COMPARATIVE REVIEW

NETWARE 6.0

Matt Ham

Preparations for a comparative review are, by now, a relatively automated response here at *Virus Bulletin*: check WildList, check product patches, check last year's notes and so the list goes on. It is at the checking of patches stage during *NetWare* comparatives that waves of unwelcome memories come flooding back – of vast patches, servers abending and long hours spent cursing the strangely poised folk whose images emblazon the OS. The notebook reading stage heightens this sense of foreboding, with strange errors and even stranger workarounds peppering last year's text. By the end of the preparations for this *NetWare* review thoughts of impending doom were greatest in my mind.

The version of the OS used in this test was *NetWare 6.0* with service pack 3 – the service pack being the usual several hundred megabytes in size. Installation of the patch failed to produce any problems, resulting in a patched and running server within minutes of beginning the process. With this promising start, the outlook seemed brighter and test sets and products could be considered.

The test set used was derived from the May 2003 WildList and, as expected, there were a large number of new worms to add to the collection. Inspection of these during replication led to the conclusion that none of the newcomers were destined to be tricky to detect – non-polymorphic worms not being the most challenging files for a scanning engine. At this stage the review looked set for a bumper crop of VB 100 % awards.

As for the products submitted for the review, there were a total of 11. In last year's *NetWare* review (see *VB*, August 2002, p.17) only nine products were on offer, so where do the differences lie? Out of the running is the now doomed *RAV for NetWare*, shelved after *GeCAD*'s takeover by *Microsoft*. This left three new arrivals, which were products from *Symantec*, *Command* and *Computer Associates*' US-based division. These products certainly existed at the time of last year's review, but were not available in a tested form for *NetWare 6*.

CA InoculateIT 4.5

ItW File	100.00%	**Macro**	99.90%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.90%
Standard	99.82%	**Polymorphic**	99.89%

Although the rebranding of this product to its new title *eTrust AntiVirus* has reached the product packaging, within the documentation and internal references the name *InoculateIT* is still predominant, hence the choice of name in this review. In some places the even older product name *InocuLAN* is mentioned, so it is to be expected that it will be a long time before the current name change takes full effect.

The first problems with this product arose upon installation, with the installer declaring that it would only run on *Windows 3.x* systems – certainly an odd statement. Ignoring this error, the *InoculateIT* NLMs and associated files were installed to the server by use of this client-side application. A few patches and updates were then applied manually before the server was rebooted to make sure of a full upgrade process.

From this point onwards the testing process proceeded smoothly, though there were a few surprises. For one, the rate of scanning for clean files was among the slower of those products reviewed. More surprisingly the clean executable set was the source of two false positives. While detection was good, W97M/Pain.A was a surprise miss, the two false positives were sufficient to deny *InoculateIT* a VB 100% for the first time in many months.

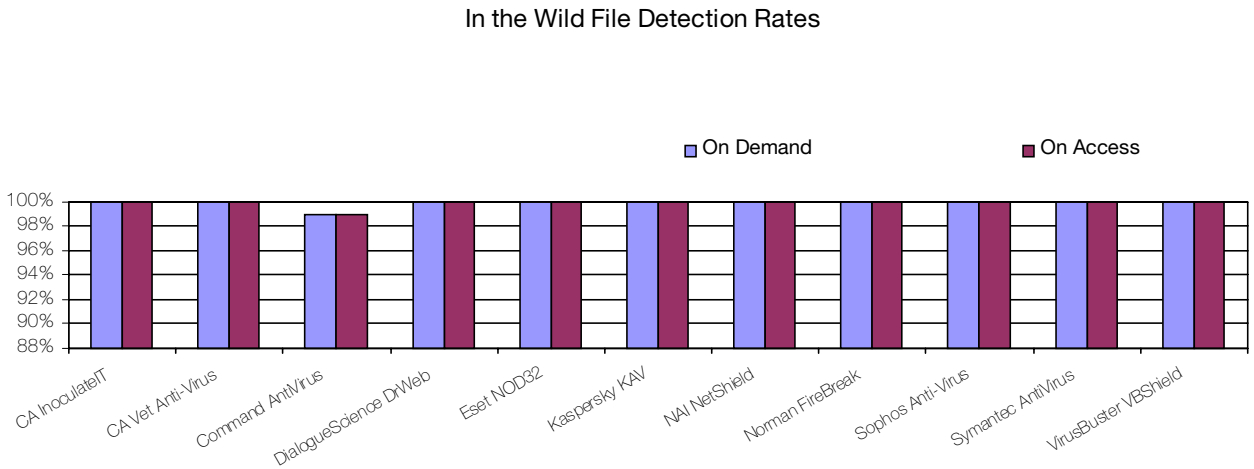
CA Vet NetWare AntiVirus 10.5.8

ItW File	100.00%	**Macro**	99.82%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.82%
Standard	99.90%	**Polymorphic**	98.50%

With its sister brand suffering a little in this review, the performance of *CA Vet* was of more interest than usual. Installation proceeded with no problems at all, being performed by a client-side *Windows* application. Update files were copied manually to the SYS:\system directory from where they update the application automatically. This method of updating is notable for the fact that the *Vet* updates are a collection of files rather than one monolithic object. The update process is triggered through one and one only of these files, making it imperative that this be the last of the files copied to the server.

On to the operation of *Vet*, which was overall a slightly less taxing experience than that of its sister product, with faster scanning in the clean sets and no false positives generated. Scanning of the clean sets was an issue for the zipped OLE files, however, where the rate of scanning was far slower than expected in comparison with other clean set scans. However, the problem was not fatal and *CA*'s *Vet NetWare AntiVirus* can therefore claim the first VB 100% award of this review. Misses in the test sets were here identical with those seen in other *Vet* products on other platforms.

Another irritation in *Vet*, common to several of the products, was that only one on-demand scan may be saved at any one



time. This makes the scanning of different areas at different times much more of a chore than might otherwise be the case.

Command AntiVirus 4.70.0.20710

ItW File	98.96%	**Macro**	100.00%
ItW File (o/a)	98.96%	**Macro (o/a)**	100.00%
Standard	98.96%	**Polymorphic**	100.00%

Command AntiVirus was supplied for this review in the form of three archives. One of these is a *Windows* application which installs the client and server side consoles, the other two contain engine and update components. Neither of the consoles were particularly user-friendly, the greatest initial problem being that it seemed impossible to tell whether a scan was actually in operation from the *Windows* version.

Further use of the consoles only added to the sense of frustration since, once applied, settings did not necessarily seem to be implemented. Examples of this behaviour included files being blocked on access when the on-access component was totally disabled and files being renamed and quarantined when set for deletion.

As a result of these quirks the scanner was tested by setting the delete option, repeatedly scanning the test set and deleting renamed files. This process was continued until no more files were flagged as infected.

The resulting figures showed that detection was good with the exception of one category. That category was .HTM-extensioned files, where none of those present in the test set were detected either on access or on demand. This alone was sufficient to deny *Command AntiVirus* a VB 100% award. These misses of .HTM files occurred despite '.HT*' being included on the list of extensions to be scanned.

DialogueScience Dr.Web 4.29c

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

Dr.Web is the first product in this review which relies entirely upon manual placing of files as its installation method. It also has one of the more basic-looking console views, the GUI being in shades of luminous green which would not have looked out of place on an early *Commodore*.

However, the lack of what could be termed as mod-cons does not detract from the functionality or effectiveness of the product.

Scanning speeds were good and only the usual *Dr.Web* warnings of possible infection were present, rather than any full-blown false positives.

As far as the interface was concerned, only one irritation stood out. This was the fact that on-demand scans did not exist on the interface. This might, at first, seem to be a serious omission, but is in fact much less important than it might seem. All that is required to operate an effective on-demand scan is to produce a scheduled scan one minute or so in the future. The ability simply to set up a scan to operate 'now' would be a welcome addition, though.

Detection rates for *DialogueScience*'s offering returned to their usual high levels after a recent blip in previous reviews, and full detection was recorded on demand. On access there were misses of samples within .ZIP and .EML

files, though nothing sufficient to deny *Dr.Web* another VB 100% award

Eset NOD32 1.455(20030707)

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

NOD32 is another product which is installed manually by copying files directly to the server. It is also unusual in having two scanning NLMs, both of which operate through command line parameters and do not have an interface during the process of operation.

Detection rates were good, both on access and on demand, but there were some discrepancies in the documentation when the help options were triggered at the command line. These declared that the scanning of archives was set as off by default – quite at odds with the detection of W32/Heidi.A within .ZIP files. Such misleading documentation, however, is not sufficient to cause any major commotion.

With the aforementioned full detection of infected files, there were also no false positives noted in the clean sets. *NOD32* thus receives a VB 100% award in this review.

Kaspersky AntiVirus 4.00.07

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	100.00%	**Polymorphic**	99.92%

Kaspersky's anti-virus products for *NetWare* have traditionally been among the better integrated into the operating system, and this offering was no disappointment on that front. Installation was quite a lengthy process in comparison with some, though this resulted in a console which is integrated into *NetWare*'s ConsoleOne interface. A further *Windows*-resident interface is also installed. The combination of these two control possibilities maximises the possibilities for control within a GUI and avoids some of the more irritating aspects of *NetWare*'s classic interface look and feel.

No false positives were recorded during the clean set testing and there were few misses in the infected samples. On demand a single sample of W32/Etap was missed, while only the .ZIP samples of W32/Heidi.A were additional misses on access. With such a performance KAV is duly awarded a VB 100%.

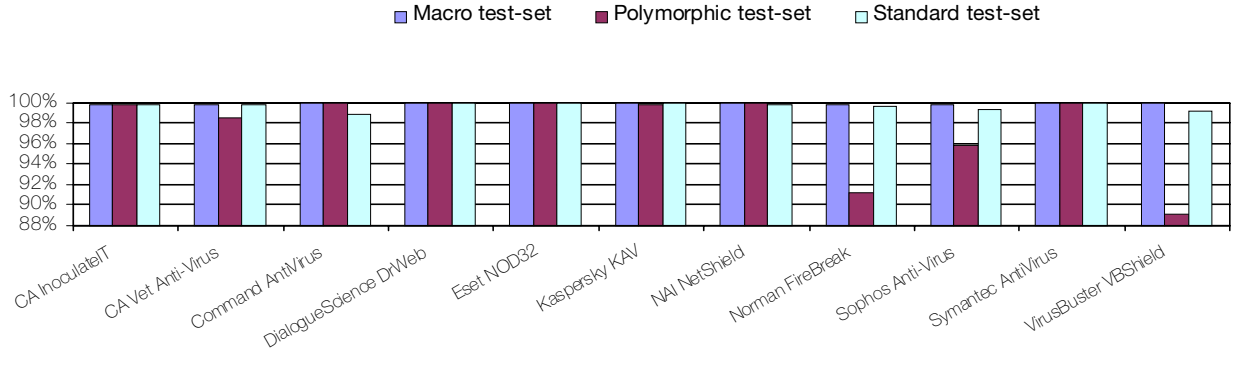
NAI McAfee NetShield 4.61 4.2.40 4.0.4275

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.82%	**Polymorphic**	100.00%

NetShield is controlled and installed through a *Windows* application, the installation of which requires, in turn, the installation of the Java Runtime Environment. Updates were performed on this occasion through unloading the application and inserting the required files. Upon reloading, the update occurred.

As was the case with several products on offer, scanning was slower than would seem comfortable. This was noted especially where files infected with W32/CTX.A were concerned, though the scanning rate of the clean set was also somewhat on the slow side. A further irritation

Detection Rates for On-Demand Scanning

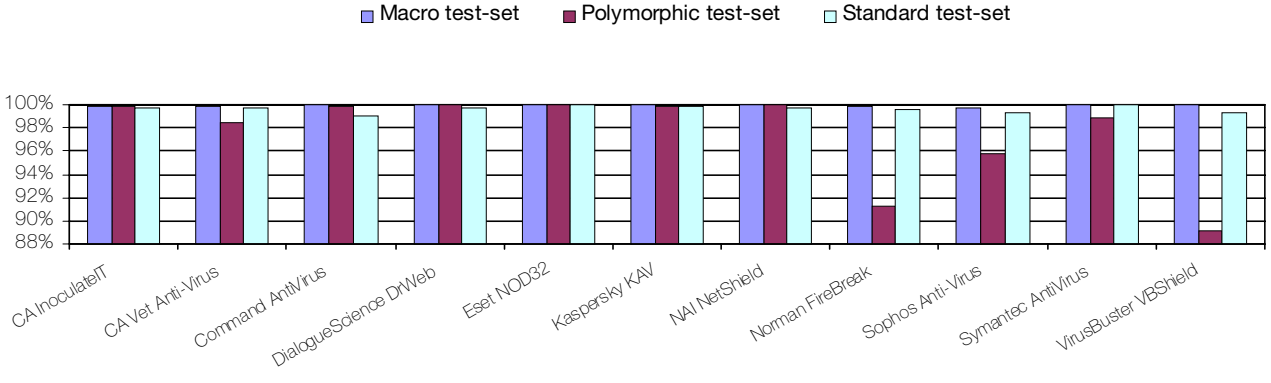


On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA InoculateIT	0	100.00%	4	99.90%	1	99.89%	3	99.70%
CA Vet NetWare AntiVirus	0	100.00%	12	99.82%	437	98.50%	4	99.78%
Command AntiVirus	5	98.96%	0	100.00%	2	99.91%	14	98.96%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	3	99.70%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kaspersky KAV	0	100.00%	0	100.00%	1	99.92%	2	99.88%
NAI McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	4	99.70%
Norman FireBreak	0	100.00%	4	99.90%	180	91.24%	11	99.64%
Sophos Anti-Virus	0	100.00%	11	99.73%	60	95.79%	15	99.31%
Symantec AntiVirus	0	100.00%	0	100.00%	35	98.86%	0	100.00%
VirusBuster VBShield	0	100.00%	0	100.00%	599	89.14%	13	99.34%

– though not confined to *NetShield* – was the inflated count of scanned files, which included all files within self-extracting archives in the count of 'files scanned'. For all this, however, no false positives were encountered.

Misses were limited in number – with samples of JS/Unicle and W32/Heidi.A comprising the total number of infections that were undetected. With this performance, therefore, *NetShield* is deserving of a VB 100% award.

Detection Rates for On-Access Scanning



On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA InoculateIT	0	100.00%	4	99.90%	1	99.89%	1	99.82%
CA Vet NetWare AntiVirus	0	100.00%	12	99.82%	437	98.50%	2	99.90%
Command AntiVirus	5	98.96%	0	100.00%	0	100.00%	14	98.96%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kaspersky KAV	0	100.00%	0	100.00%	1	99.92%	0	100.00%
NAI McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	2	99.82%
Norman FireBreak	0	100.00%	4	99.90%	180	91.24%	11	99.64%
Sophos Anti-Virus	0	100.00%	8	99.80%	60	95.79%	13	99.40%
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
VirusBuster VBShield	0	100.00%	0	100.00%	600	89.13%	14	99.15%

Norman FireBreak 4.60.2211

ItW File	100.00%	**Macro**	99.90%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.90%
Standard	99.64%	**Polymorphic**	91.24%

Firebreak demonstrates another method of installation to add to those encountered already. The *Windows* GUI installer launches a *Windows* ConsoleOne view part-way through the installation process, which must be tweaked a little before the installation can be completed. HTML help files are opened during this process to explain in detail, if required, what steps must be taken.

Control over the installed product is primarily via ConsoleOne, whether running on a client or a server. The level of control offered is similar to that offered by most GUI virus scanners, though will be less familiar to *Norman* users, the usual *Norman* interface being far from similar to the majority.

Some oddities are present in the interface, however. It is possible to set the scanner to report only on virus detections, but this appears to trigger the conditional 'actions to be taken if disinfection fails'.

It was deemed necessary to check on-access scanning by deletion, since deletion was unavoidable in these circumstances. There was further confusion at this point, since, when copying files, the target was noted as having been deleted – whereas in fact it was the source file that had undergone this fate.

Despite these strange occurrences, all was well on the detection front. Having generated no false positives and only the usual set of missed detections, *Norman*'s *FireBreak* is worthy of a VB 100% award.

Sophos Anti-Virus 3.71

ItW File	100.00%	**Macro**	99.80%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.73%
Standard	99.40%	**Polymorphic**	95.79%

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)
CA InoculateIT	751	728.3	2	61	1300.6		292	545.9	59	1264.5
CA Vet NetWare AntiVirus	177	3090.0		12	6611.1		71	2245.3	161	463.4
Command AntiVirus	1667	328.1		87	911.9		-	-	-	-
DialogueScience Dr.Web	188	2909.2	[12]	13	6102.6		77	2070.3	14	5329.1
Eset NOD32	73	7492.2		7	11333.4		108	1476.1	13	5739.0
Kaspersky KAV	315	1736.3		28	2833.3		162	984.1	44	1695.6
NAI McAfee NetShield	581	941.4		35	2266.7		166	960.3	50	1492.1
Norman FireBreak	377	1450.7		11	7212.2		27	5904.3	6	12434.6
Sophos Anti-Virus	166	3294.8		21	3777.8		40	3985.4	10	7460.7
Symantec AntiVirus	155	3528.6		24	3305.6		76	2097.6	25	2984.3
VirusBuster VBShield	234	2337.3		13	6102.6		181	880.8	18	4144.9

Sophos Anti-Virus was unique amongst products in this review in its installation method. The package is supplied as a single NLM which, when loaded, installed all the required files from within itself. This method of installation is an interesting halfway house between the two camps of total automation and manual file copying.

Other parts of the interface are, however, more irritating. It is still necessary to select all files for scanning when the target of a scan is a directory – only volumes may be scanned according to the inbuilt extension list. It is also very difficult to tell whether IDE files have been loaded so as to extend the detection abilities of the product.

Installation and interface comments aside, the *Sophos* product performed well. No false positives were apparent in any test set, and the infected samples in the ItW test set were all detected, thus earning *Sophos AntiVirus* (*SAV*) a VB 100% award. Detection rates for *SAV* are good in general, though several infected files have been missed for many months. These misses still include all the .MDB files in the test sets, although rumour has it that this detection at least will be implemented soon.

Symantec AntiVirus 8.00.0.9374

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

Symantec AntiVirus, the second '*SAV*' in this review, is certainly the product with the most involved installation process.

In order to be installed and administered this *SAV* required *Microsoft Management Console* with the *Symantec System Center Snapin*, which requires *Internet Explorer 5* or better. Even after all these are installed, it is necessary to load the NLMs manually when first installing to a server.

This rigmarole suffices to produce an interface which is identical in look, feel and most functionality to the rest of the *Symantec* product range. This is certainly worthwhile in a large organisation, for all the added time involved when installing one server for review purposes. The process was also easier than my memories of the same process in the last *NetWare* review.

The interface being the same as other *Symantec* products, it was to be hoped that the detection rates stayed the same too. This hope proved justified, as the product showed full detection of all samples in the test sets on demand. On access, however, several samples of W32/CTX and W95/SK.8044 were missed. These samples were scanned at a noticeably slow rate on demand and on access and it seems likely that the on-access scanner is timing out while processing the files.

However, the problem files did not fall in the ItW test set, and with no false positives generated a VB 100% award is owing to *SAV*.

VirusBuster VBShield 1.17

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.15%	**Polymorphic**	89.13%

Last on the list for this month's review is *VirusBuster*'s product. This is most notable in that there are far fewer comments to be made on this occasion than in the previous review. The reason is the remarkable improvement in ease of use and general user-friendliness of *VirusBuster* over the last year.

One of the major nightmares of the last review was the log format – which is now much more standard in structure. In fact, the log files of the products on offer seemed in general to be approaching a common format which required very little tinkering to be parsed into final results. The only remaining major niggle is with those products which still list files in purely 8+3 format, *VirusBuster* and *Sophos Anti-Virus* being the primary offenders.

Returning to the review, *VirusBuster* receives a VB 100% award. It takes no great leap of logic to work out that full detection was achieved In the Wild, with no false positives.

CONCLUSION

The end of another *NetWare* review signals a traditional gap in comparative reviews, with the VB Conference at the end of September, and the Christmas holidays interfering with proceedings. As such, from a reviewer's point of view at least, it seems like the end of the year. Traditionally, I gnash my teeth in frustration at the state of *NetWare* products, though the situation seems a little more positive in this case.

Of the products reviewed last year only one has vanished. The others all look to be owned by stable companies who will not give up their support for *NetWare*. The buyout of *GeCAD* and partial burial of *RAV* can hardly be considered likely to be repeated with any other developer – even if a developer were the subject of a takeover, few potential purchasers have the financial freedom simply to ditch their purchases. To a *NetWare* administrator this will come as good news. Better news, of course, will be the fact that new products have been introduced for *NetWare 6*, albeit slowly.

So the range of products is there, but what about the quality? In this I must admit to have been pleasantly surprised. Issues which made life hellish last year have simply evaporated, replaced by features which are actually useful. Some oddities remain, but the feeling that the developers simply didn't care about users no longer prevails. Of those common problems which remain, setting on-demand scans is still difficult in many cases, so there is room for improvement. It will be interesting to see whether improvement over the coming year is as significant as that seen over the last.

On a final note, in last year's *NetWare* review I predicted that this would not be the year of the *NetWare* virus. This act of soothsaying proved successful, so this year I will go a step further. Not only will this not be the year of the *NetWare* virus, but by the time the next *NetWare* review is published, *Novell* will have released another massive service pack. Check back in 12 months and evaluate my psychic powers.

Technical Details

Test environment: Server: 1.6 GHz Intel Pentium 4 workstation with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, running *NetWare 6 Service Pack 3*.

Workstation: 1.6 GHz Intel Pentium 4 workstation with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, running *Windows NT 4 Service Pack 6*.

Network: 100 Mbit ethernet.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2003/test_sets.html.

A complete description of the results calculation protocol is 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.