COMPARATIVE REVIEW

VB100 COMPARATIVE REVIEW ON UBUNTU LINUX 10.04 LTS

John Hawes

2010 saw some setting – and breaking – of records in the *VB* test lab, with several tests proving to be of truly epic proportions. 2011 promises no let up in the steady onslaught of new solutions participating in our tests, and in the coming months we hope to see more of the diversity and innovation spotted in some of 2010's products. We also hope to see less of the fragility, instability, lack of clarity and general bad design we saw in many others.

For now, however, we leave the cluttered *Windows* space behind to make our annual probe into the murkier, less cuddly but generally more robust world of *Linux*. In a market space that is much less crowded with small-time niche players, our *Linux* tests tend to be less over-subscribed than many others, and generally feature only the most committed, comprehensive security providers (most of whom make up our hardest core of regular entrants). For only the second time, we decided to run the test on the explosively popular *Ubuntu* distribution, which was first seen on the VB100 test bench almost three years ago (see *VB*, June 2008, p.16).

Despite being later than usual, the product submission deadline of 5 January caused problems for developers in some regions thanks to varying holiday times. For at least a couple of major vendors there was no submission this month, either due to lack of support for the platform chosen or due to a lack of resources to prepare a submission so close to the New Year. Other vendors chose to skip this month's test for other reasons. Nevertheless, a strong field of 14 entrants arrived on deadline day, covering the bulk of our regulars.

PLATFORM AND TEST SETS

Having last looked at *Ubuntu* version 8.04 a few years ago, we expected a few improvements in the current Long Term Support version 10.04, released in mid-2010. However, the installation process showed little sign of such improvement, with a fairly rudimentary command-line-driven set-up system, which nevertheless did the job adequately. The most fiddly part was the software selection system, which seemed far from intuitive, but fortunately we required little beyond the basics of a fileserver, intending to add in any additional dependencies on a per-product basis. Once the vagaries of the interface had been conquered, the actual work of installing was rapid and relatively undemanding, and with the system up and running, standard controls enabled implementation of all the settings we required in short order.

As in the previous test on this platform, the installer provided no graphical desktop by default, which seems a sensible approach for a server platform; graphical interfaces are generally unnecessary in the day-to-day running of services, and can be both a performance drain and a security risk. It seems likely that many if not most machines running the platform under test would operate like this, and indeed even in a setting as small as the *VB* test lab we run a number of *Linux* machines with no windowing system, including some with older versions of *Ubuntu*. Nevertheless, some of the vendors taking part indicated that their solutions were geared towards graphical operation, so we had to hope that traditional command-line methods would also be supported.

The main issue we expected to see was with on-access scanning, which is always slightly fiddly on *Linux*. In the past there have been three main approaches: protecting *Samba* shares only, using *Samba* vfs objects, which usually entails little more than an added line or two in the *Samba* configuration file; the open-source *dazuko* system, which allows more granular control of protection over different areas of the system; and proprietary methods, which can vary greatly from provider to provider. *Dazuko* has been somewhat awkward to set up in the past, involving compilation from sources and often with special flags required depending on the platform, but in some quick trials this month there were no problems in getting it up and running. A new and improved version, *dazukofs*, is also available and looked likely to be used by some products.

Building this month's test sets proved something of a challenge however, after some problems with hardware, software and the human factor set things back several weeks. The imposed delays allowed time to integrate several new malware feeds into our collection processes, which added considerably to the number of samples included in the raw sets. With time pressing, test sets were built with minimal initial filtering – the verification and classification process continued while the tests were run. These issues having eaten heavily into our already shortened month, and well aware that the large test set sizes would mean longer test times for all, we were in some hurry to get things moving.

Fortunately, little work was required in building the core certification sets. The latest WildList available on the deadline date (the November list, released in late December) featured mainly standard worms and online gaming password-stealers, and none of the major new file infectors of the sort that have been causing problems

On-demand tests	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Avast	0	100.00%	703	98.74%	10	99.42%	4339	97.44%	0	0
AVG	0	100.00%	1745	96.87%	50	97.93%	5788	96.58%	0	0
Avira	0	100.00%	102	99.82%	0	100.00%	733	99.57%	0	0
BitDefender	0	100.00%	120	99.78%	0	100.00%	1660	99.02%	0	0
Central Command	0	100.00%	2401	95.69%	187	90.52%	28019	83.45%	0	1
eScan	0	100.00%	2184	96.08%	0	100.00%	3817	97.75%	0	0
ESET	0	100.00%	768	98.62%	0	100.00%	9848	94.18%	0	4
Frisk	0	100.00%	6744	87.89%	0	100.00%	33450	80.24%	0	0
Kaspersky AV	0	100.00%	6035	89.17%	0	100.00%	11804	93.03%	1	0
Kaspersky ES	0	100.00%	6035	89.17%	0	100.00%	8002	95.27%	1	0
Norman	0	100.00%	7452	86.62%	281	85.29%	31725	81.26%	0	1
Quick Heal	0	100.00%	1748	96.86%	42	96.94%	7505	95.57%	0	0
Sophos	0	100.00%	1810	96.75%	0	100.00%	10213	93.97%	0	0
VirusBuster	0	100.00%	2401	95.69%	187	90.52%	28019	83.45%	0	1

(*Please refer to text for full product names*)

for many products of late. As replication of these in large numbers takes considerably longer than verification of less complex items, the set was compiled quickly. With several older file infectors removed from the list it shrank to a little over 5,000 samples, the bulk of which were from two remaining file infectors, a single strain of W32/Virut and the venerable W32/Polip.

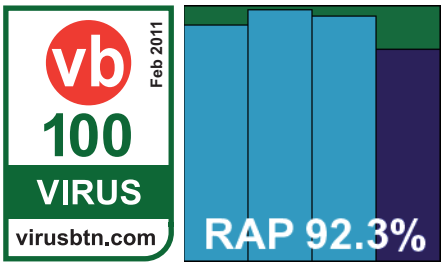
The clean set was expanded with the usual batch of new items, focusing mainly on business-related tools this month to reflect the typical user base of the platform. The speed sets were augmented as usual by a selection of *Linux* files, this time taken from the core directories of one of our standard server systems. Some doctoring of our test automation processes was required to fit with the different platform – the on-access tests and performance measures were all run from a *Windows XP Professional SP3* client system, to emulate normal usage for a *Samba* file server protecting a network of *Windows* machines. To ensure fairness, speed tests were run one at a time with other network activity kept to a minimum.

With everything set up, all that remained was to get to grips with the solutions themselves. From past experience, we expected to see some nice, simple designs in between more challenging approaches, with ease of use depending greatly on the clarity of documentation as well as use of standard *Linux* practice.

Avast Software avast! for Linux 3.2.1

Version VPS 110105-1

ItW	100.00%	**Polymorphic**	99.42%
ItW (o/a)	100.00%	**Trojans**	97.44%
Worms & bots	98.74%	**False positives**	0



Avast started things off nicely, with a compact 37MB install bundle in tar.gz format, containing three .DEB packages. Instructions were short and simple, running through the steps of installing the .DEBs, making a few tweaks to the system and getting the *dazuko* modules compiled and installed. With concise and comprehensive advice, it took only a minute or two to get everything set up just as we wanted.

With ample man pages and all the required executables easy to find, setting up and automating the full test suite was a simple process, and running through it was as rapid

On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Avast	0	100.00%	661	98.81%	10	99.42%	3614	97.87%
AVG	0	100.00%	1641	97.05%	50	97.93%	6415	96.21%
Avira	0	100.00%	102	99.82%	0	100.00%	731	99.57%
BitDefender	0	100.00%	120	99.78%	0	100.00%	1660	99.02%
Central Command	0	100.00%	3082	94.47%	187	90.52%	29346	82.67%
eScan	1	99.85%	121	99.78%	0	100.00%	1680	99.01%
ESET	0	100.00%	625	98.88%	0	100.00%	9692	94.28%
Frisk	0	100.00%	6742	87.90%	0	100.00%	33436	80.25%
Kaspersky AV	0	100.00%	6101	89.05%	0	100.00%	13029	92.30%
Kaspersky ES	0	100.00%	6101	89.05%	0	100.00%	9232	94.55%
Norman	0	100.00%	7872	85.87%	324	84.49%	37191	78.03%
Quick Heal	0	100.00%	7033	87.37%	42	96.94%	22996	86.42%
Sophos	0	100.00%	1810	96.75%	0	100.00%	10211	93.97%
VirusBuster	0	100.00%	3082	94.47%	187	90.52%	29346	82.67%

(*Please refer to text for full product names*)

as usual. Scanning speeds on demand were pretty decent, with on-access overheads perhaps somewhat higher than expected, but still pretty decent.

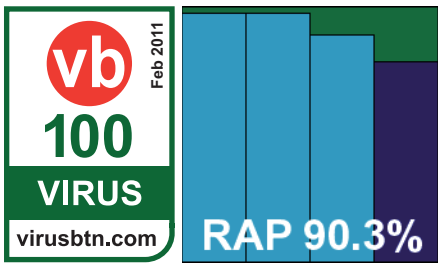
On checking the results we found solid scores in all sets, as expected, but in the RAP sets there was a bit of a surprise in that scores for the last few weeks were completely absent. We re-ran the tests keeping a close eye on the console output, and quickly diagnosed that the scanner had crashed on a malformed sample in the extended set, with a segmentation fault error. The test was repeated, skipping the offending section of the set. No further problems emerged, and even with this doubling of effort the hugely impressive speed of scanning infected files meant that all tests were completed in well under 24 hours. The core sets were handled effortlessly, and *Avast* notches up another successful VB100 pass.

AVG 8.5.863

Virus database version 271.1.1/3356; Scanner version 8.5.850

ItW	100.00%	**Polymorphic**	97.93%
ItW (o/a)	100.00%	**Trojans**	96.58%
Worms & bots	96.87%	**False positives**	0

AVG's *Linux* solution is a little more bulky, arriving as a 93MB .DEB package along with a licence key to activate it. The set-up process was simple enough to start with, but once the package was installed considerably more work was required to decrypt a rather fiddly configuration system. This involved passing configuration changes into the product as long and easily mistyped strings, rather than making changes to human-readable and self-explanatory configuration files, as is generally the case for *Linux* software. The layout, with multiple binaries with overlapping and bewildering names and functions, was also less than helpful, and man pages proved pretty eye-watering too, but in the end we got things working just well enough to get through the tests. The product has options to provide on-access protection through several methods, but we opted for the *dazuko* approach as the most simple to operate.

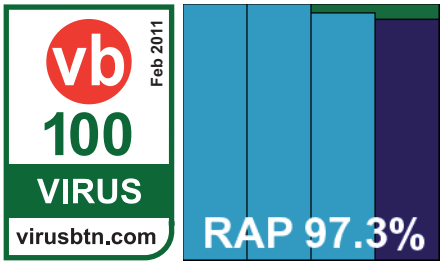


Once the configuration had been adjusted to our needs and the syntax of the scanner tool figured out, running the tests was much less of a headache. Speeds and overheads were good, and detection rates splendid, and with no issues in the core sets, *AVG* comfortably earns a VB100 award.

Avira AntiVir Server 3.1.3.4

SAVAPI-Version 3.1.1.8; AVE-Version 8.2.4.136; VDF-Version 7.11.1.20 created 20110104

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.57%
Worms & bots	99.82%	**False positives**	0



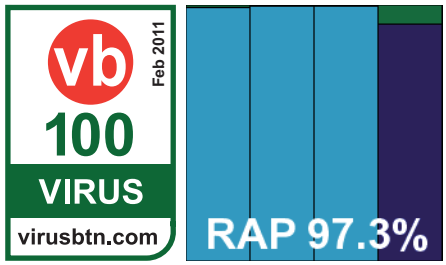
Avira's *Linux* server solution was provided as a 55MB tar.gz archive bundle, along with an extra 37MB of updates. Inside the main bundle was a folder structure containing an install script, which ran through the set-up process clearly and simply, including compilation and insertion of *dazuko*. Some additional options included a GUI for the *Gnome* desktop and a centralized management system, and the installation even informs you where the main control binaries are located, to avoid the scrabbling around often experienced with less helpful products. Despite its clarity and simplicity, the set-up still ends by urging the user to read the product manual for more detailed information.

After this exemplary install, using the product proved similarly unfussy and user-friendly, adhering to standard *Linux* practices and thus making all the required controls both easy to locate and simple to operate. Documentation was also clear and comprehensive. Speeds were super-fast and super-light, and detection rates were as excellent as ever. With no problems in the core sets, *Avira* easily earns another VB100 award.

BitDefender Security for Samba File Servers 3.1.2

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.02%
Worms & bots	99.78%	**False positives**	0

BitDefender's product was a little different from most, with its 100MB submission provided as a .RUN file. When run as the filename suggested, this installed the packages and set things up as required. Part of the set-up involved compiling components (the *Samba* vfs object code required for the on-access component), and several other dependencies also had to be met prior to installation, but it was not too much effort and completed in reasonable time. Once again, configuration was geared towards complexity rather than user-friendliness, with lengthy and fiddly commands required to bring about any change in settings, but it wasn't too horrible once the esoteric formulae for generating adjustments had been worked out.

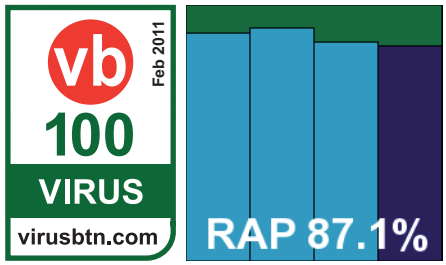


Running through the tests proved smooth and stable, although both on-demand speeds and on-access overheads were somewhat heavier than might be expected, but detection rates were impeccable and the core sets were stomped through without a problem, earning *BitDefender* a VB100 award.

Central Command Vexira Professional 6.3.14

Virus database version: 13.6.130.0

ItW	100.00%	**Polymorphic**	90.52%
ItW (o/a)	100.00%	**Trojans**	83.45%
Worms & bots	95.69%	**False positives**	0



Central Command has recently become a fixture in our comparatives, with a run of successes under its belt. This month the product was presented as a pair of .tgz archive files, the main product measuring 57MB and the additional update bundle 65MB. Unpacking the main bundle revealed a handful of .DEB files and a Perl install script. This ran through tidily, getting everything set up in good order. Some additional instructions were kindly provided by the developers with details of updating and adjusting settings. A secondary set-up script was also provided to change the settings of the *Samba* configuration, enabling on-access protection.

With everything set up, testing proved a breeze, although configuration of the on-access scanner was somewhat limited – at least as far as could be judged from the sparse documentation. Nevertheless, the default settings did well and it tripped along at a good pace. Scanning speeds were not bad and overheads were light, with the usual fairly

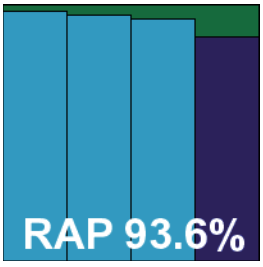
File access lag time (ms/MB)	Archive files			Binaries and system files			Linux files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Avast	155.43	155.46	155.43	49.52	49.18	49.52	310.49	308.17	310.49	67.36	65.38	67.36	86.67	83.72	86.67
AVG	12.13	11.75	NA	59.15	55.16	59.15	192.13	187.39	N/A	81.22	80.00	81.22	120.37	119.40	120.37
Avira	167.00	167.24	167.00	16.95	16.84	16.95	321.63	319.64	321.63	43.40	42.53	43.40	50.70	50.33	50.70
BitDefender	151.74	156.44	151.74	76.32	76.48	76.32	472.01	460.62	472.01	250.86	242.79	250.86	347.71	332.40	347.71
Central Command	6.94	6.90	NA	66.29	66.10	66.29	206.52	193.82	N/A	79.61	81.96	79.61	118.44	123.73	118.44
eScan	83.70	85.69	83.70	71.38	72.19	71.38	331.35	332.32	331.35	157.08	156.59	157.08	221.05	219.22	221.05
ESET	147.96	147.52	147.96	19.04	18.53	19.04	254.44	248.98	254.44	70.62	70.01	70.62	64.86	70.98	64.86
Frisk	87.05	87.28	87.05	67.08	67.54	67.08	195.47	181.07	195.47	39.61	38.17	39.61	67.52	63.28	67.52
Kaspersky AV	16.41	16.13	651.69	63.16	62.33	344.87	225.92	223.42	956.09	97.71	96.71	385.47	137.51	135.78	429.85
Kaspersky ES	17.04	16.98	517.11	47.48	48.19	200.70	195.81	192.98	777.46	79.86	77.22	227.50	100.52	96.36	248.56
Norman	9.42	0.00	N/A	93.48	0.00	93.48	413.01	0.00	N/A	303.73	0.00	303.73	402.69	0.00	402.69
Quick Heal	7.59	7.35	NA	61.77	61.24	61.77	409.14	405.03	N/A	273.07	267.20	273.07	224.01	227.45	224.01
Sophos	10.03	9.77	843.06	55.80	55.54	232.25	161.81	150.75	1295.57	46.16	45.54	215.38	101.38	100.11	279.55
VirusBuster	5.12	4.69	NA	49.44	48.79	49.44	195.23	189.73	N/A	55.93	59.70	55.93	88.68	87.09	88.68

(*Please refer to text for full product names*)

decent level of detections. With no problems in the clean set or WildList set *Central Command* earns another VB100 award for its growing collection.

eScan for Linux File Servers 5.0-2

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	99.85%	**Trojans**	97.75%
Worms & bots	96.08%	**False positives**	0



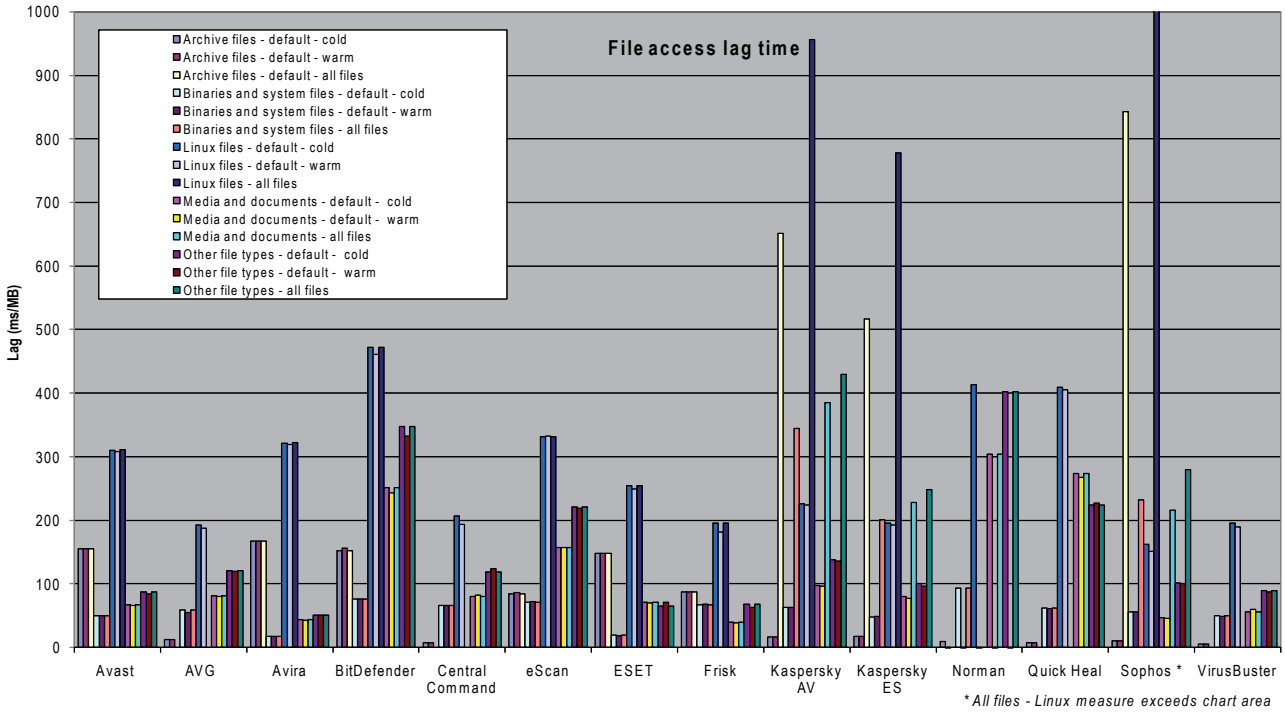
The *Linux* version of *eScan* comes as a handful of .DEB packages, installation of which required resolving a few dependencies, including for one package several components of the X desktop system – clearly this was one of those products leaning towards graphical rather than command-line usage. This was not a problem, as despite there being no evidence of configuration for some aspects (notably the on-access protection) at the local console level, it was easily accessible through a browser-based web administration tool. Checking this out from another machine, we found it fairly clear, but in places a little prone to flakiness – resetting our changes on a number of occasions as soon as 'apply' was clicked. Local console documentation also seemed a little sparse, but we soon figured things out and got the test moving along.

Speeds held up well against the rest of the field, and detection was solid. All looked to be going swimmingly until a single item went undetected in the WildList set on access – with a default setting to ignore files larger than 13MB (a reasonably sensible level), *eScan* was extremely unlucky in that this month's WildList contained a larger sample than this (25MB). This bad luck denies *eScan* a VB100 award this month, despite a generally decent performance.

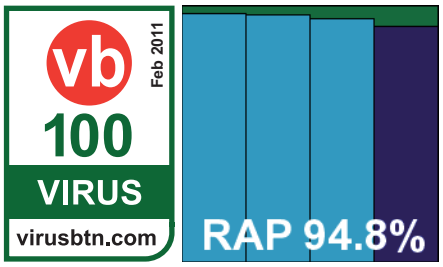
ESET File Security 3.0.20

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.18%
Worms & bots	98.62%	**False positives**	0

ESET's *Linux* edition was provided as a single 41MB .DEB package, and installed easily with minimal fuss. Clear instructions showed how to set up protection of *Samba* shares using a vfs object (*dazuko*-style protection was also



available), and the commands and configuration were properly laid out, conforming to expected norms.



Running the test was fairly painless, although a couple of files in our extended sample sets did cause segmentation faults and required the restarting of scans. Speeds were pretty zippy and overheads nice and light, particularly in the binaries section. Detection rates were solid across the sets. The clean set threw up a few warnings of potentially unwanted items (most identified precisely and accurately) and a couple of packer warnings, but nothing could stop *ESET*'s inexorable progress towards yet another VB100 award.

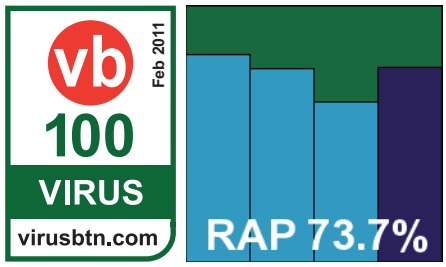
Frisk F-PROT Antivirus for Linux File Servers 6.3.3.5015

Engine version: 4.5.1.85; virus signatures 201101040744

6e8837db11f3f34f0bfe050aa91a01a9

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	80.24%
Worms & bots	87.89%	**False positives**	0

Frisk's *Linux* product came as a 24MB .tgz archive, with an accompanying 26MB of updates and a small patch file.



Installation was basic and rudimentary, with a little install script creating symlinks to the main components without moving them from where they had originally been unpacked – a nice, unobtrusive approach as long as it is expected.

Getting things up and running proved a breeze, with both *dazuko* and *Samba* vfs objects supported (*dazuko* was used for all our on-access tests), and configuration and operation were made easy thanks to the product's conformance with the expected behaviour for *Linux* solutions.

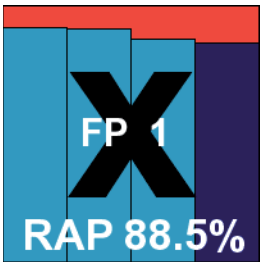
With good scanning speeds and no stability problems, tests were completed in excellent time. Detection scores were decent, with a dip in the later parts of the RAP sets but a strong resurgence in the proactive week. No problems were noted in either of the core certification sets and a VB100 award is duly earned by *Frisk*.

On-demand throughput (MB/s)	Archive files			Binaries and system files			Linux files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Avast	6.19	6.28	6.18	18.21	18.45	16.25	3.76	4.08	3.17	8.99	9.21	10.07	6.48	6.56	7.07
AVG	15.38	15.46	1.47	28.07	25.66	16.08	3.38	3.49	1.13	21.63	21.66	8.97	14.14	14.24	6.34
Avira	6.25	6.26	6.25	55.83	57.28	55.83	2.80	2.99	2.80	22.25	23.34	22.25	19.87	20.81	19.87
BitDefender	6.50	6.49	6.50	16.34	16.64	16.34	2.59	2.65	2.59	6.68	6.91	6.68	4.79	4.99	4.79
Central Command	7.20	7.21	4.39	15.13	15.39	15.43	7.05	6.62	2.04	6.32	6.34	5.76	4.75	4.81	4.57
eScan	6.14	6.16	6.14	17.91	18.11	17.91	3.40	3.40	3.40	14.46	14.57	14.46	10.25	10.02	10.25
ESET	6.55	6.62	6.55	23.30	23.68	23.30	3.69	4.03	3.69	11.62	11.40	11.62	9.26	9.41	9.26
Frisk	9.94	9.89	9.77	14.56	14.88	14.49	4.47	4.88	4.68	23.03	27.64	25.17	12.51	15.03	13.24
Kaspersky AV	2.65	2.71	2.65	21.90	21.99	21.90	1.52	1.54	1.52	12.75	13.07	12.75	10.17	10.50	10.17
Kaspersky ES	2.69	2.70	2.69	20.04	20.11	20.04	1.59	1.60	1.59	12.86	13.21	12.86	10.42	10.61	10.42
Norman	1.19	1.18	1.19	4.08	4.00	4.08	1.37	1.36	1.37	4.88	4.85	4.88	3.10	3.07	3.10
Quick Heal	2.56	2.55	2.56	24.57	24.63	24.57	1.50	1.50	1.50	6.78	6.81	6.78	8.04	8.07	8.04
Sophos	86.83	93.77	1.11	14.76	16.76	10.88	19.81	29.77	0.71	18.06	19.08	13.88	9.36	10.11	7.34
VirusBuster	7.24	7.30	4.45	19.68	19.78	19.75	6.62	6.45	2.01	6.25	6.31	5.77	4.80	4.83	4.59

(*Please refer to text for full product names*)

Kaspersky Anti-Virus for Linux File Servers 8.0.0.136

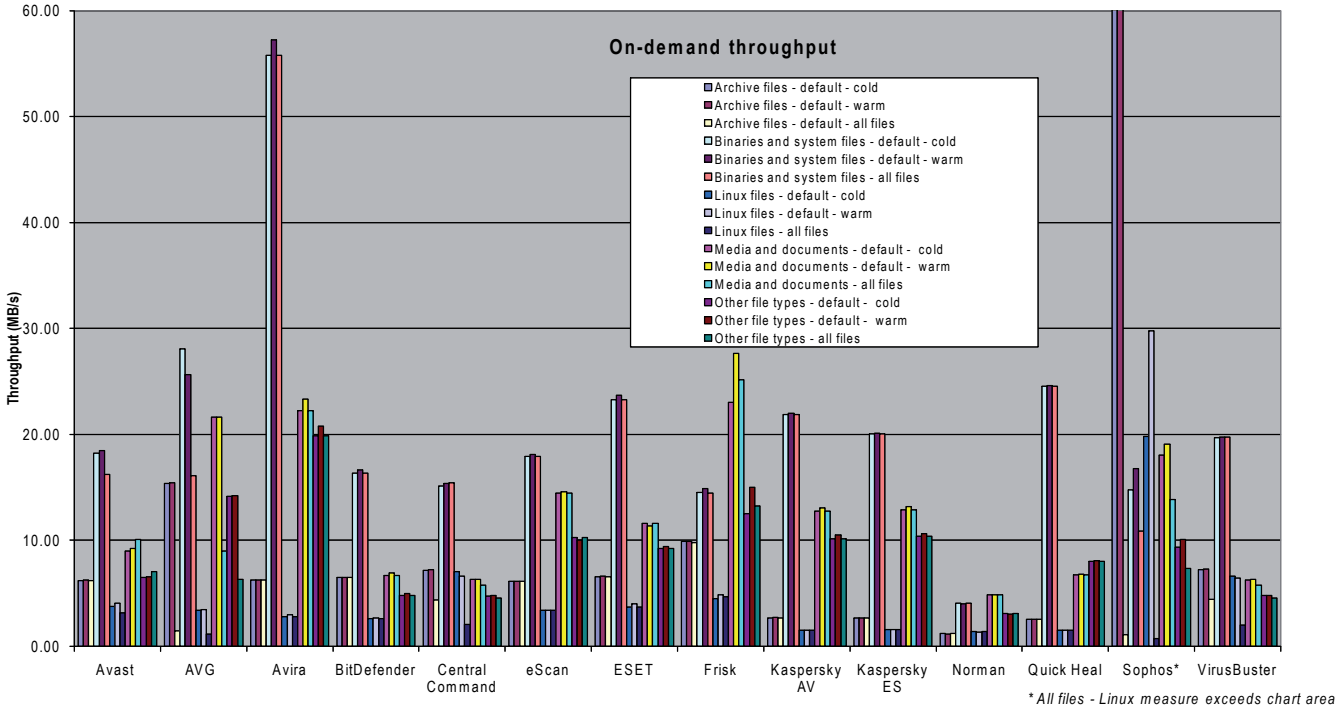
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.03%
Worms & bots	89.17%	**False positives**	1



Despite the fact that our test deadline clashed with the Russian Christmas holidays, *Kaspersky* managed to submit two products this month – both from a new and heavily re-engineered *Linux* range, and with the slightly worrying assertion that the developers had intended them to be operated via a GUI. Installing the first – which seemed to be slightly more business-focused – proved fairly simple at the outset, with a handful of installer packages provided in different formats and a readme file for instructions. Sadly this proved not to be displayable, let alone legible, and after initially running through the set-up steps of the .DEB package and finding more help was needed, we resorted to consulting the PDF documentation provided on the company's website.

This showed a horrendously complex layout for operating the product from the command line, which was eventually mastered and rendered reasonably usable with some practice and much perusal of the 215-page manual, but left us hankering for some nice simple, readable configuration files. We tried some work using a web admin GUI, but found this equally fiddly, clumsy and unresponsive. Logging was also a major problem, with detection events dumped from logs after they reached a certain size – despite having set limits in the product's controls to a considerably higher level than they ever reached.

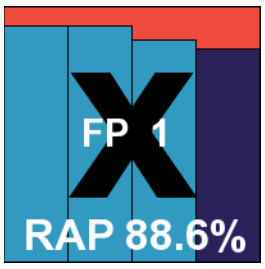
Eventually we got things moving along though, and scanning speeds proved to be very good, with excellent overheads on access with the default settings; turning the settings up to include archive formats and the like added to the overheads considerably, of course. Detection scores were very good, with no problems in the WildList set, but a single false positive in the clean sets was enough to deny *Kaspersky*'s business product a VB100 award.



*All files - Linux measure exceeds chart area

Kaspersky Endpoint Security for Linux Workstations 8.0.0.24

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.27%
Worms & bots	89.17%	**False positives**	1

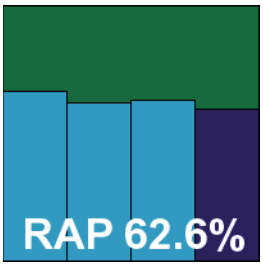


The second *Kaspersky* product seemed just about the same as the first, only with different names for some components and no sign of the web admin tool. Once again, we had to consult the manual and follow its advice to create a 40-odd-line configuration file to tweak the update settings, then enter a >50-character command to get it read in by the product, but once this was done things were all ready for us. There seemed to be some proprietary on-access system in use alongside *Samba* vfs objects, but it looked similar enough to *dazuko* to make little difference. Once again, on-access speeds were excellent, hinting that some nifty improvements had been made in this area.

Once again logging proved problematic, with the default cap set even lower this time – an initial run produced suspect results despite backing up the log database file every 30 seconds. Retrying once this had been spotted showed that the cap was removed after several restarts of the main service, but with time pressing some of the potentially suspect data still remained in the final results (which may thus be slightly inexact). Nevertheless, scores seemed close to those of *Kaspersky*'s first product – a fraction higher in most sets – but the same false positive, on a highly popular IM client, was enough to spoil *Kaspersky*'s chances of any VB100 awards this month despite a generally strong showing and solid coverage of the WildList set.

Norman Endpoint Protection 7.20

ItW	100.00%	**Polymorphic**	85.29%
ItW (o/a)	100.00%	**Trojans**	81.26%
Worms & bots	86.62%	**False positives**	0



Norman's product proved one of the most problematic at submission time, thanks to the requirement that it be installed with a live web connection. This was hastily performed on the deadline day

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Avast	Default	X/√	X/√	√	√	X/√	X/√	√	√	√	√	√
	All	√	√	√	√	√	√	√	√	√	√	√
AVG	Default	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	All	X	X	X	X	X	X	X	X	X	X	√
Avira	Default	2	√	√	√	√	√	√	√	√	X	√
	All	2	√	√	√	√	√	√	√	√	X	√
BitDefender	Default	√	√	8	8	√	√	√	√	√	√	√
	All	√	√	8	8	√	√	√	8	√	√	√
Central Command	Default	2	√	√	√	√	X	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	X	X	√
eScan	Default	√	√	8	8	√	√	√	8	√	√	√
	All	√	√	8	8	√	√	√	8	√	√	√
ESET	Default	√	√	√	√	√	√	√	5	√	√	√
	All	√	√	√	√	√	√	√	5	√	√	√
Frisk	Default	5/√	5/√	5/√	5/√	5/√	√	3/√	2/√	5/√	5/√	√
	All	5/√	5/√	5/√	5/√	5/√	√	3/√	2/√	5/√	5/√	√
Kaspersky AV	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky ES	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Norman	Default	X	√	8	1	√	√	√	8	√	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
Quick Heal	Default	X	√	X	X	√	X	√	X	√	X	√
	All	2	X	X	X	X	X	X	X	X	X	√
Sophos	Default	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	All	X	X/√	X/7	X/7	X/√	X/√	X/√	X/7	X/√	X/√	√
VirusBuster	Default	2	√	√	√	√	X	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	X	X	√

Key: X - Archive not scanned; X/√ - Default settings/thorough settings;√ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels.

(*Please refer to text for full product names*)

Reactive And Proactive (RAP) scores		Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Avast	VB100	92.27%	98.25%	95.98%	95.50%	82.55%	92.26%
AVG	VB100	97.13%	97.11%	88.86%	94.37%	78.07%	90.29%
Avira	VB100	99.71%	99.72%	96.05%	98.49%	93.55%	97.26%
BitDefender	VB100	98.76%	99.38%	99.01%	99.05%	92.10%	97.31%
Central Command	VB100	88.69%	90.68%	85.35%	88.24%	83.64%	87.09%
eScan		97.21%	95.98%	94.12%	95.77%	87.10%	93.60%
ESET	VB100	96.53%	96.34%	94.89%	95.92%	91.51%	94.82%
Frisk	VB100	80.83%	75.41%	62.50%	72.91%	76.00%	73.69%
Kaspersky AV		91.32%	90.54%	86.68%	89.51%	85.37%	88.48%
Kaspersky ES		92.41%	92.08%	86.71%	90.40%	83.25%	88.61%
Norman	VB100	66.49%	61.56%	62.78%	63.61%	59.48%	62.58%
Quick Heal	VB100	92.43%	85.20%	76.69%	84.78%	82.07%	84.10%
Sophos	VB100	91.46%	90.81%	92.84%	91.71%	87.72%	90.71%
VirusBuster	VB100	88.69%	90.68%	85.35%	88.24%	83.64%	87.09%

(*Please refer to text for full product names*)

– a little too hastily as it turned out, as the install process announces itself to be complete and returns control to the command line well before it has actually finished running. Our first attempt – when the network was reset to internal only as soon as the install seem to be done – was missing large portions of the product and a second attempt was needed. This time all went OK, but we found that most of the components refused to function without an X *Windows* system in place. We eventually managed to get some on-demand work done, but found that configuration for the on-access component was not possible without a graphical set-up (there was some confusion over whether or not a web-based GUI was expected to be fully functional – either way, we had no luck trying to use it).

In the end, we went ahead and installed the *Ubuntu* desktop system on one of the test machines – which was something of a mammoth task as it was not included with the standard install media and took some two hours to download, prepare and set up. With this done we finally got to see the interface, which closely resembled those of *Norman*'s *Windows* products, and was plagued with the same wobbliness, time lags and occasional freakouts. All we used in the end was the option not to automatically clean files spotted on access, and the desktop was then shut down for the speed measures.

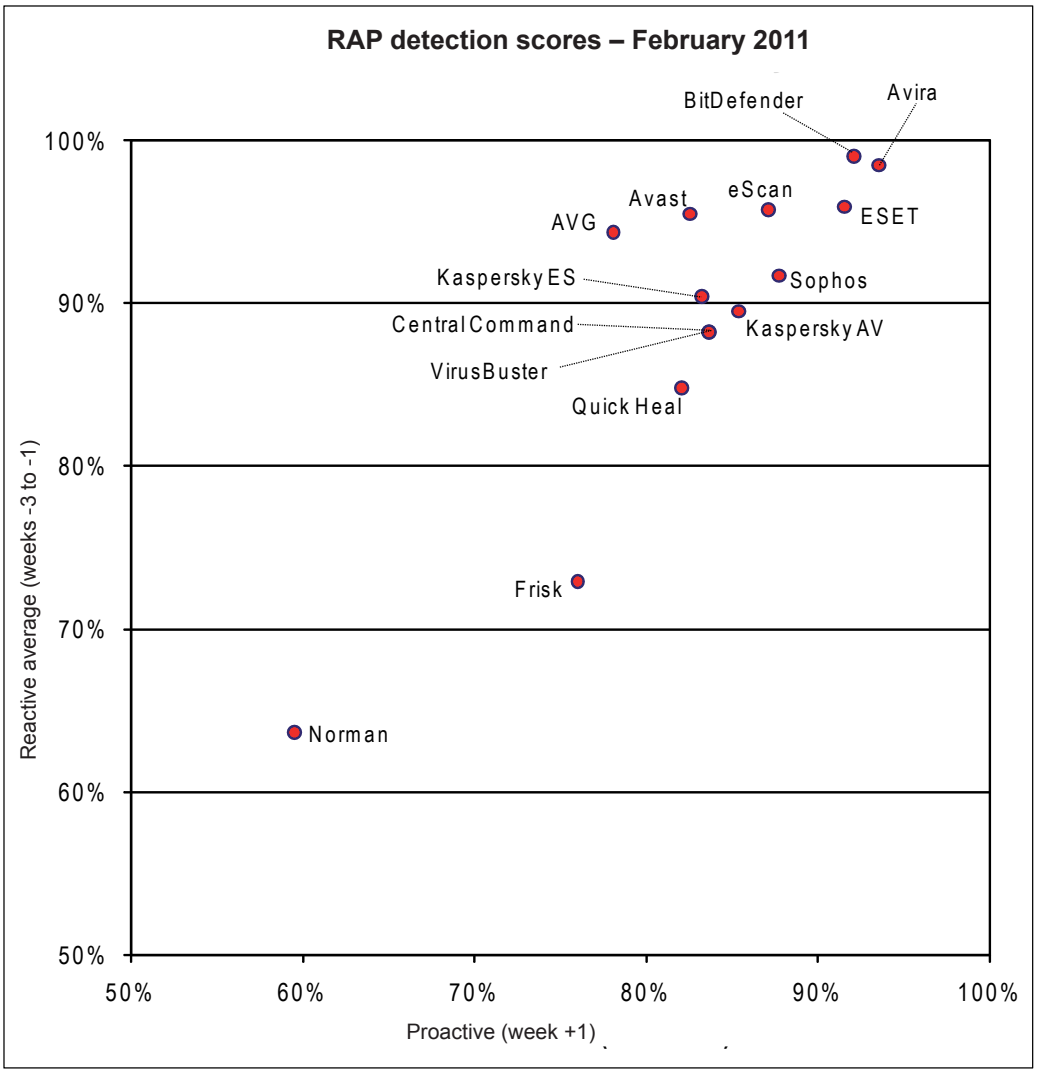
These showed the usual fairly slow times on demand, as the *Sandbox* system carefully picks each file apart. Much the same was observed on access, for the first run at least, but in the 'warm' measures, where files were checked for the second and subsequent time, an impressive improvement was observed.

Scanning of the infected sets was extremely slow – in part thanks to the deep *Sandbox* analysis – and occasionally flaky, with several runs failing to complete, or stopping output to logs part-way through. Several re-runs over two full weeks and on several systems, were still not quite complete several days after the deadline for this report, and as a result some of the data presented relies in part on on-access scores, which may be a fraction lower than the product's full capability on demand. Detection rates were less than staggering, but not too disappointing, and with the WildList and clean sets causing no problems, a VB100 award is just about earned after all our efforts.

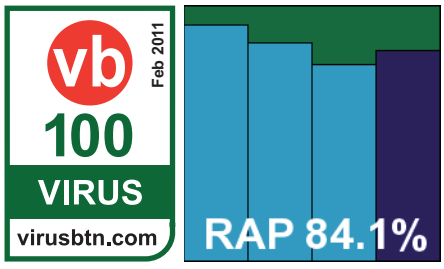
Quick Heal Anti-Virus for Linux 12.00

Virus database: 04 January 2011

ItW	100.00%	**Polymorphic**	96.94%
ItW (o/a)	100.00%	**Trojans**	95.57%
Worms & bots	96.86%	**False positives**	0



Back to something much simpler and more user friendly, *Quick Heal*'s 141MB zip archive unpacked to reveal several folders and a nice install script, which took us through the steps of getting everything up and running. After resolving a single dependency, all went smoothly, including the set-up of *dazuko* – *Quick Heal* was one of only a few products to do this itself rather than dumping the work on the sysadmin.

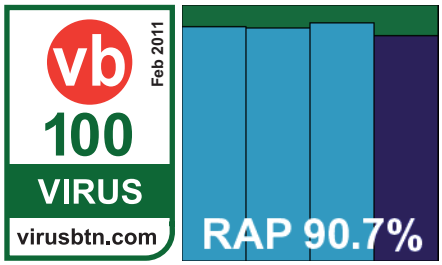


Configuration and documentation was clear, although man pages were lacking, and with simple, intuitive controls, testing went ahead without problems. Speeds were not brilliant, and overheads perhaps a little on the heavy side, but detection rates were impressive throughout. With no problems in the core sets, *Quick Heal* comfortably makes the grade for VB100 certification this month.

Sophos Anti-Virus for Linux 7.2.3

Engine version 3.15.0; Virus data version 4.61; User interface version 2.07.298

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.97%
Worms & bots	96.75%	**False positives**	0



Sophos was another product that took most of the load off the installer's shoulders, with its 232MB .tgz bundle containing a comprehensive installer utility. Detection of platform, compilation and insertion of required modules and so on was all carried out smoothly and automatically. A proprietary on-access hooking module is included.

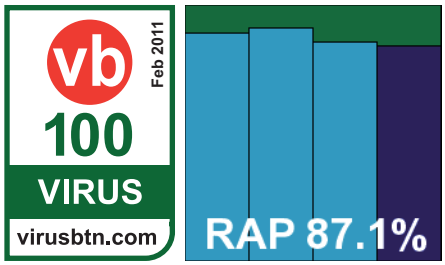
Configuration was again via several control utilities, which were perhaps less than clear in their usage instructions and difficult to operate from a purely command-line setting. A web interface was also provided, but we never got it working, mainly because the default settings got us through most of the jobs we needed to carry out without much trouble.

Scanning speeds were excellent (especially using the default settings, where no archive types are analysed), and on-access overheads were among the very lightest. Detection rates were not bad, with RAP scores a little below what we have come to expect from this product, but fairly strong nevertheless. The core sets presented no issues, and *Sophos* easily earns its VB100 award this month.

VirusBuster for Samba Servers 1.2.3_3-1.1_1

Scanner 1.6.0.29; virus database version 13.6.130.0; engine 5.2.0.28

ItW	100.00%	**Polymorphic**	90.52%
ItW (o/a)	100.00%	**Trojans**	83.45%
Worms & bots	95.69%	**False positives**	0



VirusBuster's product proved one of the simplest to set up and test, thanks to a very similar process having already been performed with the *Central Command* solution. Running the installer scripts and following instructions to set up *Samba* settings took just a few minutes. The on-demand scanner has a slightly quirky syntax but is soon rendered familiar and friendly. However, trawling through the several configuration files in /etc in the vain hope of finding some settings for the on-access scanner was abandoned quickly.

Scanning speeds proved very good indeed, with similarly impressive on-access lags, and detection rates were pretty decent too. With just a single item in the clean sets warned about, being protected with the Themida packer, *VirusBuster* has no problems claiming its latest VB100 award.

CONCLUSIONS

As is usually the case with our *Linux* tests, it was something of a roller-coaster month, with moments of joy and comfort intermingled unpredictably with moments of bafflement and horror. For the most part, the products lived or died by the clarity of their documentation and the simplicity of their approach; the usability of a tool is usually significantly greater if it runs along the same lines as other things of a similar ilk, rather than attempting a radical new approach. For those wishing to try something new, demanding that the user read carefully through several hundreds of pages of documentation – which cannot even be displayed on the machine they're trying to use the product on – may be a little much.

Thankfully, stability has been no more than a minor problem here – as one would perhaps expect from a platform which tends to need far fewer restarts than some others. Nevertheless, we did see a few problems – notably with GUIs and with those command-line tools which try to hijack and do overly funky things with the console display, returning it to its owner bedraggled, battered and occasionally broken. All in all, we saw a strong batch of performances, with a high percentage of passes; an unlucky maximum file size setting and a single clean sample (a popular product, but a fairly old version with limited usage) caused the only issues in the certification sets. Part of this is doubtless down to the solid field of regular high-achievers, but part may also be thanks to the absence of any new complex viruses.

We expect to see a tougher task next time around, when we revisit *Windows XP* and see just how many other products there are out there.

Technical details:

All products were tested on identical machines with *AMD Phenom II X2 550* processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Ubuntu Linux Server Edition 10.04.1 LTS i386*. On-access tests were performed from a client system running *Windows XP Professional SP3*, on the same hardware.

END NOTES & NEWS

RSA Conference 2011 will be held 14–18 February 2011 in San Francisco, CA, USA. For more information see http://www.rsaconference.com/2011/usa/.

The 12th annual CanSecWest conference will be held 9–11 March 2011 in Vancouver, Canada. See http://cansecwest.com/.

The 8th Annual Enterprise Security Conference will be held 14–15 March 2011 in Kuala Lumpur, Malaysia. The theme for the 2011 conference is 'Improving digital security to protect your assets from malicious cybercrime'. For details see http://www.acnergy.com/.

Black Hat Europe takes place 15–18 March 2011 in Barcelona, Spain. For more information see http://www.blackhat.com/.

Infosecurity Europe will take place 19–21 April 2011 in London, UK. For more details see http://www.infosec.co.uk/.

SOURCE Boston 2011 will be held 20–22 April 2011 in Boston, MA, USA. For more details see http://www.sourceconference.com/.

The New York Computer Forensics Show will be held 26–27 April 2011 in New York, NY, USA. For more information see http://www.computerforensicshow.com/.

The 5th International CARO Workshop will be held 5–6 May 2011 in Prague, Czech Republic. The main theme of the conference will be 'Hardening the net'. Details will be available soon on the conference website at http://www.caro2011.org.

The 20th Annual EICAR Conference will be held 9–10 May 2011 in Krems, Austria. This year's conference is named 'New trends in Malware and Anti-malware techniques: myths, reality and context'. A pre-conference programme will run 7–8 May. For full details see http://www.eicar.org/conference/.

The 6th International Conference on IT Security Incident Management & IT Forensics will be held 10–12 May 2011 in Stuttgart, Germany. See http://www.imf-conference.org/.

TakeDownCon takes place 14–19 May 2011 in Dallas, TX, USA. The event aims to bring together security researchers from corporate, government and academic sectors as well the underground to present and debate the latest security threats and disclose and scrutinize vulnerabilities. For more details see http://www.takedowncon.com/.

The 2nd VB 'Securing Your Organization in the Age of Cybercrime' Seminar takes place 24 May 2011 in Milton Keynes, UK. Held in association with the MCT Faculty of The Open University, the seminar gives IT professionals an opportunity to learn from and interact with security experts at the top of their field and take away invaluable advice and information on the latest threats, strategies and solutions for protecting their organizations. For details see http://www.virusbtn.com/seminar/.

The 2011 National Information Security Conference will be held 8–10 June 2011 in St Andrews, Scotland. Registration for the event is by qualification only – applications can be made at http://www.nisc.org.uk/.

The 23rd Annual FIRST Conference takes place 12–17 June 2011 in Vienna, Austria. The conference promotes worldwide coordination and cooperation among Computer Security Incident Response Teams. For more details see see http://conference.first.org/.

SOURCE Seattle 2011 will be held 16–17 June 2011 in Seattle, WA, USA. For more details see http://www.sourceconference.com/.

Black Hat USA takes place 30 July to 4 August 2011 in Las Vegas, NV, USA. For more information see http://www.blackhat.com/.

VB2011 takes place 5–7 October 2011 in Barcelona, Spain. *VB* is currently seeking submissions from those wishing to present at the conference. Full details of the call for papers are available at http://www.virusbtn.com/conference/vb2011. For details of sponsorship opportunities and any other queries relating to VB2011, please contact conference@virusbtn.com.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

- Single user: $175
- Corporate (turnover < $10 million): $500
- Corporate (turnover < $100 million): $1,000
- Corporate (turnover > $100 million): $2,000
- *Bona fide* charities and educational institutions: $175
- Public libraries and government organizations: $500

Corporate rates include a licence for intranet publication.

See http://www.virusbtn.com/virusbulletin/subscriptions/ for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:
Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com Web: http://www.virusbtn.com/