JUNE 2007

virus BULLETIN

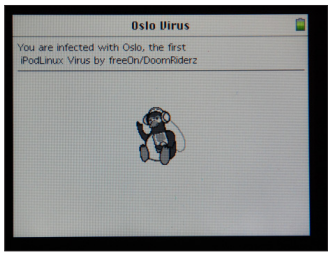
Fighting malware and spam

CONTENTS

ISSN 1749-7027

IN THIS ISSUE

HAPPY FEET



Péter Ször describes Podloso, the first *iPod Linux* virus, and looks at other possible attacks on the *iPod*.

page 4

IMPROVING THE STATUS QUO

Anti-virus researchers and testers were brought together last month in the first International Antivirus Testing Workshop. Randy Abrams summarizes the AV industry's thoughts on the current state of anti-malware testing.

page 2

VB100 REVIEW ON WINDOWS XP

A bumper crop of 37 products were submitted for this month's comparative review on *Windows XP*. John Hawes has the details.

page 10

vbSpam supplement

This month: anti-spam news & events, and Jessica Baumgart describes the lesser-known, but increasing problem of blog spam.

'Agreement was virtually unanimous that the WildList is no longer useful as a metric of the ability of a product to protect users.'
Randy Abrams, Eset

AV INDUSTRY COMMENTS ON ANTI-MALWARE TESTING

In the fine tradition of the pioneers of the anti-virus industry, the 1st International Antivirus Testing Workshop was conceived and held in Reykjavik, Iceland last month. Michael St. Neitzel, formerly of *Microsoft* and *Eset*, now working for *Frisk*, had seen one too many unacceptably bad AV tests and decided it was time to bring AV researchers and testers together to try to improve the state of malware testing.

Researchers have beaten up on testers for years with little discernable result, so the notion of such a meeting to improve the status quo may seem a little quixotic unless one realizes that the opponent the AV industry faces is not a windmill, but rather, in the words of Dr Klaus Brunnstein, its Siamese twin.

The presentations were interesting and can be found at http://www.f-prot.com/workshop2007/, however the majority of value came in the discussions that followed the presentations.

A presentation modestly entitled 'Building & leveraging white database for antivirus testing' by Mario Vuksan from *Bit9* was the sleeper. The presentation exposed not only the complexities of white-listing, but also that *Bit9* possesses an astounding data mine concerning the rate of growth of clean software. From an industry perspective it was fascinating to find out that *Bit9*, one of the sponsors of Robin Bloor's paper 'AVID (Anti-Virus Is Dead)', is a power user of anti-virus software. Bloor's rant, while firmly rooted in marketing does not depict the reality of his sponsor's situation. Despite this, *Bit9* may be able to contribute valuable false-positive feedback to the AV community for the benefit of users.

The hot topic of the event was the impending demise of the WildList. As Andrew Lee pointed out, anti-virus testing exists primarily for marketing. Myles Jordan of *Microsoft* stated that the reason the industry has hung on to the WildList for so long, and will fight to continue doing so, is because WildList testing is easy to pass. In response, *VB*'s own John Hawes posed the question: why, if WildList testing is so easy to pass, do products in each review fail to detect all WildList samples?

Agreement was virtually unanimous that the WildList is no longer useful as a metric of the ability of a product to protect users. The WildList brought a standard of scientific repeatability and credibility to testers, however if the sentiments of test and research alike are to be acted upon, the WildList will evolve or die. As if writing a dirge for the WildList, *Verizon* announced the acquisition of *Cybertrust*, ultimately the owner of *ICSALabs* and the WildList. Representatives of *ICSALabs* were conspicuous by their absence from the event. While some test organizations make little or no use of the WildList, *Virus Bulletin*, *West Coast Labs* and *ICSALabs* are well advised to work on a plan B sooner rather than later. Speculation on what would be required for a replacement included an automated system that would not rely upon human reporters.

Testers were reminded of the paramount importance of testing malware, rather than the utter garbage prevalent in some collections. Opinions were more diverse when trying to assess what malicious samples are relevant in a test, and whether non-contextual tests against active malware are acceptable. *Symantec* in particular beat the drum of testing an entire suite holistically as opposed to discrete modules.

Of particular delight to many of us was the opportunity to witness the self-proclaimed swan song of respected AV testing pioneer Prof. Dr Klaus Brunnstein, who concluded the event with a history of malware testing and urged the 'Siamese twins' to go forward in a productive manner that recognizes the symbiosis between the camps. Will this workshop make a difference? Will we see improvements in testing as a result? In a highly imperfect industry that places so much emphasis on perfection, if progress has been made it is unclear whether we will recognize it – but we are, if nothing else, persistent.

Credit is due to *AV-Comparatives.org*, *AV-Test.org*, *Virus Bulletin*, and *West Coast Labs* for the courage to enter the lion's den at dinner time!

NEWS

VULNERABILITIES GALORE

May was a month of flaw revelations, with vulnerabilities being disclosed in the products of no fewer than nine security vendors.

At the start of the month details were revealed of a vulnerability affecting *Alwil*, *Avira* and *Panda* products. The flaw involved an error in the handling of the .zoo archive format, and could have been exploited to cause an infinite loop, resulting in extreme CPU utilization or even denial of service. *Avira*'s *Antivir* product also suffered three further potentially exploitable vulnerabilities. These involved errors when processing LZH files, TAR files and UPX-compressed files.

Also in early May, *Trend Micro* released details of two buffer-overflow issues, which were thought to be exploitable only from the local system. More buffer overflows were reported in *McAfee* and *CA* products. In a wide range of *McAfee* products, a buffer overflow error in the Subscription Manager ActiveX control meant that it was possible for code to be executed from malicious websites, resulting in system compromise and remote access. A number of *CA*'s anti-virus and anti-spyware products were affected by two buffer overflows. The vulnerabilities, which could only have been exploited from the local system, could have allowed escalated privileges.

A flaw revealed in the ActiveX control of some of *Symantec*'s *Norton* products could also have been exploited by malicious websites to bypass security measures and allow remote access. It proved to be a tricky month all round for *Symantec*, with a false positive in its *Norton Anti-virus* product range rendering thousands of Chinese computers unusable after it flagged both netapi32.dll and lsasrv.dll as the Haxdoor backdoor trojan on certain Simplified Chinese language versions of *Windows XP SP2*. A number of enterprise customers are seeking compensation for losses incurred as a result of the disruption.

Back to the month's vulnerabilities: a flaw was revealed by *FrSIRT* in open source security software *ClamAV*. The flaw, which resides in the OLE2 parser, is potentially exploitable to cause denial of service. At the time of writing no official patch is available.

Finally, the end of the month saw news of vulnerabilities in *Eset* and *F-Secure* products. Two stack-overflow vulnerabilities were disclosed in *Eset*'s *NOD32 AntiVirus* product, while *F-Secure* revealed a buffer overflow relating to LHA archive handling in a number of its products.

With the exception of the *ClamAV* flaw, patches for all vulnerabilities were available prior to the announcements being made. As always, *VB* urges users to ensure they are running the latest versions.

Prevalence Table – April 2007

Virus	Type	Incidents	Reports
W32/Bagle	Worm	2,313,061	26.26%
W32/Mytob	Worm	2,154,981	24.47%
W32/Netsky	Worm	1,908,607	21.67%
W32/MyWife	Worm	811,347	9.21%
W32/Zafi	File	485,552	5.51%
W32/Virut	File	345,089	3.92%
W32/Lovgate	Worm	191,285	2.17%
W32/Mydoom	Worm	134,640	1.53%
W32/Stration	Worm	88,329	1.00%
W32/Bagz	Worm	81,849	0.93%
W32/Sober	Worm	67,233	0.76%
W32/Parite	File	50,253	0.57%
W32/Jeefo	File	44,231	0.50%
W32/Funlove	File	35,911	0.41%
W32/Klez	File	24,309	0.28%
W32/Mabutu	Worm	14,651	0.17%
W32/Bugbear	Worm	11,494	0.13%
W32/Tenga	File	6,679	0.08%
VBS/Redlof	Script	6,121	0.07%
W32/Womble	File	5,955	0.07%
W32/Valla	File	5,522	0.06%
W32/Magistr	File	3,105	0.04%
W32/Reatle	Worm	3,068	0.03%
VBS/Areses	Script	3,062	0.03%
W32/Maslan	File	2,271	0.03%
W32/Dumaru	File	1,422	0.02%
W32/Elkern	File	1,236	0.01%
W32/Dref	File	769	0.01%
W32/Plexus	File	591	0.01%
W32/Sality	File	584	0.01%
W32/Lovelorn	File	451	0.01%
W32/Rontokbro	File	362	0.00%
Others[1]		3,605	0.04%
Total		8,807,625	100%

[1]The Prevalence Table includes a total of 3,605 reports across 52 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

VIRUS ANALYSIS

ATTACKS ON IPOD

Péter Ször
Symantec Corporation, USA

'*What's wrong with your machine?*'

'Nothing, I just want to find out what type of network adapter needs to be installed in this PC to get Linux to work.'

'*Oh. What's Linux?*'

'It's an operating system developed in Finland…'

'*Aha*,' I said, and stepped outside to enjoy a cigarette at –15C .

This decade-old conversation soon came to my mind as I began installing *Linux* on my *iPod* to test run iPodLinux/Podloso, the first concept virus on this platform.

Many enthusiasts develop *Linux* for the *iPod*, which involves an enormous amount of work. One needs to reverse engineer the hardware and its firmware code to be able to build everything from the ground up. Needless to say, this is a major challenge. New hardware is released frequently with updated firmware code which is even encrypted in newer models in an attempt to discourage the *iPod Linux* developer community – but to no avail!

I love music, which explains why I have the largest collection of *iPod*s one can imagine. Although I expected *iPod* threats from the very beginning, I was not too surprised that we hadn't seen any five years after the *iPod* came out – by which time, *Apple* had sold 100 million *iPod* units worldwide.

PORTAL PLAYER

At the heart of the *iPod* is the PortalPlayer (PP) SuperIntegration System-On-Chip [1]. This is a complete digital audio system featuring dual ARM microprocessors. The PP chip supports encoding and decoding of digital audio data directly to and from flash or hard disk.

PortalPlayer also supports a PP chip with an embedded OS that includes robust development tools, enabling custom feature sets and enhancements. This chip is designed to provide support for codecs and DRMs, and is amazingly capable. Among many other features, it supports real-time encoding of MP3 and ACELP.NET audio formats, as well as real-time decoding of MP3, WMA, AAC and ACELP.NET formats.

'I WANT MY KENOO!'

iPod devices come in a variety of flavours today, but the traditional systems have the basic bootstrap code in flash ROM, which reads the *Apple* application firmware stored on the disk and jumps to it. Obviously, this process can be hijacked just as easily as any other system's boot process, and this is precisely what *Linux* does on the *iPod*. It puts a little extra boot code in place, which will optionally direct control either to *Apple*'s own firmware or to the *Linux* firmware to run either the apple-app UI, or first the *Linux* kernel, and then the *Podzilla* UI shell on top of it.

Obviously, there is a checksum function to verify that the content of *Apple*'s application is not altered. This checksum can easily be changed. All this is stored in a little partition of its own, starting typically at logical block 63, in the format of a simple file system. Not surprisingly, several versions of utilities have been released for the *iPod*, which can change the firmware resources and thus replace the familiar icons with the user's choice.

The newer release of the firmware partition starts with a volume header, which has a pointer to a directory structure. The directory entry of the bootloader image contains the checksum of the file, as well as its start address on the disk.

Linux on the *iPod* saves a copy of the original firmware, and patches itself into the boot process by extending the original firmware code with its boot code and itself. Finally, it sets a new checksum in place.

It is plain to see that hostile code could also update itself into the firmware with extra code. This is exactly why I expected to see security threats, including viruses (worms), on the *iPod*. The *iPod* is basically a general computer which lacks documentation, and an open programmable API.

The format of the file system is either HFS+ or FAT32, depending on the host OS and the initial installations. In the end, with a bit of luck, you can install all the cool games that come with *Linux*. You can even install *Nintendo NES* games, which may come in handy when your two-year-old gets tired of *Brick* on his own *Nano* (or 'Kenoo!').

INITIALIZATION

The early versions of *Podzilla* were not modularized. As a result, Podloso does not really have a chance to replicate on them – since it will not be loaded dynamically, but only by placing the virus in the module folder, for example with the installation of a game. The virus does not have any means to

jump from the desktop to the *iPod* on its own, but as explained above, this could potentially be done. The most obvious method of attack is to install *Linux* on the connected *iPod* via a desktop-compatible virus, thus taking over the *iPod* world with *Linux* on the way. However, direct attacks could also be carried out.

Podloso is limited to *Podzilla* version 2. Early releases do not support module loads from /usr/lib/ folders dynamically, loading them instead during startup. Each module is in 32-bit ELF format and contains native ARM code. The ELF file is a relocatable image library stored with a .mod.o extension, and functions much like a DLL.

Modules are loaded by the pz_module_init() function of *Podzilla 2*. If a file named 'Module' is available with little information about its content, it will be loaded as long as the file appears to be compatible with the *Podzilla* release. In such a case, the init function of the module is triggered immediately after loading the module. In Podloso, this function is init_oslo(), which will follow the standard module format. It simply installs a menu handle with the name '/Extras/Demos/Oslo', so the user will be able to run it later on. The virus follows the standard method to run a module, although this is not necessary.

Podloso requires the installation of its main file, the 6128-byte oslo.mod.o, into a folder under /usr/lib/. In addition, there is a module file, as well as a picture file called image.png, which need to be available in the same folder in order for the virus to execute its payload correctly.

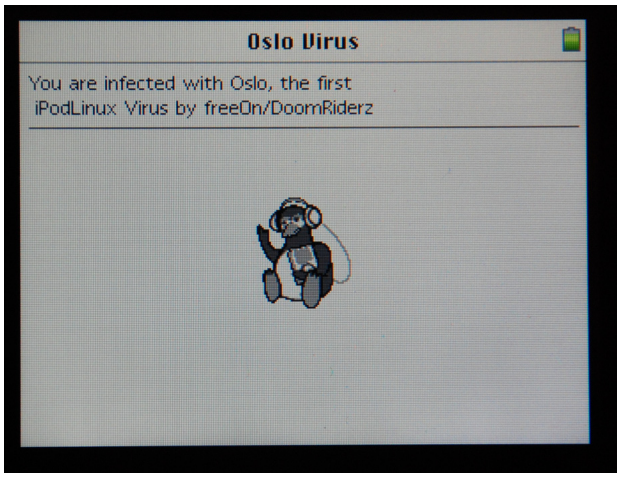
EXECUTION AND INFECTION

When the user executes the Oslo module, the virus is triggered. The infection routine is very simple. It searches recursively for new files with .mod.o extensions to infect, which appear to be in ELF format according to their header.

Podloso is a little like a library infector, but it does not infect the library files properly. For each file, the virus copies itself to the top of the host program, just like a prepender virus, saving the original ELF module content after itself, and placing an 'Oslo' infection marker after that.

Eventually, all modules will have a copy of the virus at the start, and the content of the original module will no longer run. After running the virus, therefore, only one module name will be registered: that of the virus itself. However, *Podzilla* will dutifully display all the module names according to the text of module files, as if they loaded normally. In some versions of *Podzilla*, a number of error messages will be displayed.

It should be noted that the virus ignores read-only files, thus the file system flags could be used to help avoid infection.



PAYLOAD TROUBLES

Immediately after the infection function finishes, the virus is supposed to trigger its payload, which is to display a window showing a penguin and a short message. So far, however, only Konstantin Sapronov of *Kaspersky Lab* has been lucky enough to capture this elusive moment [2], which he says was often followed by a *Linux* crash on his 5.5 generation *Video iPod*.

I have installed *Linux* on each of the more than half-dozen different *iPod* editions that I currently own, and even made use of my friend's devices [3]. On all of these releases I have attempted to bring *Podzilla* to the most recent version after installing the latest supported edition of the *Linux* kernel. On several of the devices, I got a warning from the installer stating that I was practically on my own, since they are not completely supported devices.

Only on a traditional *iPod Mini* edition did I finally achieve what seemed to be successful installation, with no warnings displayed. Yet as soon as the payload ran, either the virus hung or *Linux* crashed, displaying the system console on screen.

The error seems to be related to SDL, the graphical window library, which suddenly 'deploys parachute'. In turn, the clean-up routine of the virus, cleanup_oslo(), is triggered by the exception handling, and the virus prints the following message to the console:

```
greetz:genetix,necro,wargame
```

After this, *Linux* needs to be rebooted.

It is possible that newer, unsupported kernel editions could resolve these problems, and this may be why the virus does work in certain environments. However, in most cases, Podloso will simply crash in the installations that people are most likely to be using. This says a lot about how difficult it

is to support code on an unknown platform with all kinds of firmware flavours. The virus always infects each module on the device, regardless of the troubled payload routine.

Evidently, the virus is *iPod*-specific. Not only does it require *iPod Linux* to run, but it also requires the *Podzilla 2* environment, since it is a *Podzilla 2* module itself.

POSSIBLE ATTACKS

In this short section, I will discuss some of the attacks that have been carried out, or could be carried out, utilizing *iPod* devices.

USB ATTACKS

The earliest attacks simply used the *iPod* as a USB disk drive, placing startup files on the execution path in the hope that a program or script will be triggered from the *iPod* upon its connection to the host. Such attacks typically look for confidential information to steal from the host. An *iPod* with a large hard drive can be used by an attacker this way to 'backup' data quickly, and do so by gaining physical access to the host system.

DRM

Although Podloso is clearly a simple concept virus, it is certainly possible to make viruses that spread from desktop systems to the *iPod*. One can easily imagine that there would also be a number of opportunities for a host system to be infected from an *iPod*.

For example, people often borrow music from each other, using the *iPod* in hand-managed mode, instead of letting *iTunes* synchronize directly. Currently, the DRM settings seem to be strong enough in the newest *Shuffle* editions to disallow the copying of music from several hosts to a single device. In other editions, however, this is certainly an option, allowing people to exchange music. Details of how to find the music folder on the *iPod* and copy it back to the desktop are already common knowledge, and one can easily use the *Terminal* program, by dragging the *iPod* icon to it, to browse the music folders. These are not usually synchronized back to the host by *iTunes* to reduce music piracy.

FIRE OVER THE WIRE

The early editions of *iPod* can synchronize data very quickly, utilizing *Apple*'s *Firewire* standard. Back in 2004, a vulnerability was discovered in *Firewire* interfaces [4]. The vulnerability resides in the handling of host memory access (including PCI RAM), which is directly available to the connected *Firewire* devices, such as the *iPod*. During data transfers the device is supposed to read and write in the designated DMA memory range that the host indicates. However, the device can decide to read and write outside of these areas and thus, according to its will, modify the host's kernel memory as a result.

It would be the duty of the host to disallow access to outside regions, but this is not typically enforced by operating systems. For example, *Mac OS X* kernel (prior to 10.3.9 releases) could be modified directly by a connected *iPod* device. In 2005, another paper reported that a *Linux iPod* port of such an attack tool already existed [4].

Using *iPod Linux*, it is trivial to access the host for modification, and even plant a rootkit, or possibly a virus, back on the connected host machine. In addition, dumping of physical memory – a process known as memory imaging – can be performed, alongside memory modifications. Although *Windows 2000* crashes, and other releases such as *Windows XP* do not support direct DMA for *Firewire*, the attack can still be achieved under certain conditions. It must also be noted that *Firewire* DMA can be disabled on *Mac OS X*, for example by setting an open firmware password [5].

ITUNES AND GNU-TUNES ATTACKS

As expected, there are possible ways to simulate communication between an *iPod* and *iTunes*, and perhaps via those interfaces exploit vulnerabilities from the *iPod* on the host machine. A variety of *iTunes* vulnerabilities are already known today. In addition, there are releases of *gnu-Tunes*, to support music libraries on other operating systems.

Thus, a multi-platform concept is certainly possible. A virus (worm) could jump to the *iPod* and then back to the desktop to exploit new targets all over again.

IPOD IN A COMA

Obviously, the basic recovery of the *iPod* is supported by the device itself. Key combinations can be utilized to put the *iPod* into disk mode, and then the host can restore the *iPod* to its original state, cleaning up all the cool music and stuff on the way.

However, once code is running on the *iPod*, the key combination could be hooked by hostile code in such a way that one could not easily trigger the disk mode. In addition, there are many firmware nuances. Years ago, when I first thought about the possible attacks against *iPod* devices, I talked to the lead developer of the *iPod Linux* kernel. He

told me that during the discovery stages they played with the sleep function of the *iPod* firmware code, and accidentally put *iPod*s into comas, with no chance of waking them. When you do not use your *iPod* for a short period of time, it goes into a light sleep, allowing it to be turned back on more quickly. However, after a prolonged period of time without use, the device goes into a deep sleep, from which it will boot more slowly. Apparently, this deeper sleep will turn into a coma state if the function is called with the incorrect parameters. No wonder the *iPod Linux* developers need continuous donations of *iPod* devices to keep their operations running!

CONCLUSION

We are currently waiting for the release of the exciting *Apple iPhone* which, according to *Apple*, supports a micro *Mac OS X* kernel.

The *iPhone* will borrow from the *iPod* in many ways, so it will be interesting to see how these threats develop further, once attackers are facing wireless devices with additional personal information stored on them.

Supposedly, the *iPhone* will have additional security features beside DRM, but the ability to get around these safeguards is already on the horizon. For the moment, the *iPhone* is reportedly a closed device – at least as much as the *iPod* is today. It is very likely that the *iPhone* will also use code signing to verify new modules. However, the pressure will be huge on *Apple* to support the device with an open API in the future.

REFERENCES

[1] http://www.arm.com/.

[2] Konstantin Sapronov, personal communication.

[3] Ilan Terrell, personal communication.

[4] http://md.hudora.de/presentations/firewire/2005-firewire-cansecwest.pdf.

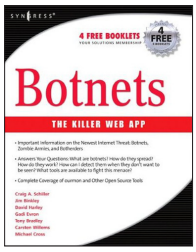
[5] http://www.ccc.de/congress/2004/fahrplan/files/95-macosx-insecurity-paper.pdf+firewire+vulnerability&hl=en&ct=clnk&cd=4&gl=us.

[*Marius van Oers will present a paper on Apple Media Files and the iPhone at this year's Virus Bulletin conference in Vienna (19–21 September). For the full programme details, including abstracts for all papers, as well as online registration, see http://www.virusbtn.com/conference/vb2007/.*]

BOOK REVIEW

LET'S KICK SOME BOT!

Martin Overton
Independent researcher, UK



Title: Botnets – The Killer Web App
Author: Craig A. Schiller, Jim Binkley et al.
Publisher: Syngress
ISBN: 1-59749-135-7
Cover Price: $49.95

This book covers what has become a hot topic in the security community since the move by cybercriminals and spam gangs towards business models that involve building and exploiting vast numbers of 'zombie' machines scattered all over the globe. These machines are infected by bots and collected, used, rented and traded by cybercriminals.

So, what does the book cover, and more importantly, does it deliver on the promises it makes?

COVER STORY?

The book's cover claims that it will provide:

- Important information on botnets, zombie armies and bot herders.
- Answers to your questions: What are botnets? How do they spread? How do they work? How can I detect them when they don't want to be seen? What tools are available to fight this menace?
- Complete coverage of *ourmon* and other open source tools.

UNDER THE COVERS

The book contains 12 main chapters and a single appendix. Each chapter starts with what *Syngress* calls 'Solutions in this chapter' (even when the chapter is all about threats, not solutions), and concludes with a summary, FAQ and a 'Solutions fast track' section.

Chapter 1 discusses why the botnet is such a powerful tool (or toolkit). The authors state: 'The software that creates and manages a botnet makes this threat much more than the previous generation of malicious code. It is not a virus; it is a virus of viruses.' I beg to differ: most (if not all) bots are not viruses at all; most are remote access trojans (RATs) or worms.

The next section offers a concise look at 'A conceptual history of botnets', which starts with the birth of IRC itself and GM, the first IRC bot. Next stop is PrettyPark, which the chapter's author claims is the prototype for today's bots.

SubSeven is also mentioned before we move to what I consider to be the real prototypes of modern bots: GTbot and the grand-daddy of most modern bots, SDbot (the first bot to be written in C/C++ and most importantly, its source code was made available). Other bots covered in this section are the usual suspects: Agobot, Spybot, Rbot, Polybot and finally Mytob.

BOTNETS FOR DUMMIES

Moving on, we come to 'Cases in the news', which covers the stories of some of the cybercriminals who have successfully been prosecuted, such as: THr34t-Krew, Axel Gembe and Resili3nt (aka Jeanson James Ancheta) and Farid Essebar (the author of Zotob), amongst others.

Wrapping up Chapter 1 is 'The industry responds', a section covering a brainstorming session in August 2006 – almost a year after the VB2005 conference at which a number of papers on bots and botnets had been presented and a lot of brainstorming and discussion of the problem had taken place.

Chapter 2 continues with the same 'botnets for dummies' approach and covers: 'What is a botnet?', 'The botnet life cycle', 'What does a botnet do?' and 'Botnet economics'. All in all, this is quite a good overview of bots and botnets for those who haven't come across them before and need to know the fundamentals.

Chapter 3 introduces the reader to 'Alternative botnet C&Cs', starting with a look at the 'Historical C&C technology as a road map' and continuing this voyage of discovery with 'DNS and C&C technology' (which is more useful as it covers newer techniques that are increasingly being used in place of traditional IRC command and control infrastructures). These include web-based, command-based, P2P and IM command and control systems or infrastructures. It also includes some of the advanced DNS techniques, such as dynamic and fastflux DNS records which allow botnet C&Cs to be more resilient than previously when they tended to use hard-coded IP addresses in the bots' bodies or configuration files.

Chapter 4 covers common botnets and includes a more in-depth look at Sdbot, Rbot, Agobot, Spybot and Mytob, detailing known aliases, infection, signs of compromise such as common registry keys, filenames, ports and propagation techniques used.

Chapter 5, 'Botnet detection: tools and techniques', opens with 'Abuse', or to put it another way, emails to your 'abuse@company.com' address complaining that your domain is doing something bad, such as spamming, phishing, DDoSing or hosting malware/spyware or other bad stuff. For many, this will be the first clue that part of their network is under someone else's control.

The next section, 'Network infrastructure: tools and techniques', covers the likes of SNMP, netflow, firewalls, switches, hubs, routers and the use of ACLs and logs from these types of devices/services.

Intrusion detection is the next area to be discussed, including some coverage of anti-virus, with information on signatures and heuristics. *Snort* is covered in some detail as an example IDS, along with a number of example signatures which are dissected and explained well. Integrity management systems are also covered.

Some material on darknets, honeypots and 'other snares' is then given, before the rest of the chapter covers in more detail how you can use the tools/techniques mentioned in the first half of the chapter to fight back.

BOTNETS FOR TECHIES

Chapter 6 offers an overview of *ourmon*, starting with some case studies and then explaining how it works and how it is installed. In a nutshell, *ourmon* is a network-monitoring tool that the author claims can be used for 'low-level anomaly detection and higher-level detection of botnets'.

Chapter 7 covers *ourmon*'s web interface as well as using it to detect TCP, UDP and email anomalies. In my opinion, chapters 6 and 7 are not suitable for those with little or no computer security/network experience.

Chapter 8 discusses the IRC protocol, then moves swiftly on to 'Ourmon's RRDTOOL statistics and IRC reports'. The chapter is wrapped up with 'Detecting an IRC botnet' and 'Detecting an IRC botnet server'. Chapter 9 is also dedicated to what seems to be the authors' favourite tool. This time it covers advanced *ourmon* techniques. As with the previous *ourmon* chapters, this would not be suitable for non-techies.

Chapter 10 covers the use of sandbox tools. It starts by explaining what a sandbox is and mentions not only a number of well-known sandboxes, but also 'real' systems and virtual machines used for the same purpose, rather than the emulated ones that sandboxes usually use. The rest of the chapter focuses on one of the better-known sandboxes, *CWSandbox*, which is described as 'an application for the automatic behaviour analysis of malware' – a good description of what it does. Yet again, though, this is not suitable for non-techies.

Chapter 11 is entitled 'Intelligence resources', and identifies the information that an organisation should try to gather. It also covers disassemblers (although why this is included here rather than in chapter 5 or 10 is beyond me). Next, a list of places/organizations that provide information about botnets is provided. The short list includes anti-virus and

anti-spyware sites as well as *Microsoft*'s security site. A list of 'Professional and volunteer organizations' includes a number of mailing lists as well as groups such as NANOG, APWG and UNISOG. Interestingly, there is no mention of AVIEN or AVIEWS.

Finally, chapter 12 is entitled 'Responding to botnets'. Here, the authors state that 'giving up is not an option', which seems to be at odds with the data on the front and back covers and in the book's own introduction. Another section asks 'Why do we have this problem?', which may have been more useful at the start of chapter 1. The usual suspects are named: phishing, spam and money, as well as touching on policies and processes (or lack thereof) within organisations.

The final section asks 'What is to be done?', which is a good question, but it's a shame they left it to the last chapter to try and answer it. The answers offered include effective practices for individual and enterprise computer users as well as reporting botnets to some or all of the groups mentioned in the previous chapter. The section is completed with 'Fighting back', which covers the saga of *Blue Security*, and 'Law enforcement', which details how to report a botnet (although no suggestions are given for those of us outside the US). It swiftly covers darknets, honeynets and botnet subversion in very little detail and finishes with 'A call to arms'.

CONCLUSIONS

This book is very good in parts; chapters 5 and 10 are excellent. Chapters 1 to 4 are a good introduction to the subject and could easily have been extended into a 'botnets for dummies' type of book. However, chapters 6 to 9 are far too technical for a non-techie or a techie that doesn't have lots of security and network knowledge/experience.

I'm left with a strong impression that this book was rushed to market, as it seems to be two books in one. The really technical stuff and the *ourmon* chapters belong in an advanced book, while the rest of the material could easily have been expanded and sold as an introductory or intermediate-level guide (in my opinion this would have been a significantly better move by the publishers).

As it stands, the book will be of no real use to those not already in IT or security with at least a year of real hands-on experience, and I suspect that the 'propeller-heads' won't get much out of it either, apart from the material on *ourmon*. However, as a single reference tome, it will end up on many bookshelves in organisations worldwide.

Things may improve if and when the book is revised, or another publisher comes up with another book on botnets. Until then it will be a one-horse race, so for now this book is the de facto winner.

COMPARATIVE REVIEW

WINDOWS XP SP2

John Hawes

It became clear several months prior to this year's *Windows XP* comparative review that it would be a popular test. Vendors of a number of new products who were interested in putting their software forward for the VB100 certification had been in discussion with us for some time, with timing or platform issues having prevented their entry into earlier tests. Meanwhile, the broad popularity of the *XP* platform as much as guaranteed that all the regular VB100 entrants would support it. With a handful of further new arrivals appearing in the weeks before the deadline, this proved to be a truly bumper crop, well outstripping previous records.

In a month that incorporated two national holidays, as well as my attendance at the *Frisk* Antivirus Testing Workshop to keep me from the test lab (see p.2), I anticipated some long days to get the comparative completed in time – particularly with so many new and unfamiliar products with which to wrestle. I could only hope for simple and responsive interfaces, rapid scanning times and clear and straightforward results.

PLATFORM AND TEST SETS

Windows XP, first released with quite some fanfare in late 2001, came rapidly to dominate the home-user market with its advances over *Windows 98* and *ME*, and has also made steady inroads into the corporate sphere. The release of Service Pack 2 (SP2) in mid-2004, with some serious security improvements including the Windows Firewall and the Security Center, has boosted the platform's popularity and stability and made it almost a global standard. With a third service pack expected some time next year, and *Windows Vista* still at the start of a long settling-down period before it becomes widespread, *XP* is sure to remain dominant for some time yet.

Setting up *Windows XP* has become a simple process for me after having repeated the task many times over the years, and all the familiar controls and settings are easy to find and use. The *Professional* edition was used for testing purposes, in case any of the corporate products required domain membership or any of the other add-ons not available in the home edition. With SP2 rolled into the installer I used, little further tweaking was required once the systems were running and talking to the test lab network.

Beyond the expansion of the WildList test set and a host of additions to the clean sets, the test collections remain fairly stable. The WildList used to compile the test sets – the February 2007 version released in mid-April – had a relatively small number of additions, which were dominated by W32/Sdbot and W32/Rbot variants, with a large number of older items falling from the list after a lengthy tenure. Most interesting among the additions were the file infectors, some more of the W32/Looked (aka Viking) variants that have been appearing in recent months, as well as W32/Fujacks (aka the Panda Burning Incense virus, among other bizarre names picked up in its flashes of media popularity).

I hoped again to include some more detailed speed test results, although I anticipated there being several products that would not fit into the testing methodology (especially regarding on-access tests where different products behave in wildly different ways when files are simply opened, copied, written to etc., rather than fully executed).

For the archive tests, I planned once more to test both with the default settings and with archive scanning switched on, to try to show reasonably equal measures across products. Again, I expected some products not to offer this level of configuration, and results are presented only in as much depth as it was possible to gather in the available time.

AEC Trustport Workstation Antivirus 2.5.0.970

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Trustport Anti-Virus is available as a component of the broader *Trustport* suite, which was reviewed in *VB* in some depth a couple of months ago (see *VB*, March 2007, p.13). The installation was thus a familiar affair. Halfway through the installation I was reminded to ensure that I had no other anti-virus solutions installed on my machine – quite a reasonable request since the four engines included with the product (*BitDefender*, *Ewido*, *Grisoft* and *Norman*) should be more than adequate for anyone.

No reboot was required at the end of the installation, and red shield and blue gem icons installed to the system tray indicated that protection was running smoothly. Accessing the configuration options from here, I found the interface sensible and highly responsive, and had on-access scanning temporarily disabled, the logging settings tuned up and the first on-demand scan under way in a matter of seconds.

With all four engines deployed for the on-demand mode, speeds were never likely to be as impressive as detection rates, but on access only two engines are in use and the slowdowns are not too severe.

On-access tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
AEC Trustport Workstation Antivirus	0	100.00%	0	100.00%	2	99.78%	0	100.00%	0	100.00%	0	100.00%		
Agnitum Outpost Security Suite Pro	18	99.55%	2	99.34%	30	99.33%	26	97.20%	19	99.61%	97	87.82%		
AhnLab V3 Internet Security 2007	17	99.79%	3	99.52%	652	97.40%	31	95.62%	47	98.97%	84	92.83%		
Alwil avast! Professional Edition	0	100.00%	1	99.67%	238	99.12%	14	97.85%	18	99.56%	243	85.35%		1
Authentium Command AntiVirus for Windows	0	100.00%	2	99.63%	0	100.00%	2	99.49%	0	100.00%	0	100.00%		
Avira AntiVir	0	100.00%	0	100.00%	32	99.78%	0	100.00%	0	100.00%	3	98.72%		
Bullguard	0	100.00%	0	100.00%	11	99.44%	3	98.22%	21	99.49%	11	97.55%		
CA AntiVirus	0	100.00%	0	100.00%	366	99.57%	3	99.34%	0	100.00%	20	92.15%		
CA eTrust	0	100.00%	0	100.00%	366	99.57%	3	99.34%	12	99.82%	20	92.15%		
CAT Quick Heal AntiVirus 2007	0	100.00%	0	100.00%	1193	90.57%	21	96.44%	82	98.04%	389	76.11%		
Doctor Web Dr.Web	6	99.33%	0	100.00%	0	100.00%	3	98.73%	0	100.00%	3	98.72%		5
eEye Blink Personal Edition	0	100.00%	1	99.67%	118	99.74%	11	98.47%	4	99.90%	274	81.94%		1
Eset NOD32 Antivirus System	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-Prot Anti-Virus	0	100.00%	1	99.67%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
F-Secure Protection Service for Consumers	1	99.88%	1	99.96%	0	100.00%	2	99.49%	0	100.00%	0	100.00%		
G DATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Grisoft AVG Professional Edition	1	99.88%	3	99.52%	264	99.29%	16	96.93%	3	99.93%	190	75.88%		
Ikarus Virus Utilities	4	99.88%	1	99.89%	2995	92.32%	45	92.82%	176	95.86%	378	71.00%	22	1
iolo AntiVirus	2	99.86%	2	99.63%	1	99.93%	0	100.00%	85	98.60%	20	96.15%	1	
K7 Total Security 2006	0	100.00%	11	97.29%	3621	88.20%	44	92.36%	153	97.23%	863	61.19%		
Kaspersky Anti-Virus	1	99.88%	0	100.00%	0	100.00%	2	99.49%	0	100.00%	0	100.00%		
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	64	99.85%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront Client Security	0	100.00%	0	100.00%	1	100.00%	5	98.54%	0	100.00%	29	96.15%		
Microsoft Windows Live OneCare	0	100.00%	0	100.00%	1	100.00%	5	98.54%	0	100.00%	29	96.15%		
Microworld eScan Internet Security for Windows	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Norman Virus Control	0	100.00%	1	99.67%	118	99.74%	9	98.97%	0	100.00%	274	81.94%		
NWI VirusChaser	9	98.90%	1	99.67%	121	99.18%	3	99.24%	4	99.90%	9	97.82%		7
PC Tools Antivirus	0	100.00%	0	100.00%	39	99.10%	9	98.46%	0	100.00%	107	87.74%		
PC Tools Spyware Doctor	0	100.00%	0	100.00%	152	98.88%	9	98.46%	3	99.93%	107	87.74%		
Proland Protector Plus 2007	21	97.93%	13	96.19%	11912	78.53%	104	82.74%	712	82.53%	1376	36.97%	2	
Softwin BitDefender Antivirus Plus	0	100.00%	0	100.00%	8	99.78%	3	98.22%	13	99.69%	5	97.86%		
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	0	100.00%		
Symantec AntiVirus	0	100.00%	0	100.00%	4	99.97%	0	100.00%	0	100.00%	0	100.00%		
Trend Micro PC-cillin Internet Security 2007	0	100.00%	0	100.00%	233	99.53%	21	96.88%	13	99.68%	150	93.10%		
VirusBuster VirusBuster Professional 2006	0	100.00%	1	99.96%	28	99.55%	11	97.96%	0	100.00%	97	87.82%		
Webroot Spy Sweeper	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		

With splendid detection throughout and not a false positive in sight, *Trustport* gets this bumper comparative off to a good start with a very well deserved VB100 award.

Agnitum Outpost Security Suite Pro

ItW	99.92%	**Worms & bots**	100.00%
ItW (o/a)	99.55%	**DOS**	99.55%
File infector	99.24%	**Macro**	100.00%
Polymorphic	87.82%	**False positives**	0

The first of the barrage of newcomers to join the test this month, *Agnitum*'s product is an expansion of its well-known firewall offering, with virus detection provided by the *VirusBuster* engine.

Installing the product was a fairly straightforward affair, although I was asked if I wanted 'Advanced' protection (recommended for more experienced users) or a 'Normal' level (suitable for all). Since the advanced option was selected by default, I went with this mode. I was also offered an option to enable 'SmartScan', which is a system that can be used to speed up scanning using checksums of known good files, stored in hidden files. This I turned down for fairness in the speed tests, and a number of other setup options were trundled through before I could get my hands on the product proper.

The interface itself is attractive, with a tree menu showing its core functions and the product's various 'plugins', of which the 'anti-malware' section was, of course, the most interesting to me. Each has its own configuration section, some stretching to several tabs, and some detailed status information was also provided.

Scanning was performed with ease, generally from the handy context-menu link, and was fast and stable. On-access protection was similarly solid and reliable. Detection across the zoo sets was in line with the results I would expect from the engine used, but some strange behaviour was encountered in the WildList set. Two samples, both with .pif extensions, were missed in the on-demand scan, and four different items, including a full set of one of the W32/Fujacks variants, were missed on access. This behavioural oddity spoils *Agnitum*'s chances of a VB100 at first attempt, but this product seems a likely contender for the award in future tests.

AhnLab V3 Internet Security 2007

ItW	99.79%	**Worms & bots**	99.52%
ItW (o/a)	99.79%	**DOS**	97.40%
File infector	95.65%	**Macro**	98.97%
Polymorphic	92.83%	**False positives**	0

AhnLab has been a regular and successful entrant in *VB*'s comparative reviews over the last few years, and it was no surprise to see *V3* back on the test bench after a brief absence. The *Internet Security* suite includes the usual firewall, web and email protection facilities, from which a selection of required components could be made during installation, which also offered a pre-install scan and was ready to go without rebooting.

Initial impressions of the GUI were very good: it looked slick and attractive, with a prominent 'Settings' button promising easy access to all the required controls. Attempting to run a few scans proved a little less straightforward than I had hoped, due to the requirement to set up a job and then run it, but a 'Run a virus scan' option was added into context menus, making speed testing much easier.

Scanning speeds themselves were on the slow side on demand, especially with the option to scan archives enabled, but on-access speeds were remarkably fast, with little control of the depth of scanning available for this mode.

Logging has proved problematic with *AhnLab* products in the past, and this occasion was no exception. Logs saved from the Log Viewer utility were invariably truncated to an apparently random size, but usable figures were obtained eventually, after splitting the scans into several sections. These, and the results of on-access blocking, showed samples to have been missed in all test sets, though not in vast numbers. In the WildList set three separate items were not detected, including the polymorphic W32/Polip.A, of which all 15 samples were missed, thus denying *AhnLab* a VB100 this time around.

Alwil avast! v.4.7 Professional Edition

ItW	100.00%	**Worms & bots**	99.67%
ItW (o/a)	100.00%	**DOS**	99.34%
File infector	98.29%	**Macro**	99.56%
Polymorphic	85.35%	**False positives**	0

Alwil's *avast!*, one of the best-known names in the home-user field thanks to the widely used free versions, is another regular in *VB* comparatives, and little was changed here from previous visits. As usual, the rather funky basic interface was avoided for most tests, with the 'Advanced' control system providing ample functionality.

Again the system for setting up scan tasks proved a little fiddly for my purposes, but my familiarity with the interface has begun to pay off and the tests were completed quickly. Speeds were middling throughout, and detection likewise – neither flawless nor disappointingly lacking.

On-demand tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
AEC Trustport Workstation Antivirus	0	100.00%	0	100.00%	2	99.78%	0	100.00%	0	100.00%	0	100.00%		
Agnitum Outpost Security Suite Pro	2	99.92%	0	100.00%	48	99.55%	8	99.24%	0	100.00%	97	87.82%		
AhnLab V3 Internet Security 2007	17	99.79%	3	99.52%	652	97.40%	31	95.65%	47	98.97%	84	92.83%		1
Alwil avast! Professional Edition	0	100.00%	1	99.67%	236	99.34%	12	98.29%	18	99.56%	243	85.35%		1
Authentium Command AntiVirus for Windows	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Avira AntiVir	0	100.00%	0	100.00%	32	99.78%	0	100.00%	0	100.00%	3	98.72%		
Bullguard	0	100.00%	0	100.00%	11	99.44%	3	98.22%	21	99.49%	11	97.55%		
CA AntiVirus	0	100.00%	0	100.00%	366	99.57%	1	99.85%	0	100.00%	20	92.15%		
CA eTrust	0	100.00%	0	100.00%	366	99.57%	1	99.85%	12	99.82%	20	92.15%		
CAT Quick Heal AntiVirus 2007	0	100.00%	0	100.00%	1193	90.57%	21	96.44%	82	98.04%	389	76.11%		
Doctor Web Dr.Web	6	99.33%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	98.72%		5
eEye Blink Personal Edition	0	100.00%	1	99.67%	118	99.74%	10	98.73%	4	99.90%	274	81.94%		1
Eset NOD32 Antivirus System	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-Prot Anti-Virus	0	100.00%	1	99.67%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
F-Secure Protection Service for Consumers	1	99.88%	1	99.96%	0	100.00%	2	99.49%	0	100.00%	0	100.00%		
G DATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Grisoft AVG Professional Edition	0	100.00%	2	99.56%	264	99.29%	14	97.41%	3	99.93%	190	75.88%		
Ikarus Virus Utilities	4	99.88%	1	99.89%	2995	92.32%	45	92.82%	176	95.86%	378	71.00%	22	1
iolo AntiVirus	1	99.97%	2	99.63%	1	99.93%	0	100.00%	85	98.60%	20	96.15%	2	
K7 Total Security 2006	0	100.00%	10	97.34%	3110	88.65%	33	93.63%	153	97.23%	368	65.00%		
Kaspersky Anti-Virus	1	99.88%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	64	99.85%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront Client Security	0	100.00%	0	100.00%	1	100.00%	2	99.81%	0	100.00%	29	96.15%		
Microsoft Windows Live OneCare	0	100.00%	0	100.00%	1	100.00%	2	99.81%	0	100.00%	29	96.15%		
Microworld eScan Internet Security for Windows	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Norman Virus Control	0	100.00%	1	99.67%	118	99.74%	9	98.97%	0	100.00%	274	81.94%		
NWI VirusChaser	9	98.90%	1	99.67%	121	99.18%	3	99.24%	4	99.90%	9	97.82%		7
PC Tools Antivirus	0	100.00%	0	100.00%	39	99.10%	9	98.46%	0	100.00%	107	87.74%		
PC Tools Spyware Doctor	0	100.00%	0	100.00%	152	98.88%	9	98.46%	3	99.93%	107	87.74%		
Proland Protector Plus 2007	3	99.76%	4	98.89%	11912	78.53%	98	84.84%	712	82.53%	1376	36.97%	2	
Softwin BitDefender Antivirus Plus	0	100.00%	0	100.00%	8	99.78%	2	98.97%	13	99.69%	5	97.86%		
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Symantec AntiVirus	0	100.00%	0	100.00%	4	99.97%	0	100.00%	0	100.00%	0	100.00%		1
Trend Micro PC-cillin Internet Security 2007	0	100.00%	0	100.00%	233	99.53%	13	98.91%	13	99.68%	150	93.10%		
VirusBuster VirusBuster Professional 2006	0	100.00%	0	100.00%	28	99.55%	8	99.23%	0	100.00%	97	87.82%		1
Webroot Spy Sweeper	0	100.00%	0	100.00%	0	100.00%	0	100.00%	6	99.93%	0	100.00%		

The product's reliability was carried over into the WildList set where nothing was missed, and likewise the clean sets, where only the usual single file labelled a 'Joke' required noting. As a result, *Alwil* is once again the worthy winner of a VB100 award.

Authentium Command AntiVirus for Windows 4.94.5

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Authentium is another fairly regular participant in *VB*'s tests, with a false positive issue in last October's test the first blot for several years on an otherwise impressive test history (see *VB*, October 2006, p.10). The company focuses on 'software as a service', but continues to sell the *Command* software both as a standalone product and as part of a suite including a firewall and so on.

The product itself is a simple little thing; installation seemed to spend some time pondering its surroundings, before suddenly announcing completion, and opening the GUI showed a tiny and unflashy but potent little tool. In a simple-to-use manner, it offered all the required tweaking, apart from the ability to add archives to the file types scanned on access, and zipped through the tests in excellent time.

Detection rates were similarly excellent, with barely a miss across the board, and the few missed detections were due to the file types not scanned by default. This performance, coupled with a complete absence of false positives, easily qualifies *Authentium* for another VB100.

Avira AntiVir

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	100.00%	**Macro**	100.00%
Polymorphic	98.72%	**False positives**	0

Avira is another perennial high achiever in VB100 terms, and its product is another which grows pleasantly familiar with repeated use. In this case, however, familiarity adds little to the product's ease of use, since it is well designed and easy to use from the outset.

A few things I had not spotted before include the whimsical title 'Luke Filewalker' given to the scanner screen, which started a scan of my system automatically after installation and had to be stopped. Several other products also carried out this auto-check, while most others offered the option of a thorough scan once they were ready to go – an option I always decline for the purposes of these tests.

AntiVir's slogan promises 'More than security', and I certainly felt secure looking at the admirable detection figures, with a only a tiny handful of misses – mostly an obscure and ancient DOS virus – and splendid speeds across the board.

Again, archives could not be scanned on-access, but this does not detract from the excellent results, easily earning *Avira* another VB100 award.

Bullguard v.7.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.44%
File infector	98.22%	**Macro**	99.49%
Polymorphic	97.55%	**False positives**	0

The second newcomer to the *VB* test bench this month is from *Bullguard*, a company founded in Copenhagen in 2001. *Bullguard*'s *Internet Security* suite has been available for around five years, offering a firewall, spam filter, anti-spyware and a backup system alongside virus detection provided by the *BitDefender* engine. The company boasts over 18 million downloads of its 60-day free trial, and also offers mobile products and chat-based online support.

The product itself, adorned with the company's bulldog logos, looked good, with a slick and professional design lending a weighty, serious feel leavened by some friendly language in its messages, and proved responsive and solid.

Configuration was generally easily achieved, although logging seemed to be entirely absent, and my only other quibble with the interface was the greyness of some of the buttons, which often made me think the functionality in question was greyed out and thus unavailable – until I tried clicking on them.

Scanning speeds were solid, with particularly thorough scanning of archive files slowing things down a little, and results were, as expected, very impressive. There were very slightly more misses in the zoo test sets here than in the parent product, but nothing from the WildList set got past it.

This performance, combined with a lack of false positives, grants *Bullguard* its first VB100 award on its first attempt, and left me hoping that all the new products would present as few problems as this.

CA AntiVirus 8.4.0.11

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.57%
File infector	99.85%	**Macro**	100.00%
Polymorphic	92.15%	**False positives**	0

CA's home user product first made an appearance in *VB* in the February *Vista* review (see *VB*, February 2007, p.14), and the product submitted this time is little changed from that occasion. Installation included *CA*'s usual trick of requiring EULAs to be scrolled all the way through, as well as a lengthy activation keycode, but once up and running the product presented no such barriers to testing.

A simple GUI was laid out in fairly standard style, and a small but reasonable amount of configuration (for a home-user product) was available. Using the handy context-menu scan option, tests were run through in good time, aided by some excellent scanning speeds. It was no surprise to find that there was no option to scan archives on access.

Detection rates were little changed from previous scores, with a smattering of misses across the zoo test sets, but nothing in the WildList. With no false positives generated in the clean set, *CA*'s home division can celebrate a second VB100 award.

CA eTrust r.8.1.634.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.57%
File infector	99.85%	**Macro**	99.82%
Polymorphic	92.15%	**False positives**	0

CA's corporate offering is also little changed from its last appearance in the *Vista* comparative – indeed, the same submission was used this time with only additional updates provided. The *eTrust* brand has a lengthy history in *VB*'s comparative testing, initially using the *InoculateIT* engine, later swapping to the *Vet* engine as the default, and now offering only the *Vet* engine, since *InoculateIT* was retired late last year.

The *eTrust* interface has never been a favourite of mine, its server-client design leaving the browser chugging slowly along as it attempts to refresh content after every click of a button. Under *Vista*, where version 8.1 was last tested, this sluggishness was notably improved, but any hopes that this was down to the new version rather than the platform were quickly dispelled and testing consisted of brief moments of activity interspersed with long periods watching the 'please wait' message – particularly when trying to view some hefty scan logs, which threatened to overwhelm it entirely.

Despite these issues, tests were eventually completed with the usual very impressive speed during the actual scanning. After converting the logs from the .dbf format in which they are stored to a style which did not require the unresponsive log viewer, results were found to be similarly good, with solid detection and no false positives qualifying *CA* for another VB100 award.

CAT Quick Heal AntiVirus 2007 v.9

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	90.57%
File infector	96.44%	**Macro**	98.04%
Polymorphic	76.11%	**False positives**	0

CAT's website lays claim to the title 'India's leading anti-virus software'. As well as the 'Lite' product submitted for testing, *Quick Heal* is available as both the 'AntiVirus Plus' version, with anti-spyware and firewall functionality constituting the 'Plus' element, and as a full 'Total Security' suite with the addition of spam-filtering and data theft prevention among other things.

The product greeted me with the message 'Welcome to the world of virus-free computing', and the built-in messenger system providing information on updates and outbreaks continued this theme of friendly communication with the user. The interface is simple, but clearly designed and easy to use, with right-click scanning used for much of the testing.

Checking the logs showed the figures to be much as expected, with a fair number of misses in most of the zoo sets, but nothing in the WildList set and no false positives. *CAT* is therefore eligible for another VB100 award.

Doctor Web Dr.Web 4.33.3.04230

ItW	99.33%	**Worms & bots**	100.00%
ItW (o/a)	99.33%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	98.72%	**False positives**	0

Doctor Web is another VB100 regular, supporting a wide set of platforms with its product range, including *Windows* versions as far back as *Windows 95*. The *XP* version, the whole thing impressively compact at little over 10 MB, installs in a shiny and attractive manner, with the customary

On-demand throughput	Archive files - default		Archive files - all files		Binaries and system files		Media and documents		Other file types	
	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
AEC Trustport Workstation Antivirus	984	1.02	984	1.02	587	2.78	54	22.25	84	4.39
Agnitum Outpost Security Suite Pro	236	4.25	236	4.25	151	10.80	44	27.31	20	18.44
AhnLab V3 Internet Security 2007	83	12.09	323	3.11	395	4.13	58	20.72	18	20.49
Alwil avast! Professional Edition	60	16.72	60	16.72	120	13.59	74	16.24	19	19.41
Authentium Command AntiVirus for Windows	71	14.08	71	14.08	127	12.82	13	90.15	12	31.56
Avira AntiVir	131	7.66	141	7.12	55	29.66	12	100.13	6	61.47
Bullguard	760	1.32	760	1.32	127	12.84	18	66.75	26	14.19
CA AntiVirus	149	6.73	149	6.73	52	31.37	17	70.68	11	33.53
CA eTrust	104	9.65	104	9.65	40	40.78	13	92.43	6	61.47
CAT Quick Heal AntiVirus 2007	47	21.35	179	5.61	44	37.07	25	48.06	15	24.59
Doctor Web Dr.Web	277	3.62	277	3.62	1017	1.60	246	4.88	360	1.02
eEye Blink Personal Edition	116	8.65	116	8.65	618	2.64	14	85.82	29	12.72
Eset NOD32 Antivirus System	241	4.16	241	4.16	97	16.82	17	70.68	10	36.88
Fortinet FortiClient	133	7.54	133	7.54	192	8.50	20	60.08	14	26.34
Frisk F-Prot Anti-Virus	86	11.67	86	11.67	112	14.57	28	42.91	7	52.69
F-Secure Protection Service for Consumers	1183	0.85	1187	0.85	142	11.49	11	109.23	6	61.47
G DATA AntiVirusKit	723	1.39	723	1.39	236	6.91	54	22.25	27	13.66
Grisoft AVG Professional Edition	481	2.09	481	2.09	219	7.45	33	36.86	47	7.90
Ikarus Virus Utilities	76	13.20	76	13.20	126	12.95	19	63.24	21	17.56
iolo AntiVirus	72	13.94	73	13.74	132	12.36	13	92.43	10	36.88
K7 Total Security 2006	67	14.98	67	14.98	66	24.72	13	92.43	8	46.10
Kaspersky Anti-Virus	711	1.41	711	1.41	279	5.85	32	37.55	21	17.56
McAfee VirusScan Enterprise	328	3.06	328	3.06	303	5.38	23	52.24	18	20.49
Microsoft Forefront Client Security	257	3.90	257	3.90	117	13.94	54	22.25	12	30.73
Microsoft Windows Live OneCare	277	3.62	277	3.62	121	13.48	57	21.08	16	23.05
Microworld eScan Internet Security for Windows	587	1.71	587	1.71	297	5.49	68	17.67	90	4.10
Norman Virus Control	117	8.58	117	8.58	610	2.67	13	92.43	25	14.75
NWI VirusChaser	412	2.44	412	2.44	151	10.80	30	40.05	59	6.25
PC Tools Antivirus	278	3.61	278	3.61	177	9.22	31	38.76	19	19.41
PC Tools Spyware Doctor	290	3.46	290	3.46	186	8.77	32	37.55	22	16.76
Proland Protector Plus 2007	9	111.48	661	1.52	77	21.19	13	92.43	21	17.56
Softwin BitDefender Antivirus Plus	408	2.46	408	2.46	123	13.26	25	48.06	20	18.44
Sophos Anti-Virus	11	91.21	329	3.05	124	13.16	16	75.10	6	61.47
Symantec AntiVirus	131	7.66	131	7.66	103	15.84	23	52.24	15	24.59
Trend Micro PC-cillin Internet Security 2007	75	13.38	75	13.38	73	22.35	10	120.15	16	23.05
VirusBuster VirusBuster Professional 2006	176	5.70	176	5.70	126	12.95	18	66.75	17	21.70
Webroot Spy Sweeper	249	4.03	249	4.03	202	8.08	69	17.41	58	6.36

stern warnings against having other security products installed on the machine.

Using the product was made easy by familiarity, and once I had remembered that the 'change' button was required to apply changes made to settings, tests were zipped through without difficulty. Unloading the on-access mode prompted a message saying that part of the SpIDer monitor system had failed to unload, but this didn't seem to cause any lasting problems.

Speeds were somewhat slow both on demand and on access, which can perhaps be put down to very thorough scanning, particularly where archives are concerned – the product reported the largest number of 'objects' scanned in this test set. Detection within the zoo sets was as excellent as usual, with most of the very few samples missed being due to the file types not being scanned by default.

Doctor Web had some issues in the last comparative review, with a log parsing problem causing several detected files to be counted erroneously as misses in our initial report. In addition, a small number of W32/Sdbot samples were confirmed to have been missed from the WildList test set. Further investigations by the vendor have indicated that these samples were covered by updates to the product's engine that were not submitted for the test along with the virus database updates, but these samples would have been protected against in a real-world setting.

Unfortunately *Doctor Web* was unlucky again on this occasion, and several more samples were missed, including three Sdbots and two W32/Rbots, all in the WildList set. This was enough to deny *Doctor Web* the VB100 award for the second time running.

eEye Digital Security Blink Personal Edition 3.0.9

ItW	100.00%	**Worms & bots**	99.67%
ItW (o/a)	100.00%	**DOS**	99.74%
File infector	98.73%	**Macro**	99.90%
Polymorphic	81.94%	**False positives**	0

Blink is another newcomer, and one of which I had little prior knowledge. Vulnerability specialist *eEye Digital Security* has been in business for almost ten years, spotting and reporting security flaws and creating software to keep networks free from exploitable software. Its *Blink* client product is a desktop offering promising a range of security features that include: vulnerability scanning, HIPS and other system protection systems, as well as firewalling and anti-malware protection, provided in part by *Norman*.

Installation includes the customary warning against combining the product with other security software, as well as a thorough list of products which could be expected to clash with *Blink*, and an assertion that running multiple products will provide no extra protection. The remainder of the installation process is slick and smooth and requires no reboot.

The interface of the product itself is similarly attractive, with an option-rich page offering controls over the full range of functionality. Scanning is designed in the typical style of an anti-spyware product, with the full system and registry the default target, but individual areas can be scanned by switching off 'deep disk scanning' and selecting the required folder. This gave some unusual speed results, with great attention paid to executable and binary files but little, perhaps sensibly, to media and documents.

On-access detection was obtained via the system's logging, as blocking was not sparked by simple file-opening.

A few times during testing the display faltered somewhat, with attempts to view scan histories producing only a 'Page not found'-type error message, but logging to file seemed more stable.

Results were good across the board, closely matching the scores recorded by *Norman*'s own product, and with the WildList set amply covered and a single suspicious file in the clean set, another impressive-looking piece of software gets its first VB100 stamp of approval.

Eset NOD32 Antivirus System 2.70.32

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

The *Windows* version of *NOD32* is another very familiar product, little changed in the last several tests, although a major new release is promised in the coming months. This should add further functionality to the current protection against malware on the local system and arriving via web and email vectors.

NOD32's configuration is straightforward with the benefit of some experience, and tests zoomed along at the customary rapid pace.

The only option that seemed not to be available was scanning inside archives on access, and the thorough detection which has become the norm for *NOD32* once again covered the entire extent of the *VB* collections. With not a single miss in any set and no hint of a false positive, *NOD32* once again proves worthy of a VB100 award.

Fortinet FortiClient 3.0.412

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Fortinet focuses on business customers with a range of server products and appliances, and unsurprisingly its *FortiClient* product is another thorough suite, with many additions to the usual firewalls and mail filters.

As befits a corporate environment, configuration is flexible in-depth, and can be navigated with ease across the clearly designed, responsive interface.

Scans were completed in very good time, despite defaulting to scanning everything thrown at it, and *Fortinet*'s recent elevation to the top rank of products that miss nothing in any of our zoo sets continues, with full detection scored throughout.

A small issue with the alert popups, which got a little overloaded during the opening of thousands of infected samples within a few minutes, did not prove a significant problem. The thorough detection extended across the WildList set without a false positive in sight, thus granting *Fortinet* another VB100.

Frisk F-PROT Anti-Virus 6.0.70

ItW	100.00%	**Worms & bots**	99.67%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Iceland's *Frisk Software* is another vendor whose history in VB100 testing dates back into the 20th century. This history has been an illustrious one, and the company's detection technology is included in several other products.

F-PROT offers a clean and simple interface in bright white with shades of red and blue. Configuration is straightforward and thorough, with a simplified scanner setting available for those less interested in fine-tuning. On-access scanning is less tweakable, but does its job efficiently.

Scanning speeds were very good throughout, and detection similarly excellent, with nothing beyond the capabilities of the product if properly configured. This included the WildList set, and an absence of false positives gives *F-PROT* another VB100 award.

F-Secure Protection Service for Consumers (7.00 build 387)

ItW	99.88%	**Worms & bots**	99.96%
ItW (o/a)	99.88%	**DOS**	100.00%
File infector	99.49%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

F-Secure's 2007 suite was favourably reviewed in these pages some months ago (see *VB*, November 2006, p.12), and has been gathering similarly positive reviews from other testers. The product submitted for review this time was apparently slightly different from the usual *F-Secure Internet Security*, having been designed for rebranded redistribution, but my user experience was not affected.

However, this preview status seems to have added a few problems into the previously solid suite. An issue with the logging provided, which was previously noted in the *Vista* test when logs containing large numbers of detections failed to export in their entirety, was once again in evidence here. A new problem also emerged on this occasion, with a sample of W32/Wotbot causing the product to seize up somewhat on one occasion.

With these fairly minor irritations overcome, testing was eventually completed, with *F-Secure*'s traditional plodding thoroughness while scanning archives adding to the delays. Detection in general proved to be excellent, with the only miss in the zoo sets caused by a file type not scanned by default. In the WildList set, however, a single sample of W32/Allaple was also missed, which was enough to see a rare failure for *F-Secure* to achieve a VB100 award.

G DATA AntiVirusKit 17.0.7089

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

G DATA's *AVK* product is another of those with a long history of superb performance in *VB*'s testing, and once more there is little fault to be found with the product.

Speeds were not as impressive as some, which is as one would expect from a multi-engine product. The product's interface is not only visually appealing but also clearly and sensibly laid out with little left to be desired. The ever-useful right-click scanning is in evidence, and any attempt to change the settings in a way which could lead to excessive system impact or lack of protection is warned against appropriately.

File access time lag (additional time taken to open a file in comparison with the time taken to perform the same task without the product in place)	Archive files - default		Archive files - all files		Binaries and system files		Media and documents		Other file types	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
AEC Trustport Workstation Antivirus	580	0.58	580	0.58	287	0.17	42	0.03	49	0.13
Agnitum Outpost Security Suite Pro	25	0.02	(NA)	(NA)	176	0.10	46	0.04	28	0.07
AhnLab V3 Internet Security 2007	27	0.03	(NA)	(NA)	185	0.11	3	0.00	12	0.02
Alwil avast! Professional Edition	9	0.01	131	117.80	95	0.05	22	0.02	17	0.04
Authentium Command AntiVirus for Windows	11	0.01	(NA)	(NA)	128	0.07	11	0.01	10	0.02
Avira AntiVir	8	0.01	(NA)	(NA)	60	0.03	11	0.01	4	0.00
Bullguard	35	0.03	182	164.39	109	0.06	18	0.01	20	0.05
CA AntiVirus	7	0.01	(NA)	(NA)	51	0.03	15	0.01	9	0.02
CA eTrust	8	0.01	(NA)	(NA)	44	0.02	14	0.01	9	0.02
CAT Quick Heal AntiVirus 2007	7	0.01	(NA)	(NA)	59	0.03	16	0.01	6	0.01
Doctor Web Dr.Web	277	0.27	277	249.68	262	0.16	39	0.03	37	0.09
eEye Blink Personal Edition	28	0.03	46	41.09	66	0.04	15	0.01	17	0.04
Eset NOD32 Antivirus System	4	0.00	(NA)	(NA)	40	0.02	19	0.01	12	0.03
Fortinet FortiClient	76	0.07	76	68.46	193	0.11	16	0.01	17	0.04
Frisk F-Prot Anti-Virus	26	0.03	(NA)	(NA)	130	0.08	27	0.02	8	0.01
F-Secure Protection Service for Consumers	11	0.01	440	396.82	123	0.07	16	0.01	8	0.02
G DATA AntiVirusKit	100	0.10	369	332.89	203	0.12	86	0.07	35	0.09
Grisoft AVG Professional Edition	9	0.01	(NA)	(NA)	76	0.04	13	0.01	7	0.01
Ikarus Virus Utilities	69	0.07	69	62.23	129	0.07	21	0.02	23	0.05
iolo AntiVirus	13	0.01	(NA)	(NA)	136	0.08	13	0.01	7	0.01
K7 Total Security 2006	7	0.01	(NA)	(NA)	75	0.04	12	0.01	10	0.02
Kaspersky Anti-Virus	10	0.01	133	119.90	115	0.07	22	0.02	15	0.03
McAfee VirusScan Enterprise	22	0.02	155	139.50	203	0.12	21	0.02	18	0.04
Microsoft Forefront Client Security	31	0.03	31	28.21	112	0.06	53	0.04	13	0.03
Microsoft Windows Live OneCare	30	0.03	30	27.39	114	0.07	53	0.04	13	0.03
Microworld eScan Internet Security for Windows	257	0.25	257	231.33	191	0.11	32	0.02	30	0.07
Norman Virus Control	12	0.01	(NA)	(NA)	66	0.04	15	0.01	17	0.04
NWI VirusChaser	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)
PC Tools Antivirus	99	0.10	99	89.55	291	0.17	35	0.03	21	0.05
PC Tools Spyware Doctor	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)
Proland Protector Plus 2007	5	0.00	12	10.92	59	0.03	8	0.00	3	0.00
Softwin BitDefender Antivirus Plus	34	0.03	306	276.16	109	0.06	18	0.01	21	0.05
Sophos Anti-Virus	15	0.01	316	284.59	121	0.07	17	0.01	8	0.01
Symantec AntiVirus	13	0.01	(NA)	(NA)	94	0.05	14	0.01	10	0.02
Trend Micro PC-cillin Internet Security 2007	12	0.01	73	66.13	75	0.04	10	0.01	8	0.01
VirusBuster VirusBuster Professional 2006	20	0.02	(NA)	(NA)	129	0.07	15	0.01	6	0.01
Webroot Spy Sweeper	3	0.00	(NA)	(NA)	12	0.00	14	0.01	9	0.02

The only minor quibble I had was a repetition of the grey-buttons-looking-greyed-out problem mentioned earlier, and the format of the logs being less than ideal for my personal needs. However, with no samples missed in any of the test sets, and just a few warnings about hacker tools and joke programs in the clean set, *AVK* racks up yet another VB100 award with ease.

Grisoft AVG 7.5 Professional Edition

ItW	100.00%	**Worms & bots**	99.56%
ItW (o/a)	99.88%	**DOS**	99.29%
File infector	97.41%	**Macro**	99.93%
Polymorphic	75.88%	**False positives**	0

Grisoft, like *Alwil* and *Avira*, makes a basic version of its product available as a free download. *AVG* anti-virus thus has a very high public profile, supported by a reputation for solidity and good detection. Its free anti-rootkit and anti-spyware products, backed up by technology brought in by the company's acquisition of *Ewido*, are also in wide use. *Grisoft* also provides full-featured and integrated versions, as well as a range of server products and support for other platforms.

Also mirroring *Alwil*, *AVG* offers simple and advanced versions of its interface, neither of which is entirely straightforward. Scans were mostly initiated using the right-click method, to avoid a rather fiddly task design system, and scanning times were far better on access, where little configuration was available, than on demand.

Detection rates were little changed from previous tests, with results generally solid with a scattering of misses in each set. In the WildList set, a W32/Rbot sample was detected by the spyware side of the product, labelled as Adware and a 'potentially unwanted program'. On access, this meant that the file was not alerted on, and although this error was apparently corrected within days of the product's submission, it was enough to deny *AVG* a VB100 award this time.

Ikarus Virus Utilities 1.0.52

ItW	99.88%	**Worms & bots**	99.89%
ItW (o/a)	99.88%	**DOS**	92.32%
File infector	92.82%	**Macro**	95.86%
Polymorphic	71.00%	**False positives**	22

This is the second appearance of *Ikarus Virus Utilities* in a *VB* comparative review – its first having been as long ago as November 2001 (see *VB*, November 2001, p.16). Austria-based *Ikarus Software* also carries a range of server products for mail and web filtering, and the product is available as a six-month free trial.

The initial download is remarkably small at only slightly over 4 MB, but this must be supplemented by the virus definition data, which for this test measured around 7 MB.

Installation was prevented initially by the need for the *Microsoft .NET* framework, which apparently is downloaded automatically when the installer is run with web access. With this in place, the process continued with a check for other security software which may prevent full operation, and the offer to install *Adobe Reader* which is needed to access the documentation (which sadly only works when running from CD and was not included in my download edition).

With the installation complete and updates added, the product showed a small status display tool with details of the scanner, updater and on-access 'guard', but the main interface seemed unwilling to open at first. After several attempts and a reboot it suddenly started responding, and from then on seemed to suffer no such problems. Configuration was minimal and a little difficult to fathom, but once figured out, things got moving quite nicely.

While scanning the large infected sets much of the interface faded away and refused to respond, leaving me fearing a total crash, but checking back some time later I found it had returned to normal and the scan completed without serious incident.

On-access scanning was easier to run through, and analysis of the results showed good speeds, though detection across the infected sets was a little uneven, with a significant number of misses in the older DOS and polymorphic sets. These figures are magnified by some large sample sets however, and overall percentage scores are more impressive.

More importantly, a small handful of WildList viruses were missed, and several false positives were alerted on, including components of the *Nero* CD recording software, *Norton Ghost* and the *GoogleTalk* installer, all of which were labelled as trojans. This was enough to deny *Ikarus* its first VB100, but with a little work the product should be a solid contender for qualification in the near future.

iolo AntiVirus 1.1.9

ItW	99.97%	**Worms & bots**	99.63%
ItW (o/a)	99.86%	**DOS**	99.93%
File infector	100.00%	**Macro**	98.60%
Polymorphic	96.15%	**False positives**	2

Best known for its repair and optimization products, *iolo* has built a considerable public profile with its presence on the shelves of high-street software outlets. The company's range of anti-virus and firewall products also includes a full security suite. Having previously licensed the *Kaspersky*

engine, *iolo* now uses technology from *Authentium*, in addition to some ideas of its own.

Having heard from *iolo* some time in advance of this test, I was lucky enough to have had a look at the product in advance and get to know its workings. The installation was smooth and unproblematic, although it spent some time getting ready for action. The interface looks thorough, crammed with information without being cluttered, and appears to have ample configuration options.

Logging seemed only to kick in when some kind of disinfection or removal took place, so scanning alone was not possible. The default setting, which involved quarantining most items, took an excessively long time when dealing with large numbers of infected files and seemed to get stuck every few thousand, locking down the interface and requiring a reboot to fix. This is not a likely scenario outside the test lab, however, and is most unlikely to affect users; setting it to delete without quarantining circumvented the problem.

Speeds over clean files were excellent in both modes, with no further crashes experienced, and detection seemed thorough throughout. However, two *PowerPoint* files in the clean set were labelled as infected, and a single WildList file was missed in both modes, with another missed on access only, which means *iolo* will have to try again to achieve VB100 certification.

K7 Total Security 2006

ItW	100.00%	**Worms & bots**	97.34%
ItW (o/a)	100.00%	**DOS**	88.65%
File infector	93.63%	**Macro**	97.23%
Polymorphic	65.00%	**False positives**	0

K7 Computing, based in Chennai, India, is yet another name that is new to the *VB* test bench, but again the firm is far from new to the game, having produced its first anti-virus product as long ago as 1992. Along with the *Total Security* suite seen here, which includes firewall and anti-spam functions, a standalone anti-virus product and a corporate edition are also available.

The installation process was a smooth and clean operation, and ends with a 'news and update' screen carrying useful information. This was, in fact, one of the only products to point out that my lack of web connection was the reason the product could not update itself. The interface showed similar attention to detail in its clear and user-friendly design, and was steady and responsive throughout.

Scanning speeds were excellent at all times, and while detection was not perfect on the less current test sets, especially the aging and less relevant DOS set, this was far from surprising for a newcomer not using anyone else's technology. *K7* has clearly been working hard on the latest threats and achieved full coverage of the WildList set. With just a couple of items in the clean sets adjudged to be 'riskware', *K7* can proudly claim its first VB100.

Kaspersky Anti-Virus 6.0.2.621

ItW	99.88%	**Worms & bots**	100.00%
ItW (o/a)	99.88%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Kaspersky's product is a far more familiar one, having been the subject of another thorough review in *VB* a few months ago (see *VB*, September 2006, p.16). The installation and use of the product were thus straightforward, and all the tests were sprinted through in good time, although things were slowed somewhat by the need for a reboot after install and some seriously in-depth scanning of archives.

Detection figures were mostly as excellent as ever, with a pair of misses in one zoo set attributable to the file types ignored by default on access. Unfortunately, however, the same sample of W32/Allaple that upset *F-Secure*'s chances of a VB100 was missed here. Investigations have shown that detection was in place both a few days before and a few days after our test, and was presumably removed temporarily for some fixing. This unfortunate timing was enough to spoil *Kaspersky*'s recent solid record of VB100 awards.

McAfee VirusScan Enterprise v.8.5i

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.85%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

McAfee's corporate desktop product was submitted for this test, and was unchanged from previous tests. It is a solid and businesslike product, with its operation and configuration thorough and lacking in either excessive simplification or over-complex razzle-dazzle.

The only confusing aspect remains the inability to deactivate on-access scanning from the main interface (it can be switched off with ease from the system tray). Scanning speeds were good, and detection excellent, with only a small handful of DOS samples missed. Another VB100 is awarded to *McAfee* without further ado.

Microsoft Forefront Client Security 1.5.1937

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	99.81%	**Macro**	100.00%
Polymorphic	96.15%	**False positives**	0

Forefront is *Microsoft*'s long-awaited corporate client product, a new implementation of the scanning technology provided for the home user market in *OneCare*. The final release to market is expected to be at around the same time as the publication of this review.

Things got off to a shaky start when my first stab at running the installation CD on a test machine proved a dead loss, the installer failing with an obscure error message. Resorting to the documentation, I found to my horror some lengthy instructions for the design of a security topology, which required a *Windows 2003* server on which to run the installer and from which to deploy to clients – this also needed such delights as *Microsoft SQL Server 2005 SP1*, *IIS* and *ASP.net*, the *.NET* framework 2.0, *MMC 3.0*, *GPMC SP1* and *WSUS*. While making moves to acquire these items, I asked the developers for a simpler client install method, which thankfully was provided and proved ample for my needs.

The user interface seemed rather simple, with less configurability than I would expect from a corporate product. Presumably most of this side of things is controlled from a proper management server, where available. Running most of the testing was fairly straightforward however, with the only problem being a complete absence of internal logging – detection details had to be gleaned from the system event log.

Scanning speeds were fairly reasonable, and detection seemed pretty thorough overall, *Microsoft* having made some efforts at improving its coverage since the recent appearance of *OneCare* in *VB*'s *Vista* test.

Some slightly unusual behaviour was uncovered when a single file in the WildList set, a sample of W32/Tenga, was not blocked on access. Further investigation showed that the default action for this file was set to 'always allow' (after detecting the file in an on-demand scan, selecting the 'apply action' option either deleted, disinfected or quarantined other items, while this one was for some reason allowed to pass unfiltered).

Despite this problem, basic detection of the file was provided, and thus without having generated any false positives in the scan of the clean test set, *Forefront* just about qualifies under the rules of the VB100 award.

Microsoft Windows Live OneCare 1.5.1890.35

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	99.81%	**Macro**	100.00%
Polymorphic	96.15%	**False positives**	0

My second attempt at testing *OneCare* was aided by some familiarity with the product, and with the special setup required to allow this web-centric software to operate without its connection to base. Installation was at first hindered by some mysterious errors, but this was soon diagnosed, with help from the developers, as being due to my system using the UK locale, for which the appropriate language packs were not included in the pared-down version provided for my test.

My experience with the interface paid off and the tests were completed without further issue, with scanning speeds a fraction slower than *OneCare*'s corporate sibling and detection rates just as good. Among the other functionality included was an offer to 'tune-up' my system, with disk defragmentation etc.

Limited configuration did not extend to logging, and results, once parsed, showed full detection of the WildList, and again no false positives, so *OneCare* is also granted the VB100 this time.

Microworld eScan Internet Security for Windows 9.0.714.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Microworld Technology provides a wide range of server and gateway products alongside those for desktops, including *Linux*.

The installation of *eScan* complained at first about the date on my test machine, which for some reason was set to before the creation date of the product. With this small issue resolved, the installation continued simply and rapidly, and required a reboot to activate fully. The interface was a little odd-looking, but fairly simple to use throughout my tests, and speed times reflected the thoroughness of the *Kaspersky* engine at the heart of the product.

Thoroughness was also a feature of scans of the infected sets. I spent a long time watching the amusing animation of

a hand crushing an insect which accompanied detection, along with a wildly inaccurate progress bar.

Microworld's submission seems to have missed the small window during which the *Kaspersky* engine missed detection of the W32/Allaple sample, and also had more complete defaults, resulting in 100% detection across the board, and with only a single piece of software labelled a risk, *eScan* wins another VB100 with some style.

Norman Virus Control 5.90

ItW	100.00%	**Worms & bots**	99.67%
ItW (o/a)	100.00%	**DOS**	99.74%
File infector	98.97%	**Macro**	100.00%
Polymorphic	81.94%	**False positives**	0

Norman is another familiar face in *VB*'s testing, and again familiarity with the rather unusual layout of the product rendered testing less of a chore than it once was. The availability of a right-click option, starkly labelled 'Norman Virus Control', also helped speed things along.

On-access scanning has always been somewhat odd in the *Norman* product, with little control of its behaviour available, and logging was a little flaky here, requiring several attempts to get a full list of detections. Scanning the WildList seemed to show a batch of files never blocked when opened, but access to those tricky logs showed that detection was indeed in place and some allergy to the testing tool in use was diagnosed as the likely cause of the oddity.

Overall, results were shown to be very good, with no false positives and some pretty decent times in the speed tests. With the WildList covered without difficulty, *Norman* also wins a VB100.

NWI VirusChaser 5.0a

ItW	98.90%	**Worms & bots**	99.67%
ItW (o/a)	98.90%	**DOS**	99.18%
File infector	99.24%	**Macro**	99.90%
Polymorphic	97.82%	**False positives**	0

NWI is the abbreviation of *New Technology Wave Inc.*, a Korean operation whose *VirusChaser* product is an implementation of the *Dr.Web* scanning engine aimed at the Asian market, and is provided in an even smaller package – this time a mere 7 MB in total.

Installation was thus simple and fast, and the clear and straightforward GUI offered more configuration of its own appearance than of actual scanning behaviour. Many tests were nevertheless carried out fairly easily using the context-menu option, and zipped along very rapidly.

On-access scanning seems not to be sparked by simple file opening, and as a result speed times were not measurable for comparison, but detection was instead measured by copying files to the machine.

Logs showed detection rates to be slightly below the level achieved by the parent product, along with a broad set of applications labelled 'Riskware'. Unfortunately for *NWI*, the product missed the same clutch of WildList samples as *Dr.Web*, as well as a handful of others, which means that no VB100 is awarded to *NWI* this time either.

PC Tools Antivirus 3.1.1.6

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.10%
File infector	98.46%	**Macro**	100.00%
Polymorphic	87.74%	**False positives**	0

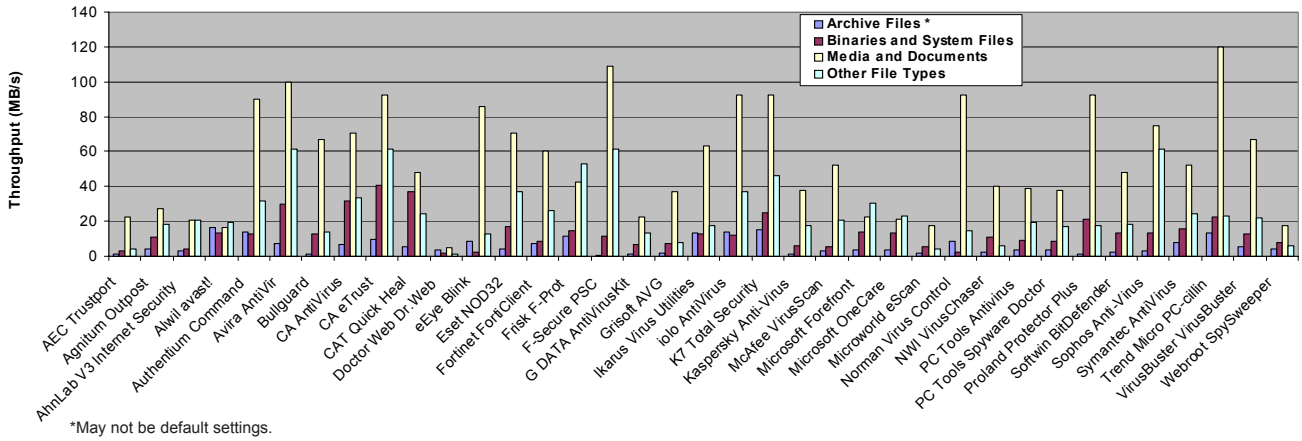
The first of two submissions from *PC Tools*, this is the company's standalone anti-virus product, which was first released in late 2005 and is assisted by *VirusBuster* technology. A basic version of the product is also made available as a free download. Alongside its anti-malware range, *PC Tools* also offers a selection of system repair, recovery and cleanup products, privacy tools, a spam filter and a firewall.

The product installed rapidly and simply with few choices to be made, and launched an attempt to update without prompting. Oddly, this reported that the product was up to date, despite having no web access from within the test lab, and the brightly coloured interface's status page also misleadingly reported that 'the last update was today'.

The GUI was simply laid out, and testing ran through without difficulty. Some hefty XML logs proved a little much for my poor tired system to bear, but scanning speeds were good and results looked promising. On-access behaviour was a little unusual too, with access to some files denied and other detections merely logged, while a cascade of alert messages gushed down the right-hand side of the screen.

In both modes, the product had difficulty with a couple of files in the clean set, which it got stuck on, refusing to go any further. On demand, trying to stop the snagged scan simply led to a 'stopping…' message, and only a reboot moved things along. With the 'On Guard' on-access scanner switched on, perusing files from *Explorer* slowed to a rather frustrating degree at times, especially while trying to analyse the large logs created.

On demand scanning speed



*May not be default settings.

With these issues surmounted, detection results were finally obtained and results proved pretty thorough across all the sets. The WildList was completely covered, with no false positives, adding *PC Tools* to the roster of new VB100 winners this month.

PC Tools Spyware Doctor v.5.0.0.182

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	98.88%
File infector	98.46%	**Macro**	99.93%
Polymorphic	87.74%	**False positives**	0

Spyware Doctor is *PC Tools*' long-standing flagship product, a widely trusted anti-spyware tool into which virus detection and protection has been added.

The installation process and appearance of the interface are similar to the previous product, colourful and curvy and aimed squarely at the home user, although this one had some more complex configuration and a lengthy list of scanning types from which to select when kicking off a localised scan.

Logging proved a little tricky again here, with output generally truncated, but results were gathered easily by setting it to delete infected items from the test sets and seeing what was left behind. On-access detection was also unusual, with no blocking of simple file access possible and so no speed figures for this mode were available, but the slowdown was fairly noticeable to the naked eye from time to time. Detection on access was measured by copying files to the system and having them deleted.

The same two files in the clean set caused problems, but once the snags were overcome no false positives were reported, on-demand scanning speeds were reasonable, and detection rates were good too, although *Spyware Doctor* missed a small set of DOS samples caught by its sister product. Everything else proved fine though, and a second VB100 is duly awarded to *PC Tools*.

Proland Protector Plus 2007

ItW	99.76%	**Worms & bots**	98.89%
ItW (o/a)	97.93%	**DOS**	78.53%
File infector	84.84%	**Macro**	82.53%
Polymorphic	36.97%	**False positives**	2

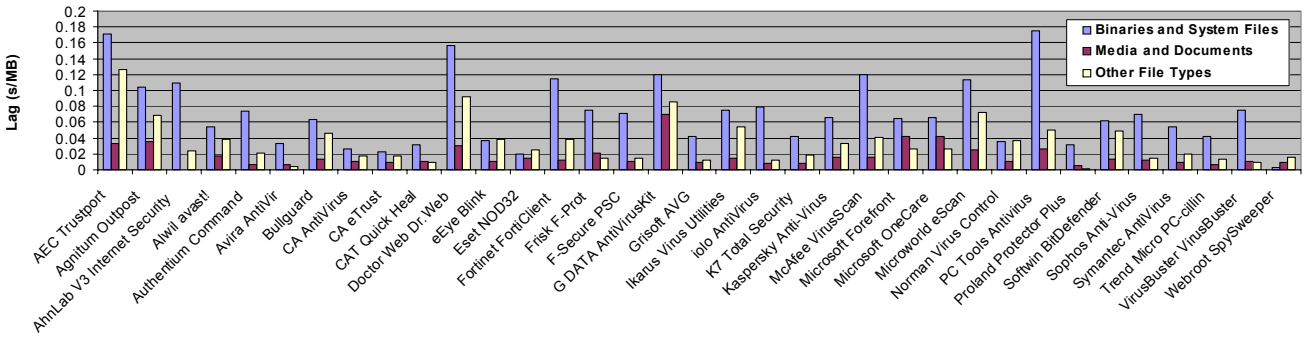
Proland is another vendor that is neither a complete newcomer to *VB*'s comparative testing nor a regular. The vendor's products previously appeared in several comparative reviews in the late 1990s, and *Proland* returns after a lengthy absence and recent acquisition.

Protector Plus is another contender for the accolade of most compact product, with the whole thing weighing in at around 8.5 MB, and again a slick and speedy installation reflects its small size. The process looks good too, and offers but does not force a system scan. The option is also provided to add support information to the *Windows* address book.

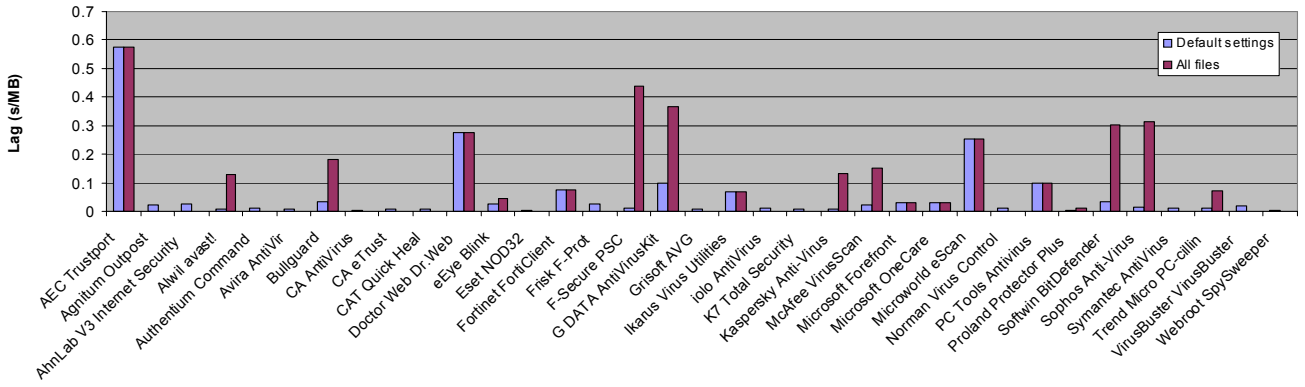
This attention to user needs was shown throughout, with lots of helpful advice, and the product's interface was attractive and well designed. It also ran well, with no freezes or crashes or other unwanted behaviour despite the heavy load of the tests.

Checking through results revealed some superb scanning speeds, as expected, and also a fair number of misses across all the zoo sets, with particularly low coverage of older samples. A couple of WildList samples were likewise missed, with several more missed on access thanks to some incomplete coverage of file extensions. This, along with the

File access lag time



File access lag time (archive files)



presence of two false positives, means that *Proland* will also have to do a little more work before qualifying for a VB100 award.

Softwin BitDefender Antivirus Plus v.10

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	98.97%	**Macro**	99.69%
Polymorphic	97.86%	**False positives**	0

BitDefender is a more well-established product, with its advanced heuristics making it a popular choice for other software makers looking for an extra engine.

The company's own implementation includes most of the standard extras, with a firewall, spam and web filters and anti-spyware functionality included, as well as the 'B-Have' behavioural intrusion-spotter.

The product boasts that it is 'a superior software package', and it certainly looks sleek and solid. The 'Activity Bar' that hovers in a corner of the screen, semi-transparent, has always been a bit of a mystery to me, and the interface itself is similarly quirky and unusual, but its nice deep red colour scheme oozes professional slickness and solidity.

Scanning was soon under way once I had re-familiarised myself with the controls. Speeds leaned towards the thorough rather than zippy, and detection rates towards the very top end with only a handful of missed samples. None of these were in the WildList set, and no false positives were recorded either, thus qualifying *BitDefender* for another VB100 award.

Sophos Anti-Virus 6.54 R2

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Sophos rarely misses a chance to enter a *VB* comparative review. Despite a major new version of the associated management tools and the addition of an optional firewall

late last year, the end-user experience has remained little changed for some time.

Installation and use skipped along simply, with the in-depth configuration available making for easy testing. Some improvements in detection have removed the small number of obscure samples regularly missed in previous tests, and the only remaining misses are in *Access* database files, ignored by default to avoid problems with *Sophos*'s corporate customer base, who can be expected to have extremely large databases.

These same customers are also served by warnings about some system tools which could present a hacking risk on a corporate network, but no actual false positives and full detection of the WildList set earn *Sophos* a VB100.

Symantec AntiVirus 1.0.0.359

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.97%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Symantec also targets the corporate market with the product submitted here, which has a serious and text-heavy feel with none of the cuddly graphics home users are generally assumed to require. Again, my familiarity with the workings of the product allowed me to complete the tests in record time.

Scanning speeds were good, although surprisingly I could find no way of activating on-access scanning inside archives.

Detection was reliably thorough, with only a tiny number of DOS samples missed, and this thoroughness extended to the WildList test set. In the clean sets a single file was flagged as suspicious, but there was nothing to prevent *Symantec* from winning a VB100 award.

Trend Micro PC-cillin Internet Security 2007

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.53%
File infector	98.91%	**Macro**	99.68%
Polymorphic	93.10%	**False positives**	0

Trend Micro's suite was reviewed in depth last month (see *VB*, May 2007, p.14), and is still installed on a few of my spare test systems, so no trouble was expected. The product is well-designed throughout, both visually appealing and easy to navigate, and includes several useful ideas.

During installation I was informed that the *Windows* firewall would be deactivated, to be replaced with the product's own firewall. I was also presented with a list of vulnerabilities detected on my bare system for which patches have since been released.

Detection was decent, if not among the most thorough, but nothing from the WildList was missed and no mistakes were made in the clean sets, resulting in another VB100 for *Trend Micro*.

VirusBuster VirusBuster Professional 2006 v.5.2

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.55%
File infector	99.23%	**Macro**	100.00%
Polymorphic	87.82%	**False positives**	0

VirusBuster is, for once, not the last product in this test alphabetically – but the offering is one that I never mind getting around to at the end of a test period, with its clear and logical design and pleasing stability.

While the layout of the on-demand scanning system is not my favourite, right-click scanning avoided much need to use this, and gave good speed results and a small selection of missed files in the zoo sets.

VirusBuster's engine has already appeared in this test, implemented in some of the newcomers' products, but the problems exhibited there were not in evidence here, and with only a warning that a zipped file in the clean set may be an attempted zipbomb, *VirusBuster* wins another VB100 award.

Webroot Spy Sweeper 5.5

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	99.93%
Polymorphic	100.00%	**False positives**	0

The final product on the list is yet another newcomer. *Webroot*'s *Spy Sweeper* has long been a popular and well-regarded player in the anti-spyware field; the company has been around for over ten years, and also produces firewall, performance management and content-filtering software. *Spy Sweeper* added anti-virus protection and detection late last year, incorporating the *Sophos* engine into version 5.2 of the product.

Installation of *Spy Sweeper* was a simple process, although some tweaking was required to add in the anti-virus components, which would normally be downloaded from the web separately from the main console. These were clearly recognisable as many of the parts that make up the *Sophos* product.

The interface is clear and simply laid out with the colourful style expected from home-user-focused anti-spyware offerings. Control of the various settings is available from several tabbed screens including those marked 'Shields' and 'Options', although these were heavier on information than actual controls.

On-demand scans were run from a tab labelled 'sweep', and were straightforward to set up and run. Here again little deep configuration was available, but it proved sufficient for my needs, and judging by the slowish speeds achieved on demand, scanning appears to default to fairly thorough settings.

On-access scanning speeds were considerably faster, and among the most impressive in this month's set of products. This led me to suspect that settings here leaned towards the lax, ignoring many file types entirely. However, this proved not to be a problem where detection of the test sets was concerned. While, once again, blocking access completely did not seem to be possible, detection of malware as files were opened clearly took place, and thorough logs were produced.

The logs included useful data on the malware found, as well as warnings whenever scanning a file took longer than a few thousandths of a second. The logs also listed the vast majority of the samples in the sets, including everything rated In the Wild. With an impressive performance overall, congratulations go to *Webroot* for claiming a VB100 award on its first attempt.

CONCLUSIONS

It has been a mixed month for all comers, with the large number of new arrivals drawing attention away from the regulars, most of whom put in their usual strong performances without fuss. One particularly unfortunate piece of timing spoiled the records of a couple of products which are used to achieving the highest standards, while another suffered from a miscategorisation, but in general little of interest occurred regarding the old hands.

The newcomers tell an entirely different story, with a wide range of products showing a diverse selection of new ideas and implementations.

Some of the newcomers were virus scanners pure and simple, with perhaps some minor extra functionality which is becoming the norm in all products these days. Of these, several have developed their own scanning technology from scratch, and a select few have done well enough to pass the award criteria.

Most of the newcomers were a little lacking in detection of the samples included in the older test sets. Some of these older sets may be losing their relevance to modern users, and the process of modernising the *VB* test sets continues apace. However, the continued appearance of reports of *Windows 95* and even DOS malware from our prevalence data providers indicates that at least some users are still affected by these aging nasties, and would benefit from some protection from them.

The majority of the new products, though, were the result of specialist vendors from other security fields rolling virus protection into their offerings. Just as the traditional anti-virus vendors have had to expand their focus to include spyware protection and firewalls, so the firewall and anti-spyware experts have seen the need to add anti-virus protection to their products. This is generally done by licensing the detection technology of an established vendor, and in these cases implementation is all – with some integrating the engines into their products very successfully, and others still suffering a few teething problems.

Many of these products were highly impressive, and seem likely to offer some stiff competition to the established vendors with the diversity of extras they offer. As always, diversity and competition can only improve standards in general, but I hope that some of these ideas will be merged rather than further enlarging the field of products. It seems unlikely that either the poor exhausted test systems, or the equally worn out tester, could handle another month like this one.

Technical details

Test were run on identical machines with *AMD Athlon64 3800+* dual core processors, 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, all running *Microsoft Windows XP Service Pack 2*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/WinXP/2007/test_sets.html.

Any developers interested in submitting products for VB's comparative reviews (and VB100 certification) should contact John Hawes on john.hawes@virusbtn.com. The current schedule for forthcoming VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.

END NOTES & NEWS

The CISO Executive Summit & Roundtable takes place 6–8 June 2007 in Nice, France. The event will focus on how today's CISO can drive and integrate security into the very core of the business. For details see http://www.mistieurope.com/.

CSI NetSec '07 will be held 11–13 June 2007 in Scottsdale, AZ, USA. Topics include: botnet subversion; Vista; compliance automation; pen testing; VoIP; insider threats; forensic analysis; web-based apps; NAC; identity management; social engineering; and wireless hacking. For details see http://www.csinetsec.com/.

ICEIS 2007 takes place 12–16 June 2007 in Funchal, Madeira. Topics include: human-computer interaction; software agents and internet computing; information systems analysis and specification; artificial intelligence and decision support systems; databases and information systems integration. See http://www.iceis.org/.

The 19th FIRST Global Computer Security Network conference takes place 17–22 June 2007 in Seville, Spain. For full details see http://www.first.org/conference/2007/.

IT Underground Dublin will be held 20–22 June 2007 in Dublin, Ireland. IT Underground will cover a wide range of security topics ranging from hacking techniques to OS hardening, reverse engineering, forensics and legal aspects of computer security. For details see http://www.itunderground.org/.

The Information Security Asia 2007 Conference & Exhibition takes place on 10 and 11 July 2007 in Bangkok, Thailand. For details see http://www.informationsecurityasia.com/.

The International Conference on Human Aspects of Information Security & Assurance will be held 10–12 July 2007 in Plymouth, UK. The conference will focus on information security issues that relate to people. For more details see http://www.haisa.org/.

The 2nd conference on Advances in Computer Security and Forensics (ACSF) will take place 12–13 July 2007 in Liverpool, UK. For details see http://www.cms.livjm.ac.uk/acsf2/.

Black Hat USA 2007 Briefings & Training takes place 28 July to 2 August 2007 in Las Vegas, NV, USA. Registration is now open. All paying delegates also receive free admission to the DEFCON 15 conference, which takes place 3–5 August, also in Las Vegas. See http://www.blackhat.com/.

The 16th USENIX Security Symposium takes place 6–10 August 2007 in Boston, MA, USA. A training program will be followed by a two-and-a-half day technical program, which will include refereed papers, invited talks, work-in-progress reports, panel discussions, and birds-of-a-feather sessions. For details see http://www.usenix.org/events/sec07/.

HITBSecConf2007 - Malaysia will be held 3–6 September 2007 in Kuala Lumpur, Malaysia. For more details see http://conference.hackinthebox.org/.

The 17th International VB Conference, VB2007, takes place 19–21 September 2007 in Vienna, Austria. For the full conference programme including abstracts for all papers, and online registration see http://www.virusbtn.com/conference/.

COSAC 2007, the 14th International Computer Security Forum, will take place 23–27 September 2007 in Naas, Republic of Ireland. See http://www.cosac.net/.

RSA Conference Europe 2007 takes place 22–24 October 2007 in London, UK. See http://www.rsaconference.com/2007/europe/.

The CSI 34th Annual Computer Security Conference will be held 5–7 November 2007 in Washington, D.C., USA. The conference program and registration will be available in August. See http://www.csi34th.com/.

E-Security 2007 Expo & Forum will be held 20–22 November 2007 in Kuala Lumpur, Malaysia. For event details and registration see http://www.esecurity2007.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)1235 531889
Email: editorial@virusbtn.com Web: http://www.virusbtn.com/

vb Spam supplement

CONTENTS

NEWS & EVENTS

PESTILENT SPAMMER ARRESTED

A man described by anti-spam organisation *Spamhaus* as 'one of the most persistent professional spammers' was arrested in Seattle late last month and indicted on 35 counts including mail fraud, wire fraud, email fraud, aggravated identity theft and money laundering.

According to *Spamhaus*, Robert Alan Soloway has been a prolific spammer and seller of harvested lists for many years. Indeed, Soloway has already been in court for spam-related offences on a number of occasions. In 2005 *Microsoft* won a $7 million civil judgment against him, and in the same year the operator of a small Oklahoma-based ISP was awarded a $10 million judgment against him. In September 2005, a US district judge issued a permanent injunction against Soloway, forbidding him to continue sending messages that violated the CAN-SPAM act. However, Soloway ignored the injunction.

If convicted of all charges, Soloway could face up to 65 years in prison (though the term is generally expected to be substantially less).

EVENTS

The 10th general meeting of the Messaging Anti-Abuse Working Group (MAAWG) will take place 5–7 June 2007 in Dublin, Ireland (members only) and a further meeting will be held 8–10 October 2007 in Washington D.C., USA. See http://www.maawg.org/.

CEAS 2007, the 4th Conference on Email and Anti-Spam, takes place 2–3 August 2007 in Mountain View, CA, USA. For details see http://www.ceas.cc/.

The Text Retrieval Conference (TREC) 2007 will be held 6–9 November 2007 at NIST in Gaithersburg, MD, USA. See http://plg.uwaterloo.ca/~gvcormac/spam.

FEATURE

THE SCOURGE OF BLOG SPAM

Jessica Baumgart
Renesys, USA

Jessica Baumgart, an active blogger since April 2003, has contributed to a variety of weblogs on at least seven different platforms, helps lead a support group for bloggers, and eagerly deletes spam. In this article she describes the lesser known, but increasing problem of blog spam.

Weblog spam doesn't get as much attention as email spam because not as many are plagued by it. However, it is a growing problem and one that has important consequences for the Internet and technology community. Blog developers, search engine companies and blog administrators will need to change their approaches to handling unwanted and unwelcome blog comments and fake weblogs.

BLOG SPAM

Most weblog spam falls into one of three categories: comment spam, trackback spam, or a spam weblog. Comment spam is basically an unsolicited and sometimes unrelated comment on a weblog that might advertise a product, service, or website. Some comment spam is added manually by a person to a particular weblog entry. Much comment spam comes from scripts that can add many comments automatically to one post or many posts simultaneously.

Trackback spam happens as a result of the ability of some weblog platforms to show links to posts linking to a particular post. In some cases, real web pages of a spam-like nature create a genuine trackback by linking to a blog post. In other cases, bots exploit the weblog software to place fake trackbacks advertising products, services, and/or websites on weblogs.

A spam weblog, or splog, is a blog created for no better purpose than to advertise various products, services, or websites. Spam blogs can be found on some free weblog sites, like *Blogger*. While sometimes invisible to and ignored by many people, these blogs can often cause problems for search engines.

Bots and scripts are often faster, more efficient, and a less expensive way to create weblog spam than hiring people. However, some unsolicited blog comments and fake weblogs are the result of humans putting fingers to keys. For targeted spam, like a comment that includes text that is related to the nature of the post, or to circumvent a tricky registration process on a high-profile blog, sometimes humans are better for the task than a bot or a script.

A lot of blog spam is very similar to email spam. It advertises medication, vacation destinations, and all sorts of items that might also appear in an email inbox. It is often easy to determine that a comment, trackback, or weblog is garbage.

However, it is not always simple to decipher whether something is blog spam. A popular comment goes something like this: 'I like your site. I find it very useful. Please visit mine', and includes a link. Until the blogger or comment reader follows the link or reads many identical comments on the same weblog, it might not be obvious that the comment is spam.

Some comments are rambling digressions that might or might not be genuine comments posted by real readers. Others are lists of links, which might be pure spam, or might have been posted by a reader in a hurry who wants to point out some related and possibly useful websites. Since the Internet has a global reach, it can also be difficult to deduce the nature of a comment posted in a foreign language and to determine whether or not it should be removed.

Some spam can be offensive and may relate to illegal activities, such as child pornography. Other spam points to malware sites that cause problems for people who follow the links. Enough trashy comments on a weblog can cause readers to change their minds about the value of the blog. Links to sites hosting malware and other unsavoury content might result in a weblog being excluded from certain search engines. Bloggers and blog administrators who choose to ignore spam on their weblogs are unlikely to be making the wisest decision.

SEARCH ENGINE PAGE RANKING

Spammers post comments and trackbacks and create spam blogs for a variety of reasons. Much like email spam, they want people to use certain products and services or visit certain websites. Unlike email spam, search engine rankings play a large role in blog spam.

People blogging on servers that have high page rankings in *Google* might find themselves besieged by more spam than someone blogging on their own personal server that does not have a high *Google* ranking. If *Google* thinks a site it ranks highly is linking to another site that appears lower in its search results, it might raise the rank of that site based on the authority of the links.

A high page rank often means heavy site traffic. If the site in question is selling anything (whether selling directly to the customer, or indirectly through advertising), heavier site traffic can translate into increased revenue. Thus, spammers use a variety of methods of blog spam to increase their page rank.

When weblog developers realized spammers were taking advantage of links in comments and trackbacks to increase their search engine page rank, many implemented a 'nofollow' tag in their link code. Adopters of the tag include *LiveJournal* and *Drupal*. The tag instructs search engine spiders not to follow links in an effort to quash spammers' attempts to increase their page rank.

The tag often appears in the HTML code for example:

```
<a href="http://www.virusbtn.com/" rel="nofollow">VB</a>
```

The blog software adds the tag to links automatically. Spiders from *Google*, *Yahoo*, and *MSN Search* obey the tag.

SPAM-BLOCKING TOOLS

Present-day spam-handling tools at the blog administrator level vary based on the blog software. Many platforms offer ways to delete comments and trackbacks en masse, at the post-level, or by other means.

On some group blogs, only the primary administrator(s) has spam-deleting capabilities, rather than any contributor. *WordPress* has the Akismet plug-in that learns what comments and trackbacks might be spam, captures them, and holds them for optional manual moderation before deleting them after a number of days. In *Manila* and several other platforms, it might be necessary to navigate through individual posts to control trackback or comment spam. Some tools, like *Blogware*, include an option at the user-level to delete and block selected spam.

Blocking spammers is not always the best or easiest option, though. Many spammers do not use the same IP address to attack weblogs, especially those who send out bots or scripts. Blocking an IP address is often, at best, a temporary measure and not very easy. It might be something the server administrator needs to do. Some spammers use common IP addresses, such as those from cafes, coffee shops, libraries and other places offering free wireless Internet access, or IP addresses from a particular Internet service provider (ISP). Blocking an IP address associated with one of these public locations or with an ISP might result in legitimate blog readers and even bloggers losing access to the weblog(s).

Some software gives bloggers the option of requiring people to register on the weblog before they can submit comments. While this works to keep some spammers and some scripts out, it is not a completely foolproof method. If the spammer is human instead of a bot, that person might simply register for access to the weblog. Also, some bots and scripts can get around required registration on some platforms. Blocking specific people from a weblog might be possible, but a persistent spammer will change their user profile on a weblog to gain access to it again.

Many platforms allow bloggers to choose whether the blog should offer comments. Since comments have become one of the main vehicles for blog spam, many managing editors consider turning them off. However, the comments form one of the main components of many weblogs. The blogosphere thrives on dialogue. Many bloggers want to be able to foster community, and turning off comments is often not what blog owners want to do.

TURINGS AND CAPTCHAS

It might be possible to add tougher registration requirements to weblogs. Completely automated public Turing tests to tell computers and humans apart, or captchas, like those that require someone to describe an image or translate text displayed in an image before they can post a comment to a weblog, do not work when the spammer is a human.

One method shows many different images and asks the viewer which one has a particular attribute, like a red umbrella, or fits an adjective, like 'cute'. While bots might not be able to handle a challenge-response test, it is probably only a matter of time before such bots include a way to test all of the possible image combinations and get past the captcha.

For now, captchas might help curb the number of spam blogs (unless a human is creating them). The free service *Blogger* once had such a severe problem with spam blogs that it caused problems for people using search engines like *Feedster*, one of the search engines specializing in blogs and XML feeds. Splogs were clogging the search results so badly that it was difficult to find legitimate weblogs. Circumstances like that not only make searching difficult, but can make a search engine look like it is full of worthless content.

It is possible that someone could hack into a free weblog-hosting site to use scripts to set up many spam blogs instead of having people create them manually. Security on that kind of blog-hosting site is often much better than it was a few years ago when blogging was a new thing that spammers had not yet completely usurped. *Blogger* addressed the problem they were having a few years ago, but splogs still exist. A search for 'Viagra' and 'Blogspot' in *Technorati* might reveal several splogs on *Blogger* to which that search engine gives top billing.

THE WAY TO GO

A blogger battling spam might often feel quite overwhelmed and as if he/she is fighting a losing battle. It seems like the spammers are always either way ahead of us, or else not very far behind. Whenever a new spam-curbing tool becomes available, spammers seem able to break through the barrier in a matter of weeks. Even armed with the best and toughest tools available, perhaps the best thing a blogger can do is hope that one day bloggers will win and spammers will lose. Regrettably, though, that does not seem likely.

Some developers believe that better captcha tools with wider adoption are the way to go. Many popular platforms do not yet offer those tools, and no one can really predict how well they might work until they are widely implemented and results are available.

Many bloggers want better server blocks. But what should they be and how should we implement them? Should individual bloggers be able to control those blocks or should only server administrators have that level of control?

What's particularly important, but sometimes lost in the shuffle, is for the servers on which bloggers work to be properly maintained, updated and secured. An insecure server can foster holes for spammers to fill and lead to a variety of problems that are worse than the average blogger might imagine.

With the constant spread of badware, keeping blogging systems up to date and securely patched has become critical. Several reports have floated through the blogosphere recently about blogs that have been hacked or spammed with links to badware. If such an attack is severe enough, it will take a considerable amount of effort and energy to repair the damage and make the weblog usable in a safe manner again.

CONCLUDING REMARKS

Despite the increases in spam during the last few years, many people are still happily blogging and reading weblogs. Although spammers pose lots of challenges to blog developers, the software is continuing to improve and offer more protection against spammers.

The only sure way to defeat blog spammers might be to stop blogging. For many people, that is simply not a desirable option.