

virus

BULLETIN

EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS FEBRUARY – JUNE 2010

VIRUS BULLETIN VB100 TESTING

The basic requirements for a product to achieve VB100 certification status are that a product detects, both on demand and on access, in its default settings, all malware known to be 'In the Wild' at the time of the review, and generates no false positives when scanning a set of clean files.

Various other tests are also carried out as part of the comparative review process, including speed and overhead measurements and 'RAP' (Reactive and Proactive) tests.

The RAP tests measure products' detection rates across four distinct sets of malware samples. The first three of these comprise malware first seen in each of the three weeks prior to product submission and measure how quickly product developers and labs react to the steady flood of new malware. The fourth test set consists of malware samples first seen in the week after product submission. This test set is used to gauge products' ability to detect new and unknown samples proactively, using heuristic and generic techniques.

While the results of these secondary tests do not affect a product's qualification for VB100 certification, they are included to provide the reader with a better overall picture of product performance.

The testing methods of the VB100 certification process are provided in more detail at <http://www.virusbtn.com/vb100/about/100procedure.xml>



FEBRUARY 2010: NOVELL SUSE LINUX ENTERPRISE SERVER 11

Always among the market leaders in Europe, *SUSE* now stands as one of few likely challengers for *Red Hat* in the business sector. The task of preparing the test systems was a straightforward one. Few adjustments were required beyond pointing a few network shares to the right places and sharing the storage areas for the test sets ready for on-access testing. A client system, running *Windows XP SP3*, was set up with these shares mounted as network drives, with the standard set of scripts to run the on-access tests, and things were ready to go.







The latest additions to the WildList were reasonably unremarkable, with Koobface and OnlineGames variants continuing to dominate the list, and the old guard – the reams of Netsky and Mytob variants which once held sway over the list – continuing to decline. The most significant items on the list remain the complex W32/Virut strains, of which yet another new variant was added in recent months.

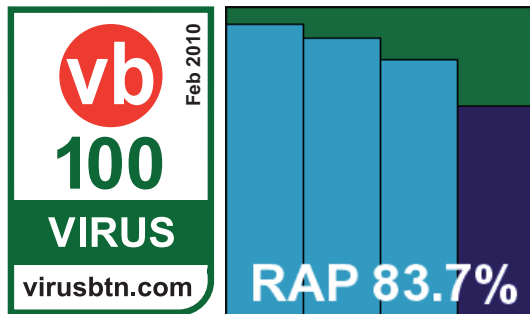
ESET Security for Linux 3.0.15

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.81%
Worms & bots	100.00%	False positives	0

ESET offers some nice simple install scripts – not as straightforward as some, but still fairly easy to operate. On-access scanning can be provided either using the *Dazuko* module, allowing full system protection, or on *Samba* shares



Reactive and Proactive (RAP) detection scores Feb 2010	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1		week +1	
Alwil avast! 	94.22%	90.30%	83.54%	89.35%	60.07%	82.03%
Avira AntiVir 	97.38%	95.60%	82.51%	91.83%	65.76%	85.31%
CA Threat Manager 	34.79%	35.10%	33.48%	34.46%	25.24%	32.15%
eScan	86.89%	82.04%	75.68%	81.54%	58.81%	75.86%
ESET Security 	94.25%	89.98%	82.76%	89.00%	67.81%	83.70%
Frisk F-PROT 	72.93%	74.11%	65.19%	70.74%	46.68%	64.73%
Quick Heal	88.42%	68.03%	61.43%	72.62%	53.99%	67.97%
Sophos Anti-Virus 	91.69%	86.57%	85.04%	87.77%	64.62%	81.98%
VirusBuster	85.69%	78.49%	68.81%	77.66%	44.77%	69.44%



only; for simplicity we opted to use this method, and again it proved simple to set up and configure.

On-demand scanning speeds were pretty reasonable, and on-access overheads not too heavy, despite some pretty intensive default scanning levels. Detection rates were quite excellent, with the only problem encountered in the RAP sets, where a couple of files caused the engine to trip up with a segmentation fault error message. With these moved out of the way, RAP scores proved just as impressive as those in the main sets, and the clean sets threw up only a few (fairly accurate) warnings of potentially unwanted adware-type products (mostly toolbars included ‘free’ with some of the trialware products added this month). With no full blown false positives, and the WildList handled with ease, ESET earns another VB100 award to add to its impressive haul.

APRIL 2010: WINDOWS XP SP3



















Despite its now venerable age, the XP platform remains the most popular operating system on the planet, with most estimates agreeing that it runs on more than 50% of all























computers worldwide. It is now, in a manner of speaking, a grandparent – succeeded by two newer generations of the Windows operating system – and is a full year into the ‘extended support’ phase, with the plug finally due to be pulled in four years. It seems likely that large numbers of users will stick by it for much of that time, thanks to the stability and simplicity of use for which it has acquired such a strong reputation.

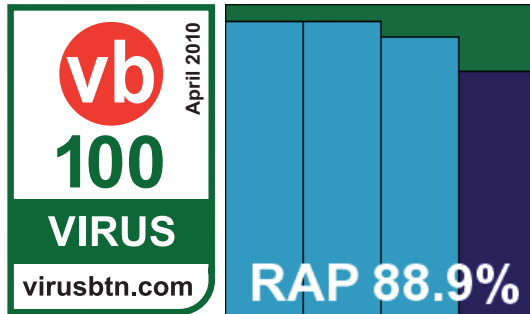
The WildList test set this time was aligned with the latest list available on the deadline of 20 February, which meant that the January list (released on 17 February) just made the cut. This list included the usual smattering of new samples, dominated by Autorun and Koobface worms and online gaming password stealers. What immediately stood out, however, was yet another strain of W32/Virut, which had appeared on the list since our last test. As always, large numbers of samples were replicated from the original control sample, each one checked to prove it capable of infecting other files, and the set was closed at a total of 2,500 Virut samples – which should be plenty to thoroughly exercise each product’s capabilities at detecting this complex polymorphic virus in all its disguises. Also of note this month was the return of an old complex polymorphic threat, W32/Polip, which first appeared in mid-2006 and has remained in our polymorphic sets for some time. Again, some 2,500 samples were moved to the WildList set to represent this threat.

ESET NOD32 Antivirus 4.2.35.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.55%
Worms & bots	99.55%	False positives	0

Reactive and Proactive (RAP) detection scores April 2010	Reactive			Reactive average	Proactive week +1	Overall average
	week -3	week -2	week -1			
Agnitum Outpost Security Suite Pro 	87.61%	75.41%	70.84%	77.95%	47.75%	70.40%
AhnLab V3 Internet Security 	68.25%	50.57%	36.40%	51.74%	21.65%	44.22%
Alwil avast! free antivirus 	96.55%	94.69%	89.78%	93.67%	52.72%	83.44%
Arcabit ArcaVir 2010	67.58%	57.78%	57.51%	60.96%	23.43%	51.58%
Authentium Command Anti-Malware	81.41%	75.54%	57.85%	71.60%	51.55%	66.59%
Avanquest Double Anti-Spy Professional	93.63%	91.68%	78.21%	87.84%	42.19%	76.43%
AVG Internet Security Network Edition 	93.55%	91.35%	81.26%	88.72%	49.28%	78.86%
Avira AntiVir Personal 	92.28%	96.19%	90.32%	92.93%	61.59%	85.10%
Avira AntiVir Professional 	92.28%	96.19%	90.32%	92.93%	61.59%	85.10%
BitDefender Antivirus 2010 	89.03%	70.53%	63.31%	74.29%	51.85%	68.68%
Bkis Bkav Gateway Scan	47.93%	43.70%	32.05%	41.23%	21.96%	36.41%
Bkis Bkav Home Edition	47.93%	43.70%	32.05%	41.23%	21.96%	36.41%
Bullguard Antivirus 	94.55%	86.08%	82.11%	87.58%	63.16%	81.47%
CA Internet Security Suite Plus 	67.23%	59.42%	64.28%	63.65%	53.20%	61.04%
CA Threat Manager 	68.69%	60.56%	65.78%	65.01%	55.35%	62.59%
Central Command Vexira Antivirus Professional 	88.47%	77.32%	71.10%	78.96%	48.28%	71.29%
Check Point Zone Alarm Suite	94.45%	95.52%	92.35%	94.11%	78.15%	90.12%
Defenx Security Suite 2010 	88.26%	77.26%	71.14%	78.89%	48.34%	71.25%
Digital Defender Antivirus 	87.42%	76.03%	69.06%	77.50%	47.64%	70.04%
eEye Digital Security Blink Professional	66.47%	57.84%	50.75%	58.35%	45.70%	55.19%
Emsisoft a-squared Anti-Malware	99.13%	99.42%	97.62%	98.72%	71.30%	91.87%
eScan Internet Security for Windows 	94.42%	85.75%	80.46%	86.88%	62.60%	80.81%
ESET NOD32 Antivirus 	94.08%	94.11%	89.18%	92.46%	78.04%	88.85%
Filseclab Twister Anti-TrojanVirus	82.74%	76.74%	67.69%	75.72%	67.66%	73.71%
Fortinet FortiClient	72.87%	69.75%	64.54%	69.05%	23.15%	57.58%
Frisk F-PROT	79.34%	72.52%	56.15%	69.34%	49.92%	64.48%
F-Secure Client Security 	91.22%	83.97%	66.53%	80.57%	55.26%	74.24%
F-Secure PSB Workstation Security 	91.22%	83.97%	66.53%	80.57%	55.26%	74.24%
G DATA Antivirus 2010 	99.09%	98.86%	91.14%	96.37%	65.25%	88.59%
Ikarus virus.utilities	98.93%	99.29%	94.64%	97.62%	68.42%	90.32%
iolo System Mechanic Professional	79.28%	72.47%	56.15%	69.30%	49.95%	64.46%

Reactive and Proactive (RAP) detection scores April 2010 contd.	Reactive			Reactive average	Proactive week +1	Overall average
	week -3	week -2	week -1			
K7 Total Security 	90.85%	85.44%	58.94%	78.41%	50.14%	71.34%
Kaspersky Anti-Virus 2010 	93.55%	96.03%	93.23%	94.27%	77.36%	90.04%
Kaspersky Anti-Virus 6 for Windows Workstations	93.24%	95.79%	92.38%	93.80%	76.47%	89.47%
Kingsoft Internet Security 2010 Advanced Edition 	32.16%	24.31%	21.93%	26.13%	17.61%	24.00%
Kingsoft Internet Security 2010 Standard Edition 	37.64%	36.53%	26.45%	33.54%	21.88%	30.63%
Kingsoft Internet Security 2010 Swinstar Edition	42.62%	38.34%	28.81%	36.59%	22.34%	33.03%
Lavasoft Ad-Aware Professional Internet Security	96.96%	96.35%	82.57%	91.96%	62.12%	84.50%
McAfee Total Protection 	94.64%	92.87%	84.84%	90.78%	66.01%	84.59%
McAfee VirusScan Enterprise 	90.83%	89.17%	82.72%	87.57%	63.61%	81.58%
Microsoft Security Essentials	91.14%	93.06%	74.15%	86.12%	55.52%	78.47%
Nifty Corp. Security 24	93.45%	94.31%	85.59%	91.12%	62.36%	83.93%
Norman Security Suite	66.36%	57.81%	50.30%	58.16%	45.75%	55.06%
PC Tools Internet Security 2010 	93.21%	92.55%	76.19%	87.32%	34.49%	74.11%
PC Tools Spyware Doctor 	93.22%	92.58%	76.20%	87.34%	34.53%	74.13%
Preventon AntiVirus 	87.42%	76.03%	69.06%	77.50%	47.64%	70.04%
Proland Protector Plus Professional 	87.71%	76.26%	70.82%	78.26%	48.13%	70.73%
Qihoo 360 Security 	93.88%	84.32%	73.68%	83.96%	56.51%	77.10%
Quick Heal AntiVirus 2010 	78.68%	69.61%	63.17%	70.49%	44.58%	64.01%
Rising Internet Security 2010 	59.40%	42.67%	34.77%	45.62%	25.07%	40.48%
SGA Corp. SGA-VC 	94.36%	85.88%	79.65%	86.63%	62.08%	80.49%
Sophos Endpoint Security and Control 	95.90%	93.43%	90.74%	93.36%	75.43%	88.88%
SPAMfighter VIRUSfighter Plus 	87.43%	76.03%	69.06%	77.51%	47.59%	70.03%
SPAMfighter VIRUSfighter Pro 	87.25%	75.84%	68.98%	77.36%	47.61%	69.92%
Sunbelt VIPRE AntiVirus Premium	96.97%	96.45%	83.53%	92.31%	66.10%	85.76%
Symantec Endpoint Protection 	91.37%	90.35%	65.00%	82.24%	31.15%	69.47%
Symantec Norton Antivirus 	91.77%	90.76%	66.49%	83.00%	33.24%	70.56%
Trustport Antivirus 2010 	98.67%	96.09%	96.74%	97.17%	79.66%	92.79%
VirusBuster Professional 	88.47%	77.32%	71.10%	78.96%	48.28%	71.29%
Webroot AntiVirus with SpySweeper 	96.48%	94.12%	89.90%	93.50%	74.40%	88.72%



ESET is a VB100 stalwart, with an unrivalled record of clean sheets. The product is provided as a pre-updated executable of just 37MB, and the installation process remains pretty much unchanged from many previous experiences. With just a handful of stages to get through, including the unusual step of forcing the user to make a choice on whether to detect 'potentially unwanted' software or not (presumably allowing the product greater freedom to detect certain types of nasty without threat of reprisals), the process is all done within less than a minute and a half, with no need to reboot.

The interface and configuration screens are as solid, slick and stylish as ever, and everything has an air of quality about it. The only issue we observed was a lack of clarity in the more advanced and unusual on-access controls, where what seemed to be options to allow archives to be scanned appeared not to function as intended – but this could have been a misunderstanding on our part of the purpose of the controls in question.

Running through the tests in short order, scanning speeds were solid and dependable, while on-access lag times were excellent, with RAM and CPU usage both at the lower end of the scale.

In the infected sets detection rates were splendid, with another excellent showing in the RAP sets, and with yet another test untroubled by WildList misses or false alarms, *ESET* further extends its remarkable unbroken run of VB100 awards.

JUNE 2010: WINDOWS SERVER 2008 R2

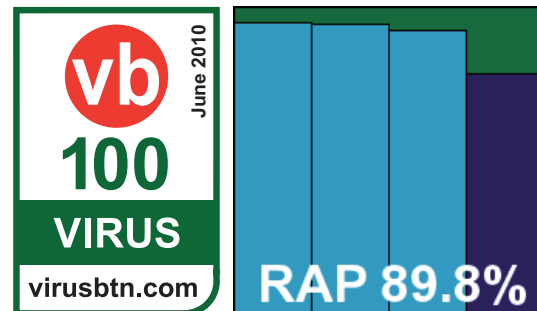
Microsoft's latest upgrade to its server solution is presented as a simple refresh of the 2008 version, but in fact is a much bigger deal, essentially being *Windows 7 Server*. The new platform is considerably revised and updated, and is available only for 64-bit hardware.

The core WildList test set saw a sprinkling of new additions, with an early deadline meaning we just missed the release of the March list; the sets were instead aligned with the February list, which included the same W32/Virut strain that caused some upsets last time around, as well as the venerable W32/Polip which was generally handled more solidly. New additions followed the trend of recent months, dominated by W32/Koobface worms with little else of particular novelty or interest.

























The other core part of the certification set, the clean sample set, saw some considerable expansion, with the usual addition of the most popular items from various freeware sites supplemented with swathes of more serious software packages from *Microsoft*, *Sun* and others as a nod to the server setting of this month's test.

ESET NOD32 Antivirus 4.2.40.0

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	96.73%
Worms & bots	99.15%	False positives	0



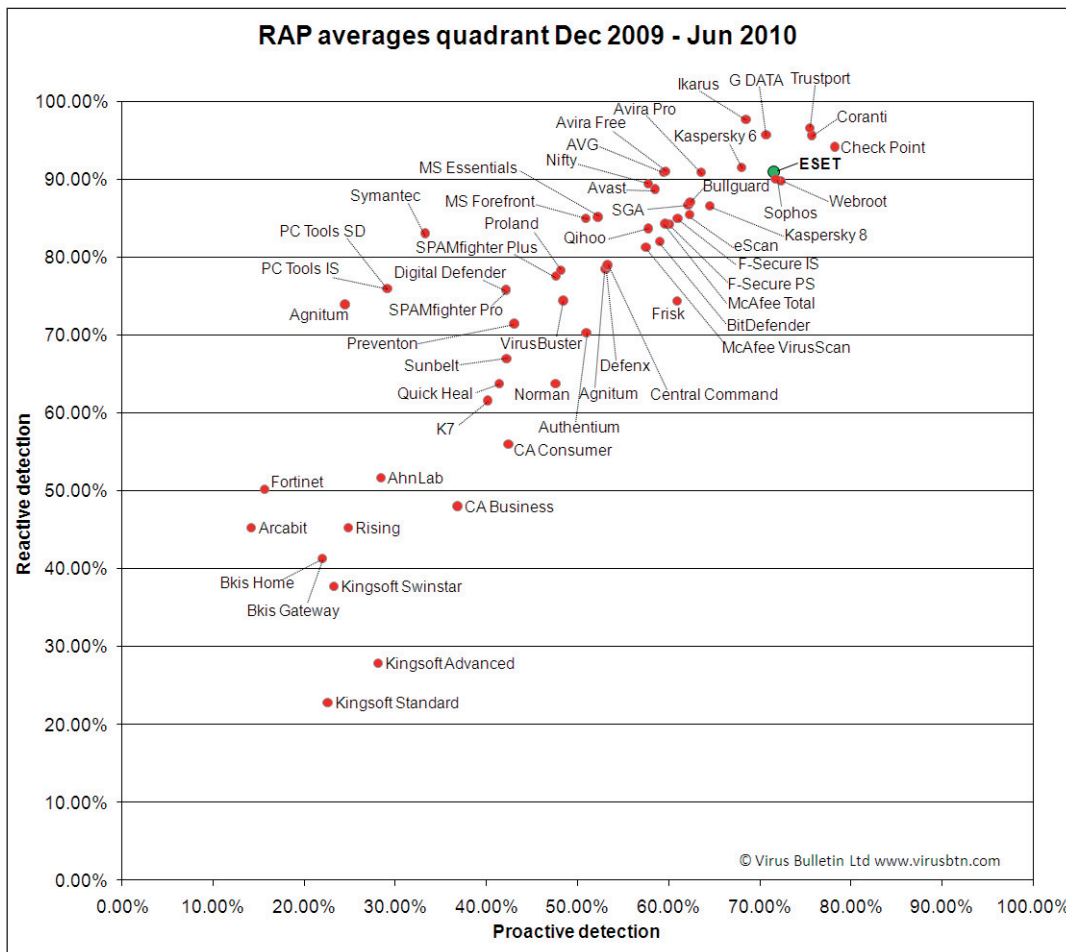
Little has changed about *ESET's* *NOD32* for some time, only a few adjustments having been made since a major redesign a few years ago. It remains attractive to look at as well as easy to use. The installation process is fairly standard – enlivened only by the unusual feature of requiring the user to make a choice as to whether or not to detect greyware items – and does not require a reboot to complete. The interface is clear and detailed, with an excellent selection of configuration options, some of which are a little repetitive in places but generally logically and clearly laid out. During testing the interface appeared to freeze up a few times when asked to do more work while under heavy stress, but it soon recovered its composure and continued to get on with the job under the hood.

Reactive and Proactive (RAP) detection scores June 2010	Reactive			Reactive average	Proactive week +1	Overall average
	week -3	week -2	week -1			
Agnitum Outpost 	84.65%	73.41%	78.90%	78.99%	58.27%	73.81%
AhnLab V3Net 	57.37%	41.27%	52.15%	50.26%	42.38%	48.29%
avast! Server 	88.63%	89.67%	85.84%	88.05%	67.32%	82.87%
AVG I.S. Network Edition 	98.28%	98.73%	96.56%	97.86%	75.07%	92.16%
Avira AntiVir Windows Server 	93.39%	89.01%	85.83%	89.41%	69.11%	84.33%
BitDefender Security 	87.59%	83.66%	84.62%	85.29%	64.16%	80.01%
Bkis BKAV Gateway Scan	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Gateway Scan Plus	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Home Edition	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Home Edition Plus	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Central Command Vexira 	84.52%	73.39%	78.88%	78.93%	58.17%	73.74%
Coranti Multicore 	99.18%	93.69%	93.94%	95.60%	75.64%	90.61%
Defenx Security Suite 	84.37%	73.16%	78.58%	78.70%	57.96%	73.52%
Digital Defender	81.68%	71.88%	68.88%	74.15%	36.53%	64.74%
eEye Blink Server	65.46%	65.87%	63.97%	65.10%	49.72%	61.25%
eScan I.S. Suite 	87.49%	83.65%	84.40%	85.18%	63.94%	79.87%
ESET NOD32 Antivirus 	94.51%	94.42%	92.02%	93.65%	78.14%	89.77%
Fortinet FortiClient 	64.39%	59.97%	34.00%	52.78%	19.41%	44.44%
Frisk F-PROT	84.77%	76.78%	79.50%	80.35%	65.87%	76.73%
F-Secure AntiVirus 	91.21%	85.83%	82.62%	86.55%	64.07%	80.93%
G DATA AntiVirus 	99.31%	99.28%	95.63%	98.07%	77.62%	92.96%
Kaspersky Anti-Virus 6 	91.93%	90.06%	90.06%	90.68%	69.99%	85.51%
Kaspersky Anti-Virus 8 	85.59%	65.42%	73.47%	74.83%	54.24%	69.68%
Kingsoft 2011 Advanced 	25.42%	12.46%	22.10%	19.99%	34.03%	23.50%
Kingsoft 2011 Standard 	22.01%	10.36%	20.03%	17.46%	31.53%	20.98%
McAfee VirusScan 	87.83%	81.72%	77.48%	82.34%	57.15%	76.05%
Norman Endpoint Protection	65.52%	65.79%	63.91%	65.07%	49.64%	61.21%
Quick Heal AntiVirus 	56.03%	43.07%	43.93%	47.67%	30.61%	43.41%
Rising I.S. 	52.90%	45.67%	35.77%	44.78%	24.45%	39.70%
Sophos Endpoint 	93.94%	91.47%	90.14%	91.85%	73.53%	87.27%
SPAMfighter VIRUSfighter	81.72%	71.90%	68.84%	74.15%	36.61%	64.77%
Trustport AntiVirus 2010 	99.64%	99.58%	98.30%	99.17%	79.10%	94.16%
VirusBuster 	84.52%	73.39%	78.88%	78.93%	58.17%	73.74%

Scanning speeds were medium, with on-access lags and CPU usage also in the middle of the field; memory usage was fairly low, however. Detections rates were excellent, showing a continuation of the upward trend seen in the last few tests. A couple of items in the clean set were alerted on as potentially unwanted – a fairly accurate description of toolbars and other functions bundled with popular freeware packages – but no false alarms were noted and the WildList was handled flawlessly, earning ESET yet another VB100 award.



ESET, 610 West Ash St, Suite 1900,
San Diego, CA 92101, USA
Tel: +1 619 876 5400, Fax: +1 619 437 7045
Email: sales@eset.com, Web: http://www.eset.com/.



The cumulative RAP quadrant gives a quick visual reference as to products' reactive and proactive detection rates over the last four tests.