

EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS 2005-2006

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.

RED HAT LINUX 9: APRIL 06

The test sets used in this comparative were aligned to the most recent WildList available at the time, which was the December 2005 WildList. Products were submitted with a deadline of 6 March 2006. This gave the vendors ample time to add new viruses to their databases, so few misses were expected in the In the Wild (ItW) test set.

There was a little more potential for problems in the clean test sets, which have undergone major changes. As has been mentioned previously (see *VB*, March 2006, p.13), self-extracting executables have been given their own test set (dynamically compressed files), which is distinct from the clean set. This has entailed the removal of many files from the old clean set, and the addition of files to both the clean and dynamic sets. As a result of these changes it should also be noted that comparisons with past clean set throughput rates are no longer valid.

Eset NOD32 2.51.2

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

The *Eset* submission not only performed admirably in detection, but also offered well documented installation procedures. There was thus ample reason to award *NOD32* a further VB 100% for its collection.



Red Hat Linux 9 on-access (OA) and on-demand (OD) tests	ItW file		Macro		Polymorphic		Standard		Linux	
	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
Alwil avast!	0	100.00%	18	99.56%	112	93.58%	13	99.57%	8	83.33%
	0	100.00%	18	99.56%	112	93.58%	14	99.38%	8	83.33%
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	86.67%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	86.67%
CAT Quick Heal	0	100.00%	75	98.18%	310	96.57%	155	92.78%	7	60.00%
	0	100.00%	75	98.18%	310	96.57%	101	96.39%	7	60.00%
Doctor Web Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet Linux Guard	-	-	-	-	-	-	-	-	-	-
	0	100.00%	4	99.90%	219	92.46%	15	99.45%	31	20.00%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	93.33%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	93.33%
Grisoft AVG Anti-Virus	0	100.00%	0	100.00%	425	83.72%	42	97.27%	16	48.33%
	0	100.00%	0	100.00%	425	83.72%	42	97.33%	16	48.33%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee LinuxShield	0	100.00%	0	100.00%	29	97.67%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	29	97.67%	0	100.00%	0	100.00%
MicroWorld eScan Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	180	91.24%	12	99.45%	5	73.33%
	0	100.00%	0	100.00%	180	91.24%	12	99.45%	5	73.33%
SOFTWIN BitDefender	0	100.00%	34	99.12%	9	99.71%	22	98.91%	11	53.33%
	0	100.00%	34	99.12%	9	99.71%	20	99.04%	11	53.33%
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend Micro ServerProtect	0	100.00%	9	99.78%	215	95.81%	23	99.28%	6	86.67%
	0	100.00%	9	99.78%	215	95.81%	25	99.16%	4	93.33%
VirusBuster 2005	0	100.00%	0	100.00%	52	97.24%	8	99.82%	37	26.67%
	0	100.00%	0	100.00%	124	92.59%	23	99.27%	32	48.33%

WINDOWS SERVER 2003 ENTERPRISE X64 VERSION: DEC 05

With 64-bit systems there is a range of hardware available, with operating systems to match.

Having asked a selection of vendors and end users, it seems that *Athlon 64* processors are the most commonly used with 64-bit operating systems and thus were chosen as a hardware platform. *Windows Server 2003 x64* version was selected as the operating system, again based on reports received from a number of vendors and end users.

The biggest surprise in the review was the lack of submissions. I was certainly expecting a smaller number of products to be submitted for this test than for the previous *Windows 2003 Server* review, but for numbers to drop to just over a third was more extreme than expected. Whether other products were missing due to corporate cowardice or known incompatibilities with the platform I will leave to the reader to imagine.

With hardware and operating systems already changed drastically it seemed unwise to make major changes to the test sets too. In the event, the most recent WildList available at the start of the test period was that from July 2005. Products were dated no later than 31 October 2005.

Windows Server 2003 Enterprise X64 version on-access (OA) and on-demand (OD) tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	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
Alwil avast!	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	18 18	99.56% 99.56%	112 113	93.58% 93.57%	17 15	99.18% 99.36%
CA eTrust Antivirus (I)	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%	4 2	99.51% 99.63%
CA eTrust Antivirus (V)	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	12 12	99.82% 99.82%	1 1	99.95% 99.95%	3 1	99.84% 99.96%
CAT Quick Heal	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	82 75	98.04% 98.18%	313 313	96.25% 96.25%	147 100	93.06% 96.48%
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%
GDATA AntiVirusKit	0 0	100.00% 100.00%	0 0	0.00% 100.00%	99.55% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%
Grisoft AVG	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	257 257	85.97% 85.97%	30 27	98.41% 98.56%
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%
McAfee VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	29 0	97.67% 100.00%	0 0	100.00% 100.00%
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%

That is not to say that there wasn't a great temptation to add new samples to both clean and infected test sets. The clean test sets in particular are perhaps unrepresentatively high in dynamic archives, which slow on-demand scan speeds more than would be seen in most real-world settings.

Since this was the first outing of this hardware, the throughput tests cannot be compared directly with past results.

ESET NOD32 1.1268(20051031)

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

Having been tested in a comparative review two months ago and a standalone review in the November 2005 issue of the magazine (see *Virus Bulletin*, November 2005, p.16), no great surprises were expected from *NOD32*.

NOD32 has ZIP archive scanning turned off by default, although *W32/Heidi.A* is detected by the engine as a special case, accounting for full detection of this virus in the standard test set. In any case, detection was at its usual high levels for this product, and *NOD32* easily obtains a VB 100% award for its collection.



WINDOWS XP: JUNE 05

The testing process for this comparative review was the smoothest that I can remember, with only a handful of crashes to mar the plain sailing. The test sets were aligned to the February 2005 WildList, with a product submission deadline of 3 May 2005. This time lag should have been enough for all but the most tardy developers to catch up with detection, thus high detection rates were expected. The additions to the In the Wild (ItW) test set were a dull bunch, as ever, and possibly the most uninspiring yet. The predominance of various *W32/*bot* samples does not give cause for further comment.

Eset NOD32 1.1087

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.63%
ItW File	100.00%	Polymorphic	100.00%

The results for *NOD32* were somewhat perplexing for a product which claims not to scan within archives. Despite this claim it detected samples of *W32/Heidi.A* in their zipped form, suggesting that such scanning may be activated by default.

On this occasion *Eset's* scanner missed two samples in the standard set, though this was not sufficient to deny the company another VB 100%.



Windows XP on-access (OA) and on-demand (OD) tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	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
AhnLab V3 Pro	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	47 52	98.97% 99.00%	3187 3180	74.80% 74.82%	70 62	96.16% 97.72%
Alwil avast!	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	18 18	99.56% 99.56%	112 112	93.58% 93.58%	19 17	98.93% 99.12%
ArcaBit ArcaVir 2005	1 1	99.96% 99.96%	1 0	100.00% 100.00%	99.96% 99.96%	34 70	99.45% 98.99%	1308 1312	85.97% 85.90%	22 19	98.91% 99.22%
Authentium Command	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.95% 99.95%	5 2	99.58% 99.72%
Avira Avira	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%
BLC Win Cleaner	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	86 81	97.96% 98.03%	339 340	96.43% 96.43%	474 101	72.45% 96.39%
CA eTrust Antivirus (I)	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%	4 1	99.51% 99.82%
CA eTrust Antivirus (V)	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	12 10	99.82% 99.88%	2 2	99.87% 99.87%	5 4	99.60% 99.70%
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%	6 3	99.54% 99.72%
CAT Quick Heal	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	86 81	97.96% 98.03%	339 340	96.43% 96.43%	474 101	72.45% 96.39%
Doctor Web Dr.Web	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 0	99.69% 100.00%
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%	2 2	99.63% 99.63%
Fortinet FortiClient	1 1	99.96% 99.96%	0 0	100.00% 100.00%	99.96% 99.96%	660 660	84.19% 84.19%	122 123	94.83% 94.72%	62 63	97.46% 97.41%
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%	6 0	99.97% 100.00%	8 6	99.40% 99.56%
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 2	99.85% 99.92%
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%
Grisoft AVG	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	3 0	99.93% 100.00%	757 257	83.64% 85.97%	34 27	98.17% 98.56%
H+BEDV AntiVir	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%
Hauri ViRobot	0 0	100.00% 100.00%	3 3	0.00% 0.00%	99.50% 99.50%	0 12	100.00% 99.71%	49 9	98.83% 99.78%	18 16	98.96% 99.08%
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%
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%
MicroWorld eScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	9 0	99.71% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%
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%	181 180	91.03% 91.24%	8 6	99.50% 99.63%
NWI Virus Chaser	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 0	99.69% 100.00%
SOFTWIN BitDefender	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 35	100.00% 99.10%	6 6	99.73% 99.73%	14 14	99.33% 99.33%
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%	14 15	99.33% 99.30%
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%
UNA UNA	12 12	97.57% 97.57%	0 0	100.00% 100.00%	97.58% 97.58%	1891 1891	55.06% 55.06%	14264 14264	20.28% 20.28%	489 489	77.45% 77.45%
VirusBuster VirusBuster	0 0	100.00% 100.00%	0 0	100.00% 100.00%	100.00% 100.00%	0 15	100.00% 99.81%	108 109	92.58% 92.55%	18 17	98.98% 99.17%

