COMPARATIVE REVIEW

REDHAT LINUX

Matt Ham

It is thirteen months since the first *Linux* comparative review graced the pages of *Virus Bulletin* (see *VB* April 2002, p.16). During those months the operating system has enjoyed a significant rise in popularity, so it came as something of a surprise to receive only 11 products for this review – the same number as last time. With the production of an on-access scanner for a *Linux* product being trickier than on more homogeneous operating systems, there were no VB 100% awards given in the previous *Linux* comparative review. (A cynical reviewer might link these two facts.)

A newcomer to the comparative reviews this month is *H+BEDV*, whose product *AntiVir* has been a feature of the anti-virus landscape since time immemorial. The only company, as far as I am aware, to give away branded beer as a marketing gimmick, I have good reason to wish them a long stay in the regular line-up for comparative review.

THE TEST SETS

The test sets compiled for this review were derived from the March 2003 test sets. With the deadline for product submission being only days after the release of a provisional WildList, this is probably one of the tougher tests for vendors – usually there are a couple of weeks' grace between the release of the WildList and the submission deadline.

Since the last comparative review was carried out before the WildList had stabilised to a new regular production schedule, there were a large number of changes to the In the Wild (ItW) test set. Some of the changes had been anticipated, while others seemed, initially at least, downright outlandish.

On-demand tests	ItW File		Macro		Polymorphic		Standard		Linux	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%
Alwil avast!	0	100.00%	3	99.56%	160	91.22%	11	99.55%	40	59.33%
DialogueScience Dr.Web	5	99.51%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	4	99.82%	4	99.73%	6	66.67%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	3	99.86%	7	65.00%
GeCAD RAV	0	100.00%	0	100.00%	35	97.61%	0	100.00%	0	100.00%
H+BEDV AntiVir	7	99.23%	47	99.42%	753	83.28%	52	97.79%	44	0.00%
Kaspersky KAV	0	100.00%	0	100.00%	1	99.92%	0	100.00%	0	100.00%
Norman Virus Control	1	99.76%	56	98.95%	179	91.25%	12	99.53%	5	85.67%
Sophos SWEEP	0	100.00%	0	100.00%	60	95.79%	15	99.31%	14	46.67%
Trend Server Protect	0	100.00%	0	100.00%	214	95.81%	11	99.59%	7	60.00%
VirusBuster VirusBuster	0	100.00%	3	99.93%	160	89.13%	11	99.52%	40	6.67%

On the way out of the test sets were a motley collection of Win32 viruses and O97M viruses. The fact that the problematic W32/CTX has finally departed the test sets will be a reason to rejoice in some camps, though some may shed a tear over Junkie for nostalgia's sake. Replacing these were a rush of Win32 mailers and network-aware pests, including nine new W32/Opaserv variants since the last comparative review.

The surprise amongst the newcomers was the large number of W95 viruses making an appearance for the first time. Six W95 specimens were added to the test sets, including a further variant of an old stalwart, W95/CIH.1049. Quite what could have caused the resurgence of infected *Windows 95* machines? In fact, there is no such resurgence, since most of these viruses throw up errors by the ton if run on any *Windows 95* machine. *Windows 98* could tempt some to run, somewhat half-heartedly. However, the mass of additional DLLs required by some of these viruses leaves a question mark as to quite how they have entered the wild.

The *Linux* test set was much the same as that used in the last *Linux* review. Internal files from malware which arrives in large packages, e.g. Linux/Lion, were removed however, since they were giving the test sets an undeserved aura of importance as a result of their bulk. The *Linux* files in the test set are present for one reason: to determine whether products are even attempting to detect *Linux* malware. As such, the files can be divided into two main categories: the archive stored worms and the ELF format file viruses.

LINUX PECULIARITIES

The *Linux* platform is a difficult one for which to design an on-access scanner, on account of the flexibility of the operating system. The number of different *Linux* kernels is as grains of sand in a desert, and offers no solidity for those who require a firm and unchanging environment.

The flexibility of the operating system is one of the strongest features of *Linux*. As users wish to perform ever more cunning tricks on a *Linux* machine, however, the number of details required as to what exactly is or is not in the kernel increases significantly. Interrupting file access is just such a sneaky trick – and one required by on-access scanners.

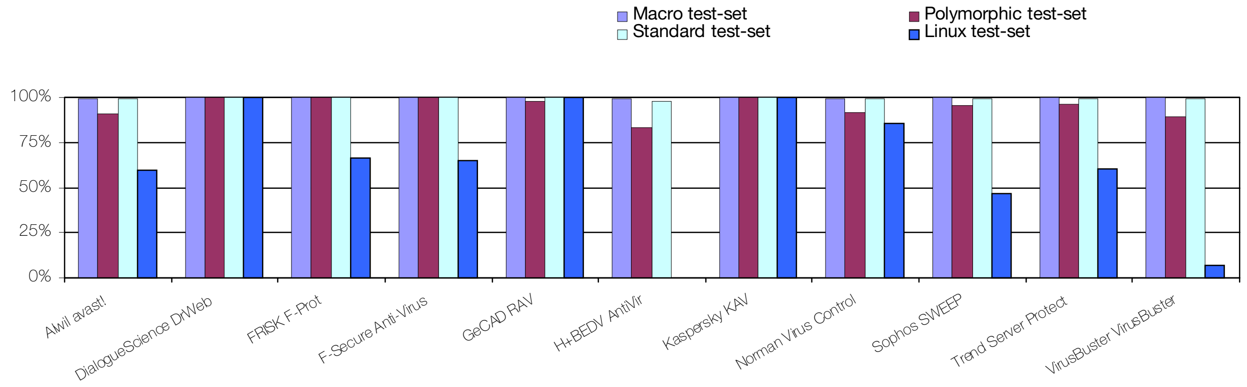
The developers of products in this review have used a number of techniques to overcome this kernel dependency. The method requiring least user interaction is that which uses a non-kernel component as a vector for filtering. The designated on-access test scenario in this review was file opens through *Samba*, therefore it was not surprising to see *DialogueScience* and *GeCAD* using *Samba* to pass files for on-access scanning. *F-Secure* offers a daemon which can intercept http GET requests in a similar fashion, though this was not tested in the review.

However, this method of scanning is somewhat limiting in that file access from other sources can occur with no checking, and such outside access can play havoc with the scanning cache, if vendor documentation is to be trusted. The use of a kernel driver can allow all file access to be filtered but is, as stressed earlier, kernel-dependent. *Trend Micro* has a sufficiently large user base that a selection of kernel modules for popular kernel constructions is offered.

This is not so much use to the inveterate tinkerer, however, who must compile his own source code for the kernel module. *H+BEDV* and *Alwil* use an open source basis named *Dazuko* for this process. The resources associated with this project were sufficient to allow easy and successful compilation of the source.

Kaspersky Lab also supplies source for its kernel module – although the documentation provided, and the peculiarities of *RedHat Linux,* made this a task which was not surmountable within the allocated timeframe. *Kaspersky*'s suggestion for obtaining sufficient information for guaranteed

Detection Rates for On-Demand Scanning



installation is to compile a kernel from scratch – which seems a rather high expectation for a user concerned with uptime and preserving a machine in a state of stabilty.

Alwil avast! 4.0 (beta1)

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.55%
Linux	59.33%	**Polymorphic**	91.22%

May 2003 100% VIRUS BULLETIN www.virusbtn.com

Alwil's *avast!* was submitted as a beta version of the software, which can be daunting when a review is to be performed. The beta status of the product may explain the slight awkwardness of the installation procedure, which required the execution of two shell scripts in different locations. A rather less avoidable part of the installation procedure was the need to compile the *Dazuko* source code – a relatively easy task once the appropriate website (http://www.dazuko.org/) had been paid a visit.

Once the program was up and running, scanning commenced, only to end speedily. The culprit was a segmentation fault caused by one of the Linux/Bliss samples in the test set. This caused the scan process to crash on demand repeatedly and the offending sample was removed from the set for this scan and recorded as a miss. The same file caused problems on access. In this case, however, there were no outward signs of the scanning failure – the engine simply ceased operating after this file had been scanned. Again the sample was noted as a miss, and once the scanning daemon had been restarted, no further problems arose.

Other than this issue, scanning results were good. Large differences in performance on *Linux* samples on access and on demand can be attributed to different treatment of archives under these two scenarios. With full detection both on access and on demand, and no false positives, *avast!* is the first product in this review to receive a VB 100% award.

DialogueScience Dr.Web for Linux 4.29.7

ItW Overall	99.51%	**Macro**	100.00%
ItW Overall (o/a)	99.51%	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	100.00%

Dr.Web arrived as two packages, one for the main on-demand scanner and another for the *Samba* daemon-based scanner, both of which were in RPM format and installed with no problems. It was notable in this review that the products were split roughly between those which installed a path or link to their executables and those which leave this task to the person installing the software. Both methods will have their advocates – *Dr.Web* is one of those in which the onus is on the user to perform the task.

Installation and activation of the *Samba* scanner was simple enough, requiring only a single-line addition to the smb.conf file for each share to be protected. What was noticeable, however, was that access to files on the *Samba* share slowed noticeably when the scanning daemon was in place. Despite this sluggishness on access, scanning efficiency was close to the usual *Dr.Web* levels – but fell short of full detection. The files that were missed were the five samples of W95/Bodgy in the ItW test set, denying *DialogueScience* a VB 100% award. Less of a surprise were the presence of the now somewhat traditional 15 suspicious files in the clean test set.

FRISK F-Prot Antivirus for UNIX 3.13a 3.13.2

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	n/a	**Standard**	99.73%
Linux	66.67%	**Polymorphic**	99.82%

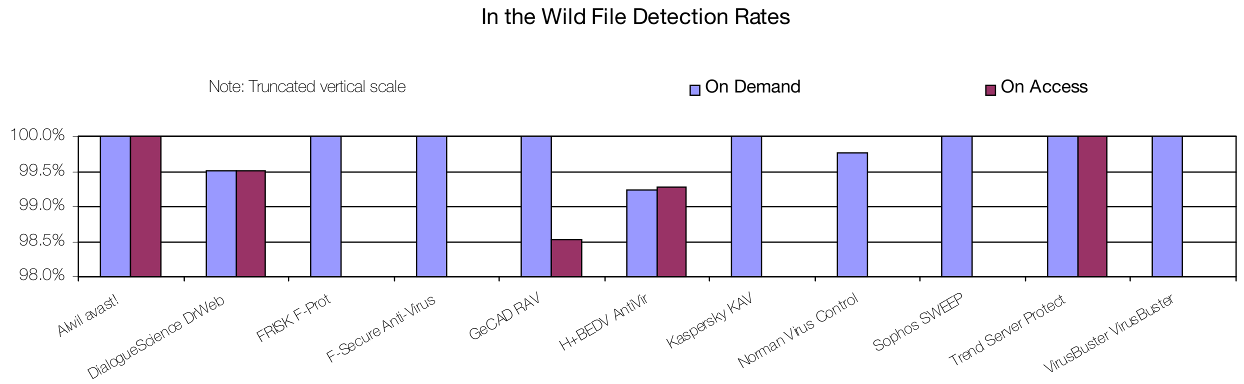
F-Prot Antivirus was another product to offer the package in RPM format, and as a result was simple to install. An on-access component is supplied with the product, though this was not tested since it filters only http GET requests, rather than the fopen/fclose accesses which are tested in *VB* protocols. Such a method of access filtering thus lies outside the scope of comparative testing. This caveat also applies to other products in this review. Several have on-access features which lie outside the scope of the review, and the lack of a VB 100% award in this test is relevant only within the limitations set by the need to keep the test procedures practical.

The *FRISK* product showed very good detection rates across all test sets. A sizeable proportion of the small number of misses seen was attributable directly to the fact that *F-Prot Antivirus* has archive scanning disabled in its default setting. This explains misses of the W32/Heidi virus and also for the *Linux* worms which distribute themselves as archives. In contrast, *Linux* ELF infectors were detected perfectly.

F-Secure Anti-Virus for Linux Server 4.50.2111

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	n/a	**Standard**	99.86%
Linux	65.00%	**Polymorphic**	100.00%

The package supplied for the installation of *F-Secure* was in a proprietary encrypted format, requiring the registration



key for installation. This format allowed a more interactive installation procedure than that seen for the RPM-based installers. The installation procedures can be divided into three camps. The first is the bare-bones approach, where scattered shell scripts, manually edited configuration files, and a healthy attention to man pages are the order of the day. A second camp opts for RPM packages – which, although very easy to use, tend to leave the user rooting around in the background when fine-tuning of the configuration is required. The approach chosen by *F-Secure* may not adhere to any industry standards, but for simplicity of both installation and configuration it certainly has its advantages.

As expected from a product using two engines, the detection rates for *F-Secure*'s product were at their usual high level. Files were missed either as the result of not scanning archives by default, or of choosing not to scan file extensions which are only rarely host to dangerous code.

GeCAD RAV for Linux 8.4.2

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	98.54%	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	97.61%

The installation method of *GeCAD*'s *RAV* was the RPM format, with an on-access scanner being supplied for *Samba*. This gave, in total, four RPMs to be installed, with the requirement that these be installed in order of their dependencies. Although this order was fairly easy to guess, this was a minor irritation.

When scanning on demand, the *RAV* engine had no problems whatsoever in the test sets, missing samples of W32/Fosforo, with the remainder of misses being a few other incompletely detected viruses in the polymorphic set. Matters were trickier in the on-access tests. *GeCAD*'s documentation states that access to the shared drive performed by methods outside the *Samba* functionality could cause problems for the scanner and this seemed to be the case even when only one or two files were concerned. Being more conscientious about methods of access to the shared resource gave several on-access scans which performed oddly and it took some patience to reach a final test result.

The final result was identical to that seen on demand, with the exception of misses on X97M/Jini.A1, W32/Gibe.B and W32/Lovgate.C. Several more tests repeated under the same conditions demonstrated that this was a reproducible set of misses. Since these are all in the ItW test set, *RAV* was denied a VB 100% award on this occasion.

H+BEDV AntiVir Workstation 2.0.7

ItW Overall	99.23%	Macro	99.42%
ItW Overall (o/a)	99.27%	Standard	97.79%
Linux	0.00%	Polymorphic	83.28%

This is another product that uses *Dazuko* – which is not a surprise, since *H+BEDV* has played a significant part in the production of this resource. With the practice obtained from installing *Dazuko* for *avast!* this part of the installation procedure proved the easiest aspect. The program installation itself was slightly complicated by the fact that the archives supplied had been produced on a *Windows* machine, this causing changes to the case of several file names.

H+BEDV does, however, offer one of the more interactive shell scripts for product installation, which allowed easy detection of which files should be called and their locations, since it declared the source of any installation errors. This was, of course, very useful for configuring the program after installation as well as this early negotiation of problems. One problem which proved insurmountable was the issue of a licence key, since none of those supplied could be persuaded to work. However, an unlicenced copy of the

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files		Linux Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	(s)	Throughput (MB/s)	(s)	Throughput (MB/s)
Alwil avast!	107.0	5111.5		12.4	6397.9		56.0	2846.7	14.8	5041.0	12.8	3269.4
DialogueScience Dr.Web	149.0	3670.7	[15]	9.3	8530.5		72.0	2214.1	11.6	6431.7	14.3	2926.5
FRISK F-Prot	77.0	7103.0		3.5	22666.8		39.0	4087.6	4.8	15543.2	6.7	6246.0
F-Secure Anti-Virus	181.0	3021.7	[1]	11.2	7083.4		185.0	861.7	34.0	2194.3	5.3	7895.9
GeCAD RAV	287.0	1905.7		4.6	17246.5		132.0	1207.7	4.5	16579.4	7.5	5579.8
H+BEDV AntiVir	101.0	5415.2	1	48.0	1652.8		83.0	1920.7	8.9	8382.9	10.3	4063.0
Kaspersky KAV	148.0	3695.5		11.3	7020.7		80.0	1992.7	19.1	3906.2	25.9	1615.8
Norman Virus Control	129.0	4239.8		9.0	8814.9		75.0	2125.6	17.0	4388.7	26.0	1609.6
Sophos SWEEP	59.0	9270.0		9.5	8350.9		37.0	4308.6	10.2	7314.5	4.9	8540.5
Trend Server Protect	93.0	5881.0		8.6	9224.9		45.0	3542.6	15.3	4876.3	18.4	2274.4
VirusBuster VirusBuster	163.0	3355.4		6.1	13005.5		93.0	1714.2	10.7	6972.7	3.7	11310.4

software lacks only logging to file and the ability to perform actions on detected viruses. Since logging of infections to syslog is supported, this was used for detection analysis.

As a product that is new to the testing process, certain misses were more or less expected, such as ACG.A and ACG.B. More concerning was the miss of W95/Bodgy In the Wild, which was sufficient to deny *H+BEDV* a VB 100% award.

Kaspersky KAV for Linux 4.0.30

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	n/a	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	99.92%

KAV for Linux arrived as a set of files, one of which is launched as a proprietary installer and searches for the others. This mechanism did not seem to be implemented perfectly, though after two or three tries of various command line options it became apparent that stating the target file explicitly was a much more reliable method of initiating installation.

On-demand detection was very good indeed, with only a single sample of W32/Etap being missed over the entire test set. An on-access scanning module was also supplied, though this was distinctly more problematic. With the installation of *Dazuko* having provided practice in the complexities of kernel modules, it was expected that *Kaspersky*'s module would prove just as easy to produce. Unfortunately this was not the case, with numerous attempts to compile the module ending in failure. The documentation supplied accepted that this was a likely outcome, given the nature of some *Linux* distributions and their kernel config files. The suggested remedy was to recompile the kernel so as to have a known version to work with. However, given the time constraints in testing, and the specific kernel stipulated for the test protocol, this remained untested.

Norman Virus Control Version 5.53.02

ItW Overall	99.76%	**Macro**	98.95%
ItW Overall (o/a)	n/a	**Standard**	99.53%
Linux	85.67%	**Polymorphic**	91.25%

Norman's product uses the RPM method of installation, resulting in an uneventful process. In fact, 'uneventful' sums up the performance of *Norman Virus Control* in the testing process, with no problems being encountered. Misses for the product were well spread among the test sets, with the In the Wild miss of W32/Zoek.D being the only surprise.

Sophos SWEEP 3.68

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	n/a	**Standard**	99.31%
Linux	46.67%	**Polymorphic**	95.79%

The *Sophos* product is installed by means of a shell script, which is not quite as intelligently constructed as it might be. The documentation supplied states that, in order to run the on-demand scanner alone, no users need to be added, though if the product is to be used with clients on other machines, a *SWEEP* user must be installed. However, the installation script will not run unless this user is created manually, despite there being no need for the user other than to satisfy the script's demands.

Once past this niggle, installation and scanning went smoothly, and detection was as expected with one exception: clearly some engine tweaking has been going on at *Sophos*, since the detection of polymorphic viruses has improved noticeably since the last test.

Trend Server Protect Linux 1.1

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.59%
Linux	60.00%	**Polymorphic**	95.81%

Trend's *ServerProtect* is the only product to have been supplied as a graphical application in this test. *GeCAD* and *FRISK* offer graphical front-ends for their home-user *Linux* software, though these were not submitted (there may be others of which I am unaware).

The use of a graphical interface requires a little preparation on the part of the user. The interface uses the http protocol to communicate with the *ServerProtect* engine, and requires Java functionality which is not a standard installed package for *Mozilla*. After installation of the appropriate Java RPM a few symbolic links must be created.

The installation packages provided by *Trend* can accept a variety of pre-made kernel modules, the method here being a forced install with standard modules and then replacing these modules with those appropriate for the kernel present on the machine in question.

After this set of procedures is completed, however, the GUI offered through *Mozilla* was one which has all the features standard on any of the other *Trend* GUIs seen on other platforms. Although not used as such in this test, the interface can, of course, be used by a browser from any machine which is allowed access to do so – which would be a more usual method of using this functionality.

Such a pretty face, though, is pointless if there are no brains behind it, and *ServerProtect* did not disappoint on this front. With no false positives and full detection In the Wild, *ServerProtect* gains a VB 100% award. One problem which was noted, however, was that on one scan of the whole test set the server protect chain of command was broken at some point, and the *ServerProtect* GUI had to reconnect in order to regain control of the application.

VirusBuster VirusBuster LINUX 7.647

ItW Overall	100.00%	**Macro**	99.93%
ItW Overall (o/a)	n/a	**Standard**	99.52%
Linux	6.67%	**Polymorphic**	89.13%

VirusBuster uses the install script method of installation, which produced errors when run. The error messages were perhaps not designed to be read in a default KDE terminal window however, as cyan-on-white made the messages all but invisible to the naked eye. Some repositioning of the files solved this problem, and thereafter *VirusBuster* performed without a hitch. Scanning results were good in all but the *Linux* test set, in which only the cross-platform W32/Lindose virus was detected. With such a result it might be suspected that the detection of *Linux* native malware is not a high priority for *VirusBuster*.

CONCLUSIONS

The last *Linux* comparative was a sorry tale indeed, with all of those products that offered an on-access scanner proving to be untestable for one reason or another. The change of review platform from *SuSE* to *RedHat* has probably helped the developers somewhat, *RedHat* having a larger user-base to discover potential pitfalls. However it is the ever-increasing popularity of *Linux,* both in businesses and amongst home users, that is a more significant factor. The situation is eerily similar to the early days of *Windows* scanners – perhaps next year the full line-up will offer on-access scanning functionality.

Technical details:

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive running *RedHat Linux 8*, kernel build 2.4.18-14 and *Samba* version 2.2.5. An additional machine running *Windows NT 4 SP 6* was used to perform read operations on the *Samba* shared files during on-access testing.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/Linux/2003/test_sets.html.

A complete description of the results calculation protocol can be found at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

NOTE CONCERNING THE LINUX COMPARATIVE REVIEW (*VB*, MAY 2003)

Concerns were expressed concerning some of the samples in the *Linux* test set following the results of the last *Linux* comparative (see *VB*, May 2003, p.18). These fell into two categories:

First, one of the samples of ELF/Siilov-5916 was found to be corrupt and non replicable. This has been removed from the test set.

Secondly, the samples in the *Linux* test set were copied from a *Linux* machine, to a *Windows* server, and then returned to the *Linux* test machine. During this process the *Linux* attributes – most importantly those denoting an executable file – were lost. It has been pointed out that these attributes are valuable in determining whether *Linux* files should be scanned, since extensions cannot be used for this purpose and may in fact be misleading. In future tests *Linux* executables and scripts will be marked with the correct attributes. In practice this should render one sample of ELF/Obsidian.E (with an extension of .EXT2) more easily recognisable as an object which should be scanned.