COMPARATIVE REVIEW

NETWARE 6.5

Matt Ham

Those who have read *Virus Bulletin*'s previous reviews of *NetWare* products will be familiar with my views about the platform – overall, I have found the platform less than convenient to work with and the products themselves generally even worse.

To be reasonable, however, *NetWare* has become significantly more tolerable with version 6 and newer, though to a certain degree this is a function of the fact that hardware has only recently been able to deal with the demands of *NetWare*'s GUI. Thankfully, the GUI in *NetWare 6.5* has been relieved of the images of eccentric gymnasts which graced version 5, which has also made the review process a little more bearable.

With the improvements to the operating system, therefore, it was left to the products to determine whether the review experience would be pleasant or otherwise. One issue made itself known early on: several products caused message boxes to pop up on the client when viruses were detected on the server, and there was no obvious way to remove this feature. With large test sets the added network traffic slowed down scanning and the client emitted irritating beeps as a result. I hoped that no greater irritations would come my way.

PRODUCTS, TEST SETS AND PLATFORM

The deadline for the submission of products for this review was 4 July 2005 – unwittingly causing some chaos for reasons that will be obvious to those in the US. *NetWare* itself was installed freshly from the minimum patch files provided on *Novell*'s site, for both client and server on 29 June 2005. Thus the version of *NetWare* used was *Novell Open Enterprise Server NetWare 6.5 Support Pack Revision 03, Server Version 5.70.03*. *NetWare Client version 4.91.0.20050216* was used on *Windows XP Professional Service Pack 2*. The client and server were connected over a 100Mbs LAN link.

The test sets were based on the April 2005 WildList, since this was the most up-to-date version available at the time. As has been noted in recent comparative reviews, the new additions to the WildList seem to become more tedious on every occasion, though they increase numerically as if to compensate. With the new additions closing in on the 100 mark, there was only one that was not a direct variant of a sample already contained in the sets – W32/Serflog.

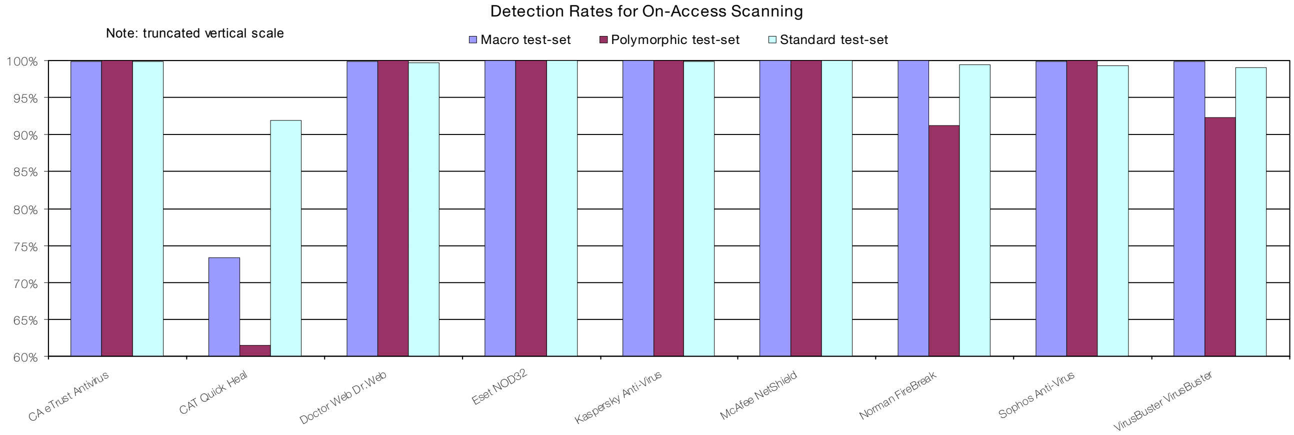
The majority of the new additions to the In the Wild (ItW) test set were multiple variants of W32/Sdbot and W32/Mytob. With decent handling of archives and some care in creating generic detections, these variants can, in many cases, be detected as soon as they are produced. Therefore, it seemed from the outset that simply having a *NetWare* product would almost be enough for a developer to gain a VB 100% award.

CA eTrust Antivirus 7.1

ItW File	100.00%	**Macro**	99.82%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.82%
Standard	99.96%	**Polymorphic**	99.95%

Aug 2005 100% VIRUS BULLETIN www.virusbtn.com

eTrust is a useful example of the two facets of administration where *NetWare* products are concerned. The two main methods are to administer from a GUI (either on a client or server) or simply to interact in the server console. The latter tends to look very archaic compared with the usual interfaces for such software. In the case of *eTrust*, the on-demand scanning can be controlled fully through the



On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust Antivirus	0	100.00%	12	99.82%	1	99.95%	3	99.84%
CAT Quick Heal	0	100.00%	1069	73.35%	5807	61.44%	178	91.95%
Doctor Web Dr.Web	0	100.00%	4	99.90%	0	100.00%	3	99.69%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	3	99.85%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman FireBreak	0	100.00%	0	100.00%	180	91.24%	12	99.45%
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	15	99.30%
VirusBuster VirusBuster	1	99.80%	7	99.88%	162	92.31%	17	99.01%

server console. This may also be controlled through an administration tool on a client. If full control of on-access scanning is required, however, this must be performed from the client.

Having been somewhat confused by this division of control options, the actual scanning processes were easy by contrast. Even better, *NetWare* logging is free from those strange formats which plague the *Windows* versions of *eTrust*. When logs were parsed there were no real surprises and a VB 100% award was the result.

CAT Quick Heal Antivirus 8.00

ItW File	100.00%	**Macro**	98.18%
ItW File (o/a)	100.00%	**Macro (o/a)**	73.35%
Standard	96.54%	**Polymorphic**	95.93%

Installation of *Quick Heal* is by a client-side installation routine, though the same effect may be obtained manually with little trouble. Along with this simplicity of installation, the interface is simple both in appearance (it operates through the server console) and in the limited number of options available. All the usual options are present, it is simply that they are more conveniently grouped than in many products and are not obscured by components of dubious value. Admittedly, this feeling of a lack of clutter is much helped by the fact that the on-demand and on-access components are separate NLMs. Offsetting the clarity somewhat was the log file, which changed the cases of filenames and reduced long file names to 8+3 format, somewhat hindering extraction of test results.

Aug 2005 100% VIRUS BULLETIN www.virusbtn.com

In fact, of all the products in this test, the results for *Quick Heal* showed the most variation between on access and on demand. Despite this, however, *Quick Heal* detected all the samples in the ItW test set, and generated no false positives, and a VB 100% award is thus due.

Doctor Web Dr.Web 4.32c (4.32.3.06300)

ItW File	100.00%	**Macro**	99.90%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.90%
Standard	99.69%	**Polymorphic**	100.00%

Doctor Web's *NetWare* product remains essentially the same in look and feel as when I inspected it several years ago. Setting it up is performed simply by copying the files to the server and loading the NLM. This either results in a working interface or exits with the reason for

Aug 2005 100% VIRUS BULLETIN www.virusbtn.com

On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust Antivirus	0	100.00%	12	99.82%	1	99.95%	1	99.96%
CAT Quick Heal	0	100.00%	75	98.18%	418	95.93%	101	96.54%
Doctor Web Dr.Web	0	100.00%	4	99.90%	0	100.00%	3	99.69%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman FireBreak	0	100.00%	0	100.00%	180	91.24%	12	99.45%
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	12	99.45%
VirusBuster VirusBuster	1	99.80%	7	99.88%	151	92.62%	14	99.31%

failure dumped to a log. The lack of an on-screen message to inform me that the licence key was not found, caused me a little perplexity until I found this log. However, once installed all went smoothly.

Scanning results were much the same as have been noted in recent *Windows* testing. *Dr.Web* seems to alternate between full detection and missing a small number of samples – the latter presumably being due to the tweaking of older definitions for efficiency. No misses occurred in the ItW set, however, and with no false positives *Dr.Web* receives a VB 100%.

Eset NOD32 1.11.61

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	100.00%

Likewise unchanged since the last few tests, the on-demand and on-access scanners of *NOD32* are each comprised of an NLM which is loaded from the server console. The word 'loaded' is perhaps a little misleading in the case of the on-demand scanner which, alone in these tests, operates as a command-line scanner rather than having any more advanced interface. This rather aged interface might cause second thoughts for some users. The full detection rates and good scanning speed, however, can cause no such issues and result in a further VB 100% award for *Eset*.

Aug 2005 100% VIRUS BULLETIN www.virusbtn.com

Kaspersky Anti-Virus 5.6.1

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	100.00%

The *Kaspersky* product is rather more evolutionarily advanced than some others, the default installation from the client being one sign of this. It installs as a snap-in to ConsoleOne, *Novell*'s *NetWare* GUI. After installation there are two server console interfaces, one each for the on-demand and on-access scans. These are, however, informational rather than interactive, and scanning during testing was controlled via the ConsoleOne interface. Logging proved somewhat confusing for a while, until it became clear that the use of ampersands in file names was causing the log entries to become garbled.

Aug 2005 100% VIRUS BULLETIN www.virusbtn.com

With the log files unravelled there was a small difference in results between the on-access and on-demand tests, with the latter showing full detection. However, the files missed on access were due to the understandable removal of archive handling for files in this mode – a common efficiency measure. None of the files missed were in the ItW test set and thus *Kaspersky* receives another VB 100% in this month's bumper crop.

McAfee NetShield 4.6.3 4.4.00 4.0.4529

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	100.00%

The installation of *NetShield* was delayed a little by the requirement for a Java runtime to be available on the machine from which the install will take place. Once this hurdle had been overcome, the process of installation from a client was simple enough. Updates and upgrades were applied to the software by the expedient of unloading the NLMs and overwriting old files with new – which seems to be a common method in *NetWare*.

The main NLM for *NetShield* operates as a server console-viewable interface, though it can only be inspected in this state. In order to adjust the configuration, the client side application must be used. This offers exactly the same interface as *NetShield* on other platforms. The developers seem to have opted for minimising network traffic during scanning, since despite having a scan status visible in the GUI, this status was not updated between the start and end point of any scan.

With no samples missed in any of the test sets, and no false positives generated in the clean set, *McAfee* is due a VB 100% award without further ado.

Norman FireBreak 4.74 2311

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.45%	**Polymorphic**	91.24%

The installation procedure for *FireBreak* is performed from the client, requiring a drive to be mapped to the root of SYS: on the server. A ConsoleOne snap-in and Internet update module are installed as part of this process, though the server console interface was used for testing.

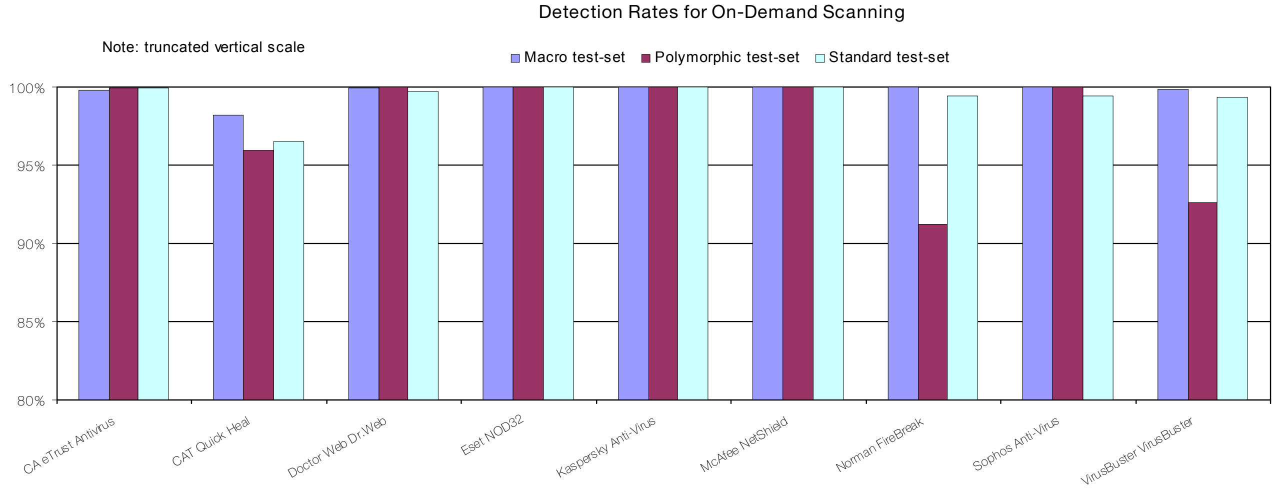
On the occasion of the last review, there were a number of problems for *Norman*'s product, associated with scanning. Thankfully these were notable only by their absence this time.

The detection rate was very much at the level usually achieved by *Norman*. Weaknesses still exist in the handling of relatively modern polymorphic viruses, though none of these were present in the ItW test set. A VB 100% award is the net result.

Sophos Anti-Virus 3.95.0

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.80%
Standard	99.45%	**Polymorphic**	100.00%

Another product adhering firmly to the server console style of interface, *Sophos Anti-Virus* is also very much unchanged by the passage of time. Installation is by the loading of a single NLM, which creates the appropriate



Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
CA eTrust Antivirus	267.0	2048.4		15	5288.9		130.0	1226.3	15.0	4973.8
CAT Quick Heal	140.0	3906.7		13	6102.6		76.0	2097.6	19.0	3926.7
Doctor Web Dr.Web	180.0	3038.5		16	4958.4		31.0	5142.5	5.0	14921.5
Eset NOD32	75.0	7292.4		9	8814.9		20.0	7970.8	4.0	18651.9
Kaspersky Anti-Virus	285.0	1919.1		29	2735.6		116.0	1374.3	27.0	2763.2
McAfee NetShield	420.0	1302.2		29	2735.6		265.0	601.6	31.0	2406.7
Norman FireBreak	248.0	2205.4		14	5666.7		22.0	7246.2	5.0	14921.5
Sophos Anti-Virus	152.0	3598.2		17	4666.7		18.0	8856.5	7.0	10658.2
VirusBuster VirusBuster	621.0	880.7	[1]	25	3173.4		207.0	770.1	20.0	3730.4

directories and populates them. This is a convenient set up procedure, which avoids the irritation of setting search paths and directory structures. Having added supplementary virus identities the product is ready for operation.

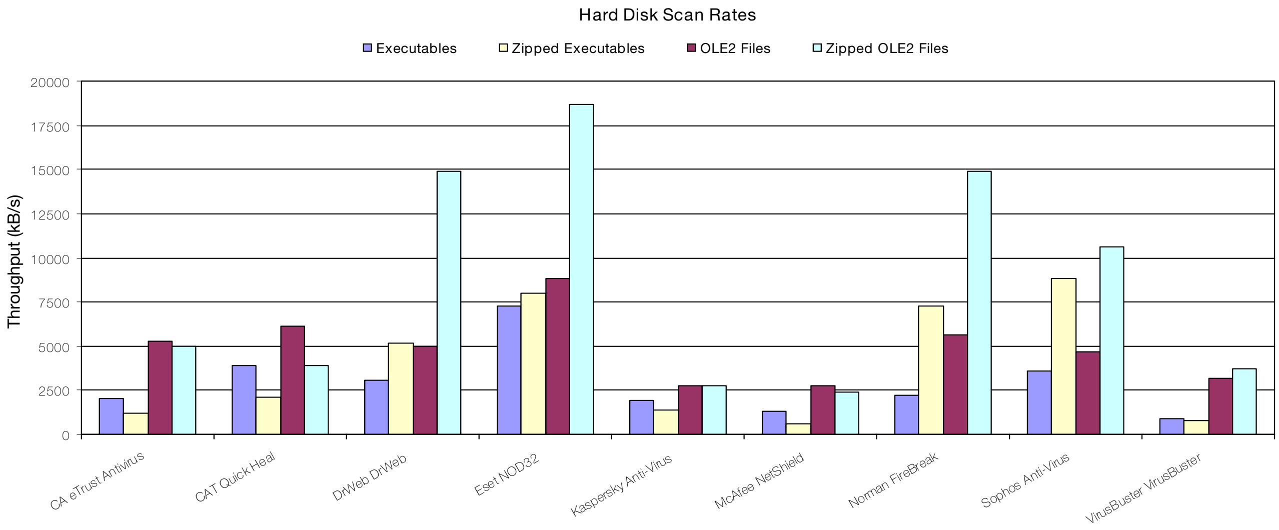
Age-old niggles still exist during operation, however. The requirement to prepend '>' to paths in order to force recursive scanning is among the more idiosyncratic parts of the interface. The log file is now out of step even with other *Sophos* products, still reducing long file names to the less than useful '?????~?.???' format. It should be noted that it is impossible to scan anything other than a full volume using the extension lists supplied, thus the scanning here was performed on all files in a supplied path. Despite these peculiarities the scanning performed without any hitches and resulted in a full detection of ItW files. A VB 100% is thus secured by *Sophos*.

VirusBuster VirusBuster 2005 v2.02.003

ItW File	99.80%	**Macro**	99.88%
ItW File (o/a)	99.80%	**Macro (o/a)**	99.88%
Standard	99.31%	**Polymorphic**	92.62%

VirusBuster installs by copying its files to the server, setting the location as a search path and loading the main NLM.

The main issue with *VirusBuster* concerned its speed of scanning infected files. This was noticeably slow in the ItW



test set, though this is common enough with the unpacking required for some of the bot samples in the collection.

Rather more frustrating were some polymorphic samples. In particular, Satanbug.5000.A took over a minute per sample to be scanned in many cases. With 500 samples of this virus alone in the test sets, scanning was a time-consuming and tedious process indeed. On the plus side, the *VirusBuster* logs now make a distinction between worms and viruses, though with the eternal debate over the fine distinctions of the nomenclature, this may only serve to inflame passions.

VirusBuster demonstrated the only false positive in the tests, although this was simply a sample which was declared suspicious rather than a full-blown declaration of viral content. Unfortunately, however, *VirusBuster* missed the W32/Lovelorn.A sample in .HTM form both on access and on demand. As this sample is in the wild, *VirusBuster* misses out on a VB 100% on this occasion.

CONCLUSION

Looking back over the last few *NetWare* reviews (see for example *VB*, August 2004, p. 14 and *VB*, August 2003, p.17) I find myself repeating my comments, especially concerning the two broad groups into which the developers have fallen. On the one hand some developers continue to add to their products administrative functionality and integration within a managed anti-virus environment. On the other hand there are those whose only developmental effort seems to have been in making the product detect more viruses, with all other features remaining in stasis.

NetWare itself seems in a healthier state than it has been in the recent past, with *Novell*'s strategic partnerships being chosen to bring the company out of the dark corner into which it was pushed by other server offerings. Whether this will be enough to encourage further anti-virus developer effort remains to be seen.

Technical details:

Test environment: Identical 1.6 GHz *Intel Pentium* machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive. Server running *Novell Open Enterprise Server NetWare 6.5 Support Pack Revision 03*, Server version 5.70.03. Client running *Novell NetWare Client* version 4.91.0.20050216 installed on *Windows XP Professional Service Pack 2.*

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2005/test_sets.html.

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

ADDENDUM: NETWARE 6.5 COMPARATIVE REVIEW

Unfortunately, due to a combination of miscommunication and missed communications, *Symantec AntiVirus* was not included in last month's *NetWare 6.5* comparative review. *VB* has since tested the product and is pleased to reveal that *Symantec AntiVirus 10.0.0.1* detected all samples in the wild, with no false positives, and is awarded a VB 100%.