virus BULLETIN

EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS 2003–2004

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.

WINDOWS 2003 SERVER: NOV 03

Although the deadline for product submissions for this test was 6 October 2003, the test sets were based upon the July 2003 WildList – a long delay indeed. However, this was the newest data available at the time. Although new WildList data was available three days after the deadline, this data was not used as it was from the newly inaugurated Real-Time WildList.

As for additions to the test sets this month, there were rather more than the usual bunch and a selection across the various types. Most unusually, a batch virus, BAT/Mumu.A, made its way into the wild, as well as the slightly more common sprinkling of macro viruses.

Eset NOD32 1.529

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

NOD32 produced an unsurprising 100 per cent detection rate and thus earns a VB 100% award. There was one fly in the ointment which affected many of the products in this review – this is by no means specific to *NOD32*, and neither was *NOD32* one of the worst offenders. The problem is that over 50 per cent of the products require a reboot when installing. Given that *Windows 2003 Server* is a server platform, this seems likely to irritate administrators no end.

Windows 2003 Server on-access (OA) tests and on-demand (OD) tests	ItW File		ItW Boot		ItW Overall		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	Number missed OA OD	% OA OD	Number missed OA OD	% OA OD	Executables throughput (kB/s)
AhnLab V3Net	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	81 79	98.11% 98.18%	9239 9119	42.74% 45.48%	314 313	85.38% 85.42%	23779.7
Alwil Avast!	- 1	- 99.56%	- 0	- 100.00%	- 1	- 99.58%	- 18	- 99.56%	- 153	- 91.21%	- 13	- 99.73%	3255.5
CA eTrust Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	4 4	99.90% 99.90%	1 1	99.89% 99.89%	2 0	99.88% 100.00%	6286.6
CA Vet Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.87% 99.87%	4 2	99.78% 99.90%	7012.0
CAT QuickHeal	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	107 101	97.45% 97.54%	1086 1078	92.85% 92.89%	660 318	60.88% 82.60%	9115.5
DialogueScience Dr.Web	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1953.3
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%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	9270.0
FRISK F-Prot Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 3	97.53% 97.53%	3 3	99.79% 99.79%	6145.3
F-Secure Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.92% 99.92%	3 1	99.85% 99.98%	2681.0
GDATA AntiVirusKit	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 1	100.00% 99.92%	0 0	100.00% 100.00%	1286.9
Grisoft AVG	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	23 20	99.44% 99.51%	925 257	81.40% 85.97%	47 23	97.15% 99.01%	4340.7
Kaspersky KAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.92% 99.92%	11 0	99.69% 100.00%	4340.7
MicroWorld eScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.92% 99.92%	11 0	99.69% 100.00%	3906.7
NAI McAfee VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 3	99.79% 99.79%	5944.9
Norman Virus Control	3 3	99.67% 99.67%	0 0	100.00% 100.00%	0 3	99.68% 99.68%	- 3	- 99.93%	- 180	- 91.24%	- 4	- 99.87%	8043.1
NWI VirusChaser	1 1	99.56% 99.56%	0 0	100.00% 100.00%	1 1	99.58% 99.58%	4 4	99.90% 99.90%	0 0	100.00% 100.00%	4 0	99.69% 100.00%	3255.5
SOFTWIN BitDefender	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	13 13	99.69% 99.69%	22 23	96.55% 96.50%	40 38	98.88% 99.01%	347.0
Sophos Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	8 8	99.80% 99.80%	18 18	98.06% 98.06%	14 14	99.49% 99.49%	9270.0
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%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	4340.7
Trend ServerProtect	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	215 515	95.77% 94.38%	1 3	99.98% 99.85%	9595.3
VirusBuster VirusBuster	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	101 101	91.45% 91.45%	11 8	99.67% 99.82%	2804.8

WINDOWS NT 4.0: FEB 04

It is sometimes a knotty problem deciding which platforms should be included in *Virus Bulletin* comparative testing. The decision by *Microsoft* to remove support from an OS is not necessarily an indication of that OS becoming extinct in the wild. From a marketing point of view, *NT* users are likely to upgrade to *XP* if *NT* is no longer supported. *NT* was always much stronger among corporates than in the home-user environment and, in a large company, expense is not always as significant a consideration as continuity and the ability to make long term plans. On balance, although doomed to lack of support in the near future, *NT* is still a rather more relevant platform for business users.

The test sets used in this review were the first to be aligned to the real-time WildList and as such were expected to provide rather more of a challenge for the products than the test sets used in past reviews. Unfortunately, both the *VB2003* conference and the Christmas period conspired to cause delays in the updating of the real-time WildList and, on the date when the test set was finalised, the 'real-time' WildList was updated only as far as late October 2003.

Eset NOD32 1.595

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

This month sees another addition to *Eset*'s growing collection of VB 100% awards. With 100 per cent detection in all categories and no false positives, *NOD32* pulls no surprises out of the bag.

Windows NT 4.0 on-access (OA) tests and on-demand (OD) tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard		Scanning rate
	Number missed OA OD	% OA OD	Number missed OA OD	% 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)
AhnLab V3VirusBlock	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	82 82	98.08% 98.08%	9139 9139	43.19% 43.19%	313 313	85.57% 85.57%	3824.7
Alwil Avast!	N/A 0	- 100.00%	0 0	100.00% 100.00%	- 100.00%	N/A 18	- 99.56%	N/A 124%	- 93.54%	N/A 23	- 99.10%	2040.8
Authentium Command	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.91% 99.91%	4 1	99.76% 99.91%	2161.8
CA eTrust Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	4 4	99.90% 99.90%	1 1	99.89% 99.89%	2 0	99.88% 100.00%	1866.7
CA Vet Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.87% 99.87%	4 2	99.78% 99.90%	2307.7
CAT Quickheal	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	107 103	97.45% 97.49%	1086 1044	92.85% 95.12%	647 310	61.99% 83.33%	3670.7
DialogueScience Dr.Web	1 1	99.59% 99.59%	0 0	100.00% 100.00%	99.60% 99.60%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1841.5
Eset NOD32	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	2681.0
Fortinet FortiClient	9 9	98.94% 99.10%	9 9	0.00% 0.00%	95.39% 95.55%	2328 2328	43.10% 43.10%	12524 12524	23.44% 23.44%	1226 1226	27.40% 27.40%	2119.9
FRISK F-Prot Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.91% 99.91%	3 5	99.79% 99.74%	2298.0
F-Secure Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 1	99.85% 99.98%	1799.1
GDATA AntiVirusKit	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	663.8
Grisoft AVG	0 N/A	100.00% -	0 0	100.00% 100.00%	100.00% -	23 N/A	99.44% -	757 N/A	83.64% -	30 N/A	98.50% -	1709.2
H+BEDV AntiVir	1 2	99.79% 99.76%	0 0	100.00% 100.00%	99.80% 99.77%	56 31	99.26% 99.53%	1004 1004	84.94% 84.94%	52 50	97.91% 98.03%	1912.4
Kaspersky KAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	2 0	99.88% 100.00%	1886.0
MicroWorld eScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1406.0
NAI VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 3	99.79% 99.79%	2567.8
Norman Virus Control	N/A 0	- 100.00%	0 0	100.00% 100.00%	- 100.00%	N/A 2	- 99.95%	N/A 174	- 91.72%	N/A 3	- 99.89%	1229.1
SOFTWIN BitDefender	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	13 13	99.69% 99.69%	11 10	97.46% 97.51%	60 60	97.79% 97.79%	710.3
Sophos Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	8 8	99.80% 99.80%	1 1	99.95% 99.95%	14 14	99.49% 99.49%	3005.1
Symantec SAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1829.2
Trend PC-cillin	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	215 215	95.77% 95.77%	8 8	99.82% 99.82%	2776.3
Unasoft UNA Pro	157 126	76.03% 80.03%	9 4	0.00% 55.56%	73.30% 79.15%	3048 1783	26.88% 57.92%	14446 14379	11.67% 12.85%	904 773	57.30% 64.31%	2170.4
VirusBuster VirusBuster	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	101 101	91.78% 91.78%	8 8	99.82% 99.82%	1747.4

WINDOWS XP PROFESSIONAL: JUNE 04

Changes to the test sets this month were limited to the addition of samples to the In the Wild (ItW) test set – though this was quite enough replication for one review – there were in excess of 60 on this occasion. The majority of these were samples of W32/Bagle and W32/Netsky. Smaller numbers of W32/Mydoom, W32/Dumaru, W32/Mimail and W32/Sober were also added, together with the usual collection of viruses which do not occur in a plethora of versions and varieties.

The test sets were aligned with the Real Time WildList as of 5 May 2004, with the products being supplied on 7 May 2004.

Eset NOD32 1.753

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

While neck-and-neck with *CA eTrust*, *NOD32* maintains its reputation for speed in the OLE test set. Upon compressed executables, however, *NOD32* is comfortably the fastest product on test. Like several other products, *NOD32* does not detect the DLL-extensioned W32/Lovelorn sample, but does detect this in those samples within the ItW test set. The result, as might be suspected, is a VB 100% award for *Eset*.

Windows XP Professional on-access (OA) tests and on-demand (OD) tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard		Scanning rate
	Number missed OA OD	% OA OD	Number missed OA OD	% 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)
AhnLab V3 VirusBlock	1 1	99.67% 99.67%	0 0	100.00% 100.00%	99.67% 99.67%	75 75	98.28% 98.28%	9168 9163	44.97% 44.99%	305 305	85.53% 85.53%	14782.0
Alwil Avast!	1 1	99.67% 99.67%	0 0	100.00% 100.00%	99.67% 99.67%	18 18	99.56% 99.56%	112 112	93.58% 93.58%	18 15	99.12% 99.36%	5259.0
Authentium Command	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.91% 99.91%	5 2	99.58% 99.72%	4840.1
CA eTrust Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	6 4	99.86% 99.90%	1 1	99.89% 99.89%	4 1	99.51% 99.82%	3824.7
CA Vet Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.87% 99.87%	5 3	99.60% 99.72%	3992.2
CAT Quick Heal	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	103 103	97.54% 97.49%	1085 1044	92.86% 95.12%	647 300	62.82% 83.56%	9270.0
DialogueScience Dr.Web	1 0	99.89% 100.00%	0 0	100.00% 100.00%	99.89% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 0	99.69% 100.00%	1974.5
Eset NOD32	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	14023.9
Fortinet FortiClient	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	35 35	99.15% 99.15%	5065 5065	64.28% 64.28%	107 107	96.57% 96.57%	2278.9
FRISK F-Prot Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	2 2	99.91% 99.91%	4 2	99.60% 99.72%	3934.8
F-Secure Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 1	99.85% 99.98%	3125.3
GDATA AntiVirusKit	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	664.6
Grisoft AVG	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	23 20	99.44% 99.51%	757 257	83.64% 85.97%	34 27	98.17% 98.56%	4797.7
H+BEDV AntiVir	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	56 28	99.27% 99.52%	622 522	86.72% 87.18%	35 34	98.24% 98.42%	3506.0
Kaspersky KAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	11 0	99.69% 100.00%	3598.2
MicroWorld eScan	1 1	99.67% 99.67%	0 0	100.00% 100.00%	99.67% 99.67%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	2655.0
NAI McAfee VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 3	99.79% 99.79%	5415.2
Norman Virus Control	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	2 2	99.95% 99.95%	180 112	91.24% 96.53%	12 1	99.45% 99.82%	1212.7
NWI Virus Chaser	1 1	99.89% 99.89%	0 0	100.00% 100.00%	99.89% 99.89%	4 0	99.90% 100.00%	0 0	100.00% 100.00%	3 1	99.69% 99.82%	3720.6
SOFTWIN BitDefender	2 1	99.58% 99.94%	0 0	100.00% 100.00%	99.59% 99.95%	13 13	99.69% 99.69%	4 4	99.78% 99.78%	49 48	98.10% 98.28%	869.5
Sophos Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	8 8	99.80% 99.80%	0 0	100.00% 100.00%	16 16	99.12% 99.12%	8163.2
Symantec SAV	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3335.0
Trend Internet Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	215 215	95.77% 95.77%	9 9	99.63% 99.63%	7926.6
UNA UNA Pro	104 92	80.72% 81.78%	7 3	0.00% 57.10%	78.88% 81.21%	1986 796	53.06% 80.96%	14284 14229	16.34% 17.50%	755 682	64.62% 67.79%	7012.0
VirusBuster VirusBuster	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	101 102	91.45% 91.45%	13 10	99.30% 99.45%	2863.5