COMPARATIVE REVIEW

Windows XP Professional

Matt Ham

It was with a certain degree of trepidation that I embarked upon this review: new hardware, a new platform and some new products to do combat with – and my anticipation of troubles was well founded.

The platform, *Windows XP Professional*, has an unhealthy obsession with attempting to contact the outside world, causing it to complain a few times in the process of testing. At first, boot-up of *XP* seems remarkably speedy, however the illusion is soon dispelled since, for several minutes, no network access is available, and on-access scanner components took up to five minutes to begin under normal circumstances. Under some circumstances, on-access functionality vanished or took literally hours to appear.

In addition to the new software, this month's Comparative saw an improvement in hardware. This has one major effect upon the results of the tests in that the results of past tests are no longer directly comparable with those produced from now on. Other than these (admittedly fundamental) changes, the testing procedure remained the same as it has been in the past. For details of the test regime please refer to past Comparative reviews. As ever, the results are specific to *VB*'s particular configuration and a product which proved impossible to test on our machines may show friendlier behaviour for other users.

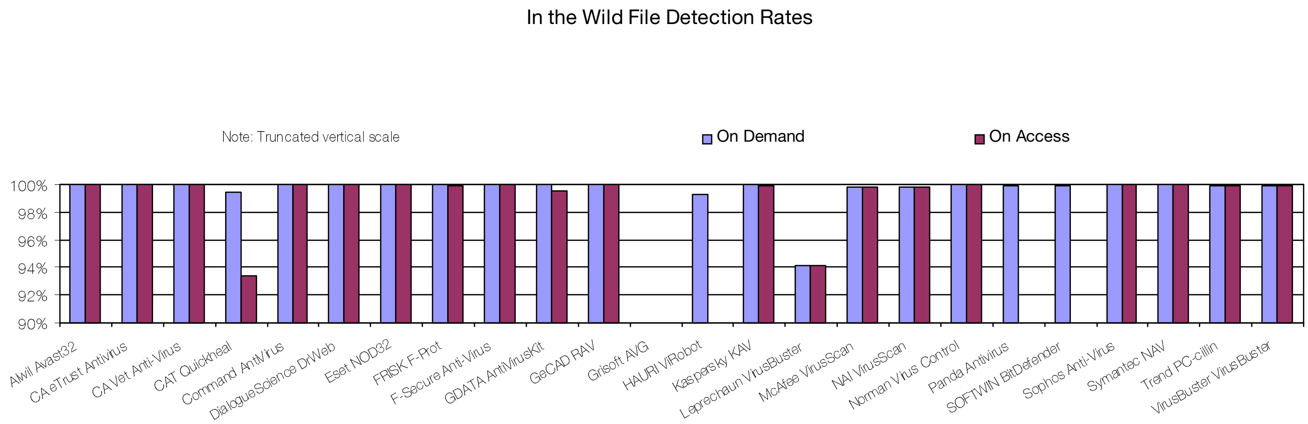
The Products

The line-up of products was the largest that has ever been assembled for a *Virus Bulletin* Comparative. Only one product proved totally untestable: *Ggreat*'s offering – a small downloader program which relied upon an Internet connection for the installation of its files. It was decided that giving test machines laden with viruses free access to the Internet was not an ideal plan. Of the remaining 24 products two were stated by their developers to have known bugs in the versions tested: *HAURI*'s *ViRobot* and *Grisoft*'s *AVG*. These were tested nonetheless. Of those products which were both new and testable there were offerings from *Leprechaun* and *CAT Computer Systems*.

Alwil Avast32 3.0.459.3

ItW Overall	100.00%	Macro	99.55%
ItW Overall (o/a)	100.00%	Standard	99.46%
ItW File	100.00%	Polymorphic	93.61%

Alwil's *AVAST32* is unfortunate in that it is the first product which will be described in less than awed tones. In what became something of a running theme, the on-access



scanner of *Avast32* did not perform as well as expected at first. This is a kind way of describing an on-access component which refused to start up, complaining of time-out errors. The answer to this problem lay in the traditional magic trick of rebooting the computer.

Once into its working state, *Avast32* scored full detection both on access and on demand in the Wild. Since no false positives were detected, *Alwil* gains the first VB100% of this review. As far as overall detection was concerned, results were good in all areas, with polymorphics being the only area where improvements might be hoped for.

CA eTrust Antivirus 6.0.96

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.87%
ItW File	100.00%	Polymorphic	99.94%

eTrust continued its tradition of being the product with the largest collection of mandatory patches. It was sometimes a little less than clear as to where the files involved should be placed, an area where improvement might be delivered.

However, *eTrust* put in another sterling performance, resulting in a VB100% award. One theme which became notable during the tests was the general increase in scan speed as produced by the combination of new hardware and operating system. Although the increase in machine specification would give an obvious boost to scan rates, the effect of the operating system is as yet difficult to gauge.

CA Vet Anti-Virus 10.4.7.0

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.81%
ItW File	100.00%	Polymorphic	97.00%

Vet has long been the only remaining product to be submitted to *VB*'s tests on floppies. This time, however, a CD was the medium of choice for *Vet*. This may be a sign of the increasing size of the products. Not including those three products supplied on CD, the size of the files submitted averaged over 30 MB per product. *Vet* still gains prizes for its small footprint in comparison, and walks away with a VB100% award for its detection performance. Weaknesses in detection were few, though the performance on the polymorphics is, again, an area where things could be improved.

CAT Quickheal 6.06

ItW Overall	99.45%	Macro	95.45%
ItW Overall (o/a)	93.35%	Standard	59.01%
ItW File	99.42%	Polymorphic	29.08%

CAT impressed from the start, having none of the technical difficulties so often associated with a new product. This was slightly tarnished by its inability to perform on-access boot sector scanning, despite the on-access file scanning being clearly operational. As far as detection was concerned, the results were decidedly mixed. When faced with a modern virus *Quickheal* is much more effective at detection than when faced with one of the older in the *VB* test sets. As an example, W32/CTX was detected in all of its samples in the test set, while older polymorphics were passed by without a mutter. Quite how disturbing this lack of detection is, will be very much a matter of opinion.

On the small niggles front, a couple of features surfaced. First, the performing of floppy scans was remarkably irksome, with the settings in need of constant adjustment. Secondly, the scanner would not delete infected archive files – despite detecting infections within these files.

Command AntiVirus 4.64.3

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.68%
ItW File	100.00%	Polymorphic	95.43%

Command AntiVirus is the fourth product to be worthy of a VB100% award. This is not without a measure of anger at the product due to the nature of its log files, which reported scanned files in a manner requiring some degree of

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast32	0	100.00%	0	100.00%	100.00%	18	99.55%	116	93.61%	18	99.46%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.94%	2	99.87%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	73	97.00%	3	99.81%
CAT Quickheal	2	99.42%	0	100.00%	99.45%	181	95.45%	12408	29.08%	784	59.01%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	99	95.43%	6	99.68%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	34	99.20%	0	100.00%	1	99.98%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	99	95.43%	10	99.65%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.96%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.96%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	49	97.60%	5	99.73%
Grisoft AVG	115	86.06%	0	100.00%	86.91%	106	97.32%	242	86.05%	81	96.20%
HAURI ViRobot	1	99.75%	1	92.31%	99.30%	185	95.02%	10890	36.11%	628	67.55%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.96%	0	100.00%
Leprechaun VirusBuster	32	93.72%	0	100.00%	94.10%	220	95.15%	1478	82.68%	131	92.10%
McAfee VirusScan	1	99.83%	0	100.00%	99.84%	0	100.00%	8	99.86%	3	99.85%
NAI VirusScan	1	99.83%	0	100.00%	99.84%	0	100.00%	8	99.86%	3	99.85%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	623	90.81%	30	98.65%
Panda Antivirus	1	99.92%	0	100.00%	99.92%	2	99.93%	1091	86.33%	22	99.39%
SOFTWIN BitDefender	1	99.92%	0	100.00%	99.92%	14	99.63%	128	90.93%	61	97.62%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	12	99.71%	64	95.54%	18	99.41%
Symantec NAV	0	100.00%	0	100.00%	100.00%	0	100.00%	14	99.76%	0	100.00%
Trend PC-cillin	1	99.95%	0	100.00%	99.95%	0	100.00%	263	93.32%	7	99.84%
VirusBuster VirusBuster	1	99.95%	0	100.00%	99.95%	0	100.00%	140	90.98%	10	99.73%

cajoling when extracting results. This and the log files of other products were the primary cause of reviewer rage in the analysis of this Comparative.

DialogueScience DrWeb 4.28

ItW Overall	100.00%	Macro	99.20%
ItW Overall (o/a)	100.00%	Standard	99.98%
ItW File	100.00%	Polymorphic	100.00%

DrWeb seems prone to producing strange results of late, and in this test managed to miss a selection of *Excel* viruses which the product has detected in all previous tests.

Whether this is due to some virus database bug or an overzealous trimming of heuristic triggers, will likely remain a secret known only by the *DrWeb* team. Other than this momentary flash of excitement, *DrWeb* performed in just the manner expected, notching up yet another VB100%.

Eset NOD32 1.256

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

Once more comes the arduous task of noting details of *NOD32*, before declaring it to have gained yet another VB100% award. Speed and detection rate were maintained once more for *Eset*'s product leading to a predictable, but no doubt welcome, result for the Slovak team.

FRISK F-Prot 3.12

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	99.92%	Standard	99.65%
ItW File	100.00%	Polymorphic	95.43%

The second of the two purely *F-Prot*-based products in this month's line up, *FRISK*'s product showed both similarities to and differences from *Command F-Prot*. Similar were the overall detection rates and speed of scanning. The difference was that W32/Nimda.A samples were missed due to extension issues in the Wild on access. This was sufficient to deny *FRISK F-Prot* a VB100% award.

F-Secure Anti-Virus 5.40

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.85%
ItW File	100.00%	Polymorphic	99.96%

F-Secure Anti-Virus remained the slowest of the three products utilizing the *F-Prot* engine, no doubt due to its use of the *AVP* engine in parallel. This extra line of defence proved worthwhile, with the detection rate of the two engines combined being predictably higher than either component. This was sufficient to gain *FSAV* a VB100% award.

GDATA AntiVirusKit Professional 11.0.4

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	99.53%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.96%

AntiVirusKit is another of those products offering two scanning engines in one package – in this case the *RAV* and *KAV*. Although *AVK* is not the speediest of scanners, it has not suffered too much by the additional lag that such a combination can produce. In this case the combination has also proved fruitful in detection rate – with file detection In the Wild being perfect. However this was spoiled by the product's failure to detect Michelangelo in the boot sector tests on access and a false positive in the clean set. With a performance so close to a VB100%, however, it seems likely that such an award is not far around the corner.

GeCAD RAV 8.5.8.0

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.73%
ItW File	100.00%	Polymorphic	97.60%

RAV's on-access scanner failed to operate at all when first installed. Reinstallation solved this problem, and the results were well worth waiting for. With full detection of In the Wild viruses and no false positives, *RAV* duly gained a VB100% award. Other results were solid, with the polymorphic set showing good signs of improvement.

Grisoft AVG

ItW Overall	86.91%	Macro	97.32%
ItW Overall (o/a)	86.91%	Standard	96.20%
ItW File	86.06%	Polymorphic	86.05%

In my last review of *AVG* I noted the longevity of the CD supplied – and the remarkable manner in which the updater for *AVG* had managed to cope with this antiquated base program. Alas, a piece of history vanished in this review, with this version of *AVG* causing a blue-screen and proving impossible to update. *Grisoft* provided a slightly less ancient copy of the base software which did not have these problems – but warned that the update software had serious, now corrected, bugs which would render the detection rates 'interesting'. This proved well founded, with results being far below those expected from the *AVG* product. Since, effectively, a crippled version was on test, comments on detection do not seem relevant to current performance.

HAURI ViRobot Expert 4.0 2002-05-07

ItW Overall	99.30%	Macro	95.02%
ItW Overall (o/a)	N/A	Standard	67.55%
ItW File	99.75%	Polymorphic	36.11%

The second of the self-declared crippled products, *HAURI* got off to a predictably unhappy start, as it locked up the machine when the on-access scanner was activated. This was corrected easily by removing the on-access component – a drastic but effective measure. *HAURI* state that current versions have been altered, and this problem does, indeed, seem to have been remedied in the products shipping currently.

The performance of *HAURI* on the last few tests caused considerable woe both for reviewer and developer, so it was pleasant to note significant improvement in detection rate. Detection was definitely in the acceptable range for In the Wild viruses, though narrowly missing complete detection. Akin to *Quickheal*, this improvement in detection rates has been applied with the seeming priority of more recent viruses over aged zoo specimens. As was noted for that product, the decision as to whether these files are worthy of detection lies with the individual user.

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast32	0	100.00%	0	100.00%	100.00%	18	99.55%	112	93.42%	18	99.48%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.94%	2	99.87%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	73	97.00%	5	99.62%
CAT Quickheal	2	99.42%	13	0.00%	93.35%	181	95.45%	12408	29.08%	931	46.09%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	99	95.43%	6	99.74%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	34	99.20%	0	100.00%	1	99.98%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	1	99.92%	0	100.00%	99.92%	0	100.00%	99	95.43%	12	99.60%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.96%	3	99.85%
GDATA AntiVirusKit	0	100.00%	1	92.31%	99.53%	0	100.00%	1	99.96%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	49	97.60%	5	99.73%
Grisoft AVG	115	86.06%	0	100.00%	86.91%	106	97.32%	410	83.75%	81	96.20%
HAURI ViRobot	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Kaspersky KAV	3	99.88%	0	100.00%	99.88%	19	99.60%	1	99.96%	2	99.87%
Leprechaun VirusBuster	32	93.72%	0	100.00%	94.10%	220	95.15%	1478	82.68%	131	92.10%
McAfee VirusScan	1	99.83%	0	100.00%	99.84%	0	100.00%	8	99.86%	3	99.85%
NAI VirusScan	1	99.83%	0	100.00%	99.84%	0	100.00%	8	99.86%	3	99.85%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	623	90.81%	30	98.65%
Panda Antivirus	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
SOFTWIN BitDefender	n/a	n/a	0	100.00%	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	12	99.71%	64	95.54%	18	99.41%
Symantec NAV	0	100.00%	0	100.00%	100.00%	0	100.00%	14	99.76%	0	100.00%
Trend PC-cillin	1	99.95%	0	100.00%	99.95%	0	100.00%	263	93.32%	7	99.84%
VirusBuster VirusBuster	1	99.95%	0	100.00%	99.95%	0	100.00%	140	90.98%	12	99.60%

Kaspersky Anti-Virus 4.0.50

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	99.88%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.96%

With the arrival of the new hardware in the *VB* offices there came a new peril – the new machines came complete with sound cards and an audible, if tinny, internal speaker. When faced with viruses, *Kaspersky Anti-Virus* squeals like a pig. This had the effect of attracting a great deal of astonished attention, followed by a rapid clearance of the environs. Should this not be the desired effect, of course, the sound may be turned off as a program option.

As has so often been the case in the past *KAV* missed out on a VB100% award by the slimmest of margins – and, once more, through opting not to scan extensionless programs on access. Other than deliberate non-scanning, detection rates were impressive.

Leprechaun VirusBuster II

ItW Overall	94.10%	Macro	95.15%
ItW Overall (o/a)	94.10%	Standard	92.10%
ItW File	93.72%	Polymorphic	82.68%

This product, as its name suggests, is a rebadging of the *VirusBuster* product. *Leprechaun* has been a player in the Australian market for a considerable time now, yet it is the first time that I have reviewed the product. Unfortunately, first appearances did little to thrill. *VirusBuster* lacks that most vital of reviewer utilities – an obvious version number.

All functions operated as expected and scanning was easy, if a trifle inelegant. However, the detection rates were none too impressive and definitely worse than the performance of the other versions of *VirusBuster* tested in the past. With a plethora of misses In the Wild, *VirusButer* managed to rank bottom in this category for detection, despite competing against a product declared by its manufacturer to be defective. It also appeared not to have an option to scan inside archive files – rendering the archive scanning speed tests impossible. With evident potential in the engine, it remains to be seen whether this incarnation can fare better in future.

McAfee VirusScan 6.02.1019.1

ItW Overall	99.84%	Macro	100.00%
ItW Overall (o/a)	99.84%	Standard	99.85%
ItW File	99.83%	Polymorphic	99.86%

With a greed for possible VB100% awards, the Siamese twins that are *Network Associates* and *McAfee* submitted two products on this occasion. Unlike *CA*, whose products use different default engines, these two offerings use the same engine, differing in interface and functionality. Despite this it is possible to treat them as separate products, since history has shown that an interface can exercise all manner of influence upon the program lying behind it.

In fact, the results for the two programs were essentially identical, though missing out on a VB100% award as a result of missing a sample of W32/Gibe.A In the Wild. The *McAfee* product is the retail version of the software and, as such, the complexities of the program are remarkably hidden under the interface – lest casual users be scared away by the options which do exist.

NAI VirusScan 4.51

ItW Overall	99.84%	Macro	100.00%
ItW Overall (o/a)	99.84%	Standard	99.85%
ItW File	99.83%	Polymorphic	99.86%

Having summed up much of the two sister products in the preceding paragraph the matter of scanning speed remains. Most interesting is the comparative speed of *McAfee VirusScan* as opposed to *NAI VirusScan*. The two versions of the program offer almost identical throughput rates on both archived and unarchived files.

Norman Virus Control 5.3

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	98.65%
ItW File	100.00%	Polymorphic	90.81%

Norman Virus Control proved somewhat enigmatic in its on-access behaviour, which on first installing was most notable by its absence. Tweaking and cajoling had no effect, though on-access component error messages were generated, but performing the same actions upon an identical freshly re-imaged machine resulted in a fully functional on-access scanner.

In the past few reviews *NVC* has been castigated for its lack of a log facility and wondered at for the slow speed of scanning the clean set. There is now a log file facility, though the sluggish clean set scanning remains on the uncompressed executable set. This aside, *NVC* put in a good performance – good enough to result in a VB100% award. Distinct holes do remain on detection, however, with the polymorphic set continuing to give intriguing half detection in several of the sets.

Panda Antivirus Platinum 6.25.90

ItW Overall	99.92%	Macro	99.93%
ItW Overall (o/a)	N/A	Standard	99.39%
ItW File	99.92%	Polymorphic	86.33%

Panda Antivirus was another whose on-access component proved unpliable. Despite trying two versions of the software, the on-access component remained greyed-out permanently, with no amount of manipulation resulting in any on-access alerts or activity. In the remaining tests detection was by and large good, though there were weaknesses in the polymorphic set.

SOFTWIN BitDefender Professional 6.4.1

ItW Overall	99.92%	Macro	99.63%
ItW Overall (o/a)	N/A	Standard	97.62%
ItW File	99.92%	Polymorphic	90.93%

The subject of a recent standalone review, *BitDefender* behaved much as it did on its last inspection. In terms of on-access testing, however, Murphy Shield demanded a confirmation after every infected file had been detected. This was too tedious a key-press challenge and thus on-access file scanning was untested on this occasion. As far as detection was concerned, *BitDefender* was caught out In the Wild by samples of W32/Nimda.A which prevented it from achieving a clean sweep in that set. Elsewhere, the polymorphics were somewhat weak on detection and

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time(s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	Time(s)	Throughput (MB/s)
Alwil Avast32	93.0	5881.0		13.0	6102.6		63.0	2530.4	19.0	3926.7
CA eTrust Antivirus	89.0	6145.3		5.0	15866.8		44.0	3623.1	10.0	7460.7
CA Vet Anti-Virus	112.0	4883.3		6.0	13222.3		63.0	2530.4	12.0	6217.3
CAT Quickheal	125.0	4375.5	1	27.0	2938.3		50.0	10938.6	26.0	3051.3
Command AntiVirus	100.0	5469.3		4.0	19833.4		51.0	3125.8	6.0	12434.6
DialogueScience DrWeb	118.0	4635.0	[15]	8.0	9916.7		53.0	3007.9	9.0	8289.7
Eset NOD32	33.0	16573.7		3.0	26444.6		27.0	5904.3	7.0	10658.2
FRISK F-Prot	86.0	6359.7		4.0	19833.4		54.0	2952.2	6.0	12434.6
F-Secure Anti-Virus	204.0	2681.0		9.0	8814.9		124.0	1285.6	33.0	2260.8
GDATA AntiVirusKit	450.0	1215.4	1	23.0	3449.3		220.0	724.6	56.0	1332.3
GeCAD RAV	326.0	1677.7	[1]	11.0	7212.2		29.0	5497.1	14.0	5329.1
Grisoft AVG	171.0	3198.4		7.0	11333.4		68.0	2344.4	10.0	7460.7
HAURI ViRobot	32.0	17091.6	[1]	17.0	4666.7		40.0	3985.4	38.0	1963.4
Kaspersky KAV	154.0	3551.5		12.0	6611.1		85.0	1875.5	24.0	3108.6
Leprechaun VirusBuster	130.0	4207.2		40.0	1983.3	12	n/a	n/a	n/a	n/a
McAfee VirusScan	94.0	5818.4		5.0	15866.8		40.0	3985.4	9.0	8289.7
NAI VirusScan	100.0	5469.3		5.0	15866.8		42.0	3795.6	8.0	9325.9
Norman Virus Control	2222.0	246.1		4.0	19833.4		186.0	857.1	9.0	8289.7
Panda Antivirus	95.0	5757.2		6.0	13222.3		43.0	3707.4	7.0	10658.2
SOFTWIN BitDefender	701.0	780.2	4	8.0	9916.7		516.0	308.9	10.0	7460.7
Sophos Anti-Virus	64.0	8545.8		9.0	8814.9		36.0	4428.2	10.0	7460.7
Symantec NAV	152.0	3598.2		21.0	3777.8		87.0	1832.4	21.0	3552.7
Trend PC-cillin	67.0	8163.2		5.0	15866.8		51.0	3125.8	18.0	4144.9
VirusBuster VirusBuster	119.0	4596.1		9.0	8814.9		84.0	1897.8	14.0	5329.1

BitDefender had the dubious privilege of being one of the slowest of the scanners tested.

Sophos Anti-Virus 3.57

ItW Overall	100.00%	Macro	99.71%
ItW Overall (o/a)	100.00%	Standard	99.41%
ItW File	100.00%	Polymorphic	95.54%

Starting with the good news, the detection rates with which *Sophos Anti-Virus* has been blessed in the past are continuing to improve, the polymorphic set in particular showing improved detection in the trickier samples there. This, combined with the usual lack of false positives in the clean sets, resulted in a VB100% award for *Sophos Anti-Virus*.

On the irritating side, however, *SAV* has some of the least pleasant log files to deal with of those tested. Along with *Command AntiVirus* and the Hungarian version of *VirusBuster*, it converts file names in the logs to 8+3 format.

SAV also adds some compressed file details directly onto these file names. Not so relevant to testing, but unpleasant in the real world, the results for each sample in the test set also span several lines. In comparison with the ease of use of the rest of the product, these irritations are magnified.

Symantec Norton Anti-Virus Corporate 7.61.935

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.76%

Having gained a string of VB100% awards recently, *Norton Anti-Virus* remained true to form, putting in a perfect detection rate for In the Wild files. Across the remaining test sets the results were similarly good, with only one miss in the usually recalcitrant polymorphic test set.

Trend PC-cillin 2000 7.61

ItW Overall	99.95%	Macro	100.00%
ItW Overall (o/a)	99.95%	Standard	99.84%
ItW File	99.95%	Polymorphic	93.32%

Having pulled in two VB100% awards in as many reviews, *Trend* brought forward a promising record of success. Unfortunately, this run was brought to a halt by the less than perfect detection of W32/CTX.A. The polymorphics as a whole remained *PC-cillin*-resistant to more than a comfortable extent. This was notable in both newer and older polymorphics despite relatively recent claims that polymorphic detection was in the process of improvement. Perhaps future reviews will bring new heights of polymorphic detection to brighten *Trend*'s corporate visage.

VirusBuster VirusBuster 3.009-14

ItW Overall	99.95%	Macro	100.00%
ItW Overall (o/a)	99.95%	Standard	99.73%
ItW File	99.95%	Polymorphic	90.98%

VirusBuster scored good rates of detection across the board. Unfortunately one spectre loomed to haunt *VirusBuster*: W32/CTX. This was detected on occasion, but not infallibly so, and patchy detection of this virus denied *VirusBuster* a VB100%. With the differences in detection seen between the two versions of *VirusBuster* it is a mystery quite where the differences lie. It is to be hoped that it is simply a case of an antiquated version having been supplied by *Leprechaun*.

Logs, Logs and More Logs

With close to 50 logs to deal with in the space of this review, the quality or otherwise of those provided became quite a pressing concern. Each of these logs must be deciphered into a form which provides the basic information – a virus was or was not detected in file x. Unfortunately, in many cases the developers who have designed these log files have added extraneous information, contorted the information present or simply rendered it all but impossible to interpret.

A prime example is the degree to which packed files are explained in some log files. Consider the case of a *Powerpoint* file infected with a virus in one of its several OLE streams. In the log file this may simply be presented as the file being infected, though this does not present all the information available. Some log files include a detailed breakdown of the contents. In the best case this leads to additional entries describing the subcomponents, yet clearly labelling the file itself as infected. In many cases, however, the logs declare the infected file to be clean, before embarking on several descriptions of areas which are infected – despite these areas being within the 'clean' file. When parsing log files this results in a file which is infected being declared clean, in addition to the appearance of infected objects which are not in the test set – hardly ideal.

Much less forgiveable are those log files which use reporting methods which, although easily readable to the human eye, are obscure as far as machine parsing is concerned. Such log files are most commonly of the form where multiple lines are used to report one scanning event.

Next we reach those log files which alter the scanned file names or paths. Log files which change the case of scanned files or path descriptions are a prime example.

Exactly the same horror greets those products which transform file names into 8+3 format. The platform here was *Windows XP*, which does not use 8+3 format under any circumstance. Despite this, three of the products reviewed converted file names in their listings to this ancient format. Not only does this make log file parsing difficult, it also makes it impossible to determine exactly which files have been declared infected.

Conclusion

While the detection rates in the products reviewed were variable, the trend in detection rate is upwards, if not at an outstanding rate.

The problems encountered in this test were more of a practical nature than a lack of detection. However, if a product does not load reliably or cannot be cajoled into loading at all, it is of little use. Customers tend to be somewhat put off if a product sits on their machine unable to perform as advertised.

Technical Details

Test environment: Three 1.6 GHz Intel Pentium 4 workstations with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, all running *Windows XP Professional* Version 2002.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/WinXP/2002/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

ADDENDUM

Windows XP Professional Comparative Review

Matt Ham

Since the publication of the *Windows XP* comparative review in the June edition of *Virus Bulletin* (see *VB* June 2002, p.16), a number of the tests have continued in the interests of determining the cause of problems which arose during these tests. The following conclusions have been drawn.

Panda Antivirus Platinum

The review noted that *Panda Antivirus Platinum*'s on-access scanner did not function when tested. Clearly this was an issue about which the developers were concerned, and the tests were repeated at that time, gaining the same result.

However, more recent tests, using the same hardware and software, have not demonstrated these problems. The lack of functionality noted in the review cannot, therefore, be taken to be indicative of a reproducible problem with the software.

Discussions with other developers have confirmed that the type of problem described is not uncommon with *Windows XP*. One theory put forward is that, at boot-up, *XP* does not always load all operating system components in the same order. With anti-virus programs being interwoven with the OS to an extreme degree, this might be a cause of such oddities.

NAI VirusScan

Also noted in the review was the fact that the sample of W32/Gibe.A was missed In the Wild by *NAI VirusScan*. This proved to be the result of an update method which, despite updating virus definitions, did not fully update the underlying engine. While this was the update method provided by the vendor, the results are not indicative of those which would have been obtained had SuperDAT files been used rather than DAT files.

June 2002
100%
VIRUS BULLETIN
www.virusbtn.com

The test results as published in the June issue are correct for the older engine tested, however, it should be noted that when subsequent tests were performed using SuperDAT files as an upgrade method, no files were missed by *VirusScan* In the Wild. Therefore, with the current 4.1.60 engine the product would qualify for the VB 100% award.

ERRATUM

Windows XP Comparative Review: McAfee VirusScan

Unfortunately an error occurred in *Virus Bulletin*'s *Windows XP* comparative review (see *VB* June 2002, p.21): the results for *Network Associates' McAfee VirusScan* were replaced by those for *NAI VirusScan*. The correct results for *McAfee VirusScan* are reproduced in the table below.

The samples missed by *VirusScan* were mainly in the polymorphic set, where the offending items were Sepultura, W32/CTX and W32/Fosforo. The .TMP file dropped by W32/Nimda.A was undetected both in the *XP* review and in this month's *NetWare* tests. The file is included in the standard set as something of a curiosity file since, although it contains Nimda's code and is dropped by Nimda, this file is not a threat under any normal circumstances.

The results reported in the review for clean set scanning and false positives were correct. In light of the fact that no false positives were encountered and all In the Wild scans resulted in full detection, *McAfee VirusScan* is rightfully awarded a VB 100 % award for its performance. *VB* offers its apologies to *Network Associates* and to readers for the confusion.

McAfee VirusScan		On Demand	On Access
ITW File	number missed	0	0
	% detection	100.00%	100.00%
ITW Boot	number missed	0	0
	% detection	100.00%	100.00%
ITW Overall	number missed	0	0
	% detection	100.00%	100.00%
Macro Virus	number missed	0	0
	% detection	100.00%	100.00%
Polymorphic	number missed	8	8
	% detection	99.86%	99.86%
Standard	number missed	1	2
	% detection	99.98%	99.87%

NEWS

Addendum: June 2002 *Windows XP* Comparative Review

In the June 2002 comparative review of anti-virus products for *Windows XP* (see *VB*, June 2002, p.19), we stated that W32/Nimda.A samples were missed by *F-Prot 3.12* 'due to extension issues In the Wild on access.' The files in question were the EML files dropped by Nimda. *VB*'s documented testing procedure involves the opening/closing of tested files and, for practical reasons, does not include the execution of any malicious code. In the vast majority of cases such methods are sufficient to trigger a reaction from tested products. However, it has been drawn to our attention that the on-access protection implemented in *F-Prot* purposely ignores the opening of an EML file as a non-threat event (treating such a file as a container) – yet, if an infected EML message is accessed in the real world (an attempt made to execute its contents), the product *will detect and block* the execution of the malicious code. We have tested the claim and are happy to report that, although the product did not detect Nimda's EML files, *F-Prot* users relying on the on-access protection against W32/Nimda.A are safe ■