 MB RAM, CD-ROM and 3.5-inch floppy running NetWare 5.1 with Service Pack 1.

Workstation: 166 MHz Pentium with 4 GB HD, CD-ROM and 3.5-inch floppy, running Windows NT 4 with Novell's Client for Windows.

Virus test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NetWare/200009/test_sets.html.

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