

EXCERPTS FROM VIRUS BULLETIN NETWARE COMPARATIVE REVIEW AUGUST 2004

VIRUS BULLETIN VB 100% TESTING

Virus Bulletin's comparative tests tend to focus on virus detection rates, scanning speed and performance overhead of on-access or resident scanning components. As far as the VB 100% award is concerned there are two fundamental tests involved: the detection of 100 per cent of the viruses in the In the Wild (ItW) test set, and no detection of infections in the test set of clean files.

The samples used for *Virus Bulletin's* ItW test set are derived from the latest Real-Time WildList at midday GMT, two days prior to the deadline for product submission for the test. The samples in the test set may range from a simple worm, with one file only ever representing it, to a polymorphic virus which has billions of potentially variable samples. One sample of the worm in the test set will clearly be sufficient – on the other hand, several hundred samples of the polymorphic virus may need to be tested to give a good idea of a product's detection capabilities. For this reason the number of samples of each virus in the test sets varies considerably. When calculating results, however, it is the number of *viruses* missed, rather than number of samples missed, that is of importance.

The test sets used for review purposes are not restricted to the ItW set – the macro, standard and polymorphic test sets contain a host of viruses which range from samples that are purely of academic interest, to samples of viruses that have only just left the ItW test set. As far as the VB 100% award is concerned, however, these other samples are not taken into consideration.

What constitutes a detection is no longer as clear cut as it once might have been. Initially, on-demand scanning with a command-line version of the product on test was deemed sufficient. This has now expanded to include both testing of GUI-based applications and the requirement for detection in real time when a file is accessed. These two methods of scanning, referred to as 'on demand' and 'on access' respectively, are sufficiently different that they must be considered separately. One unusual feature of *VB* testing is that products are run in default mode as far as possible. This equates to using out-of-the-box settings, and choosing the default or manufacturer-recommended settings wherever a choice is offered.

Another requirement for certification is that a product produces no false positive detections on scanning a collection of files that are known to be clean.

In order to use the results of these tests in any serious fashion, historic trends for a product must be examined. Most developers will concede that, for ItW viruses at least, detection is uniformly good over almost all products. Misses can occur as a result of bad luck, bad timing or an oversight in default settings in an otherwise solid product. Whether

these are of relevance to an end user depends on the individual user's requirements and situation. It is because there are such important caveats to be considered, that the *Virus Bulletin* reviews have never offered recommendations or top scorers. *VB* provides the information and the choice of product must be the end user's decision alone.

NETWARE: AUGUST 2004

True to form, *Novell* has been busy updating its server software with yet another batch of upgrades and patches. In fact, a new patch was released on the date of finalising the test platform. However, the patch had not been uploaded to *Novell's* website by midday GMT and therefore it was not included in this test. I suspect that a sigh of relief would have accompanied this decision as far as the submitting anti-virus developers were concerned.

The line-up for this year's test was similar to that of last year's *NetWare* comparative (see *VB* August 2003, p.17), with *CAT's Quick Heal* the only newcomer to the process. *NetWare* products are very much slower to be upgraded than the operating system upon which they run – leading to a general impression of them as being clunky, irritating and tending towards the user-friendliness of *NetWare 3*. Of course there are exceptions, where the products make use of the multiple methods supplied by *Novell* for integration within ConsoleOne and other admin interfaces. Some companies seem rather indecisive as to which of these paths to pursue and spread control over both. Others use Java or custom GUIs to facilitate administration from clients.

The test sets were aligned with the most recent Real-Time WildList (RTWL: <http://www.wildlist.org/WildList/Real-Time.htm>) available two days before the submission deadline for products. Since the maintainer of the WildList was on a scheduled vacation at this time, the most recent RTWL was not particularly new. The batch of additions to the test set this month contained no new samples of any great interest. Given that the newest inclusions were all samples with well-known extensions, and the majority

were worms of some sort, it was not anticipated that any of these would cause problems.

One point of note concerning testing is that both on-access and on-demand scans are performed for files located on the server. However, the accesses in the on-access tests are performed from a client machine. Thus there is an additional variable for the throughput functionality when scanning on access – namely that of data transfer from server. Since, in all cases, scanning occurs on the server, the bulk of the information transferred relates to the status of files as being infected or not – which may or may not be transferred to the client directly.

Some products provided popup warnings on the client, and others kept a real-time summary of files scanned and infected. However, the level of information in these real-time views seemed to have been reduced considerably in some cases, with the result of lessening network traffic and improving scanning speeds.

ESET NOD32 1.804

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

NOD32 for *NetWare* retains the distinction of functioning as two NLMs (a module each for the on-access scanner and

on-demand scanner). On-demand scans are performed via a command-line interface. The product has had this configuration for as long as I can remember and, despite being archaic in nature, it serves well as a local solution on *NetWare*. However, external administration options are not the order of the day here – such would have to be created by the user.



Despite the antiquated feel of the scanner, detection rates were as might be expected from *NOD32* (given its recent history in *VB* comparatives), with all samples detected both on access and on demand. Since no false positives were noted, *NOD32* is left with a new *VB* 100% award to add to its collection.

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 NetWare 6.5* service pack 1.1. Clients running *NetWare Client 4.9* service pack 2.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2004/test_sets.html.

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

NetWare 6.5 on-access (OA) tests and on-demand (OD) tests	ItW File		Macro		Polymorphic		Standard		Scanning rate
	Number missed (OA) (OD)	% (OA) (OD)	Number missed (OA) (OD)	% (OA) (OD)	Number missed (OA) (OD)	% (OA) (OD)	Number missed (OA) (OD)	% (OA) (OD)	Executables throughput (kB/s)
CA eTrust Antivirus	0 0	100.00% 100.00%	12 12	99.82% 99.82%	2 2	99.87% 99.87%	2 2	99.90% 99.90%	2103.6
CAT Quick Heal	0 0	99.95% 100.00%	77 77	98.13% 98.13%	882 882	95.37% 95.37%	191 188	91.29% 91.60%	3314.7
DialogueScience Dr.Web	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 0	99.69% 100.00%	2629.5
Eset NOD32	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	7103.0
Kaspersky KAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 0	99.85% 100.00%	1967.4
McAfee NetShield	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 1	99.79% 99.91%	994.4
Norman FireBreak	0 0	100.00% 100.00%	2 2	99.95% 99.95%	180 180	91.24% 91.24%	11 11	99.63% 99.63%	2010.8
Sophos Anti-Virus	0 0	100.00% 100.00%	11 3	99.73% 99.93%	0 0	100.00% 100.00%	17 14	99.09% 99.24%	3824.7
Symantec SAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3906.7
VirusBuster VBSHield	0 0	100.00% 100.00%	0 0	100.00% 100.00%	602 602	89.12% 89.12%	17 16	99.01% 99.19%	1886.0

