AUGUST 2008

virus BULLETIN

Fighting malware and spam

CONTENTS

2 **COMMENT**
The secret life of old malware

3 **NEWS**
VB2008 Ottawa – call for last-minute papers
Neosploit business wound up
Security companies splash out

3 **VIRUS PREVALENCE TABLE**

4 **ROOTKIT ANALYSIS**
'Yet another Rustock analysis ...'

FEATURES
7 The case for AV for Linux: Linux/Rst-B
9 Improving heuristics

13 **COMPARATIVE REVIEW**
Windows XP SP3

28 **END NOTES & NEWS**

ISSN 1749-7027

IN THIS ISSUE

MORE RUSTOCK

The architecture of Rustock.C allows it to be put to use for pretty much any malicious task. Lukasz Kwiatek and Stanislaw Litawa describe a version of the rootkit used as part of a botnet.
page 4

HACK ATTACK

A high prevalence of Linux/Rst-B seen recently on hacked Linux boxes is not due to ingenious spreading mechanisms or Linux users swapping binaries, but a proliferation of infected hacking tools. Billy McCourt has the details of this real, in-the-wild Linux threat.
page 7

VB100: WINDOWS XP SP3

With a new set of samples to measure detection against, a new platform on new hardware and a selection of new products in the mix, John Hawes had his work cut out in this month's comparative review on Windows XP SP3.
page 13

vbSpam supplement

This month: anti-spam news and events, and Martin Overton looks at the use of CAPTCHAs in computer security and at how cybercriminals attempt to evade them.

virus BULLETIN COMMENT

'It may even come to pass that an entire class of malware gets forgotten because they are rarely heard of any longer.'

Kurt Wismer

THE SECRET LIFE OF OLD MALWARE

The traditional view of how AV vendors interact with malware is pretty straightforward: the vendor receives a sample of the malware, analyses it, creates a detection routine for it, and then moves on to the next one while the one they just dealt with begins its gradual decline towards eventual death. Only, death doesn't necessarily come easily for malware. Detection routines are a reasonably effective form of population control, but only where they actually get used.

That doesn't stop people from believing the malware has completely died out, however. After the malware falls off the WildList's radar (if it made it there in the first place) unconfirmed reports decrease in frequency until eventually it is forgotten about. It may even come to pass that an entire class of malware gets forgotten because they are rarely heard of any longer and because it is felt that they can't operate properly on today's hardware or software.

As the memory of such malware fades, it is easy to forget the security considerations and best practices that were peculiar to and/or prompted by such malware. While the advice to alter the boot sequence in BIOS used to be commonplace, it is rare to encounter it any more. Likewise, the advice to boot from a known-clean, bootable, write-disabled medium in order to scan a suspect system has largely been supplanted by advice to boot into 'Safe Mode' or even advice that goes straight to loading an online scanner in your web browser (not to detract from the convenience of such options, but they don't capture all the benefits of a true clean boot).

Another piece of advice rarely heard these days is to scan your floppy disks. That may seem quite reasonable – after all, who uses or even *owns* floppy disks any more? Increasingly computers are being sold without floppy drives so the threat posed by the oldest PC infection vector seems all but irrelevant. This is where the trouble begins though, because there *are* still computers with floppy drives and there are still people using them. Some may only use them once in a blue moon to get an old piece of data from their backups. Others may use them frequently, as many living in the many less affluent areas of the world have to make do with older hardware and software because it's all they can afford. With that in mind it no longer seems so strange that Stoned.Empire.Monkey took 10 years to fall off the WildList's radar, or that people were still reporting problems removing Form.A from Win98SE systems as recently as March this year.

Boot sector viruses are perhaps the best example of the persistence of old malware because they're the oldest and people are still getting exposed to them – even if they can't spread on modern systems, they can still infect them and pose as much of a problem as any trojan. But there are other examples, such as email worms like NetSky, which are still prevalent in spite of having been detectable for years, in spite of the widespread adoption of email gateway scanning that should be blocking them in transit, and in spite of the widespread adoption of email content controls that strip the very types of attachment they use.

The discovery of malware on consumer electronics like MP3 players and digital picture frames may pose a persistence problem because of inconsistencies we've already seen in the application of recalls, leaving malware-laden products in stores, warehouses, and maybe even on *eBay* for years to come.

Magazine issues that came with malware-laden CDs may quickly be forgotten, but will your local librarian know and have the resources to keep abreast of such potential threats hidden among the library's stacks? Books with CDs pose a similar problem not only for libraries but also for bookstores.

There are countless cracks and crevices like these for malware to hide in. Since users will forget how to protect themselves from old malware, and since AV solutions sometimes compound the problem by having older detection signatures removed or simply by not getting the opportunity to detect such malware (e.g. on-access scanners missing a BSI because the disk isn't accessed while the scanner is running), then, like some abandoned minefield from some long forgotten war, old malware will continue to find victims far into the future.

NEWS

VB2008 – CALL FOR LAST-MINUTE PAPERS

Virus Bulletin is seeking submissions from those wishing to present last-minute technical papers at VB2008, which will take place 1–3 October 2008 at the Westin Ottawa, Canada.

The conference will include a programme of 40-minute presentations running in two concurrent streams: Technical and Corporate, the running order for which can be seen at http://www.virusbtn.com/conference/vb2008/programme/.

In addition, a portion of the technical stream has been set aside for last-minute technical presentations, which will be selected by a committee consisting of members of the *VB* advisory board. The committee will be looking for presentations dealing with up-to-the-minute specialist topics.

Those selected for the last-minute presentations will be notified 14 days prior to the conference start, and will be required to prepare a 20-minute presentation to be given on the afternoon of Thursday 2nd October.

Those selected for the last-minute presentations will receive a 50% discount on the conference registration fee. Proposals must be sent to editor@virusbtn.com no later than **Friday 5th September 2008**.

NEOSPLOIT BUSINESS WOUND UP

We hear a lot lately that cybercrime these days is run in an organized fashion for profit. Proving that the cybercrime business is prone to the same economic pressures as the legitimate business world, it has been reported that the developers of the Neosploit infection kit have abandoned their business. Researchers at *RSA* believe Neosploit was finding it difficult to sustain its new customer acquisition rate, while existing customers were not generating sufficient revenue to sustain the rate of development.

SECURITY COMPANIES SPLASH OUT

Security vendors *Aladdin Knowledge Systems* and *Sophos* have both laughed in the face of the so-called global credit crunch and between them spent (or indicated their intent to spend) millions on new acquisitions in the last month. Anti-malware vendor *Sophos* has issued official notice of its intent to buy German encryption firm *Utimaco* in a share deal worth over $340 million. This will add encryption to the company's range of services which currently include anti-spam and network access control in addition to anti-malware. Meanwhile, *Aladdin Knowledge Systems*, which specializes in authentication and software DRM as well as content security, has announced that it will acquire the *Secure SafeWord* two-factor authentication technology from *Secure Computing Corporation* for approximately $65 million in a bid to strengthen its position in the authentication market.

Prevalence Table – June 2008

Malware	Type	%
Agent	Trojan	38.60%
NetSky	Worm	20.35%
Cutwail/Pandex/Pushdo	Trojan	14.52%
Rays/Traxg	Worm	4.36%
Clagger	Trojan	4.34%
Mydoom	Worm	4.19%
Mytob	Worm	4.02%
Bagle	Worm	1.56%
Buzus	Trojan	1.32%
Virut	Virus	1.13%
Zbot	Trojan	0.90%
Bifrose/Pakes	Trojan	0.70%
Mywife/Nyxem	Worm	0.66%
Sality	Virus	0.61%
Zafi	Worm	0.41%
Stration/Warezov	Worm	0.41%
Womble	Worm	0.23%
Sdbot	Worm	0.20%
Inject	Trojan	0.20%
FunLove/Flcss	Worm	0.13%
Bagz	Worm	0.13%
Lovelorn	Worm	0.11%
LovGate	Worm	0.07%
Forbot	Worm	0.07%
VB	Worm	0.06%
WMF	Exploit	0.06%
Nuwar/Peacomm/Zhelatin	Trojan	0.06%
Chir	Worm	0.05%
Nimda	Worm	0.04%
Sober	Worm	0.04%
Grum	Worm	0.04%
Thus	Macro	0.03%
Klez	Worm	0.03%
Others[1]		0.32%
Total		100.00%

[1]Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

ROOTKIT ANALYSIS

'YET ANOTHER RUSTOCK ANALYSIS...'

Lukasz Kwiatek, Stanislaw Litawa
ESET, Poland

In this article we are not going to talk about the history of this rootkit, nor will we talk about all the speculation that we have heard during the last year [1]. Instead, we will simply describe in detail a driver protector and an infector (which is also a disinfector), and then present an overall view of system hooks and a few of the self-defence techniques used by Rustock.C.

DRIVER PROTECTOR

The driver protector used by Rustock.C is very similar to some of the well-known ring 3 PE protectors. In this instance, we can find anti-debugging and anti-patching tricks, import table redirection, heavy code obfuscation, multiple encryption layers and so on. One 'old' new feature is hardware locking. Hardware locks are often used in commercial software protection schemes to avoid piracy and restrict usage to just one machine per licence. From the anti-virus industry's point of view, we should also take note of the fact that the infected driver doesn't have an import table.

In the Rustock.C protector, we can distinguish three protection layers:

- L0: very simple encryption (xor/sub/add-based)
- L1: initialization layer
- L2: actual protector layer

Since layer L0 consists of very simple encryption, it will not be discussed in detail.

LAYER L1

L1 is responsible for finding ntoskrnl (ntkrnlpa, ntkrnlmp, ntkrpamp) in memory and allocating a new memory buffer to which to copy itself. In a normal situation, analysis of this kind of protector would be very easy (even trivial), but this time we have to deal with a very advanced, multi-layer code obfuscator. During our research on Rustock.C, most of our time has been spent on the development of a deobfuscation tool to facilitate the analysis of the protector and the rootkit. So, what can we see in layer L1 after deobfuscation?

The functions for which it is responsible are:

- Searching ntoskrnl in memory – a well-known trick used by ring 3 packers.
- Obtaining the addresses of imported functions – functions are imported by 32-bit checksum value. This is also a very popular 'ring 3' trick (used, for example, in PESpin).

Layer L1 uses two functions from ntoskrnl: NtQuerySystemInformation with SystemModuleInformation as a parameter and ExAllocatePoolWithQuotaTag with the tag 'Info'.

When the whole driver (less the first few bytes) is copied to a new memory buffer, the execution flow is transferred immediately to that buffer.

LAYER L2

Layer L2 is the main layer of the protector. It handles decompression, decryption, filling of the import table, correction of the relocations and finally jumps to the original driver entry. The whole protection scheme is based on an encrypted structure that contains descriptions for each section, including the addresses and keys needed to handle imports and relocations.

Each section is compressed with aPLib and encrypted with the RC4 algorithm. The key for RC4 is constructed from three dwords, the third of which is stored in the protected driver (whose structure was mentioned earlier). The first two dwords are collected from the PCI bus. Data gathered from the PCI bus can be identified as the DeviceID and VendorID for the following two devices:

- Bridge device – 'Host/PCI'
- Bridge device – 'PCI/ISA' or 'Other'

The DeviceID and VendorID are 16-bit values – those values (in particular VendorID) can be found on a small number of lists on the Internet. The full decryption key will have the following format:

```
0xDDDDVVVV 0xDDDDVVVV 0xXXXXXXXX
```

DDDD – DeviceID
VVVV – VendorID
XXXXXXXX – from the protected driver

After RC4 initialization we can observe 111 'empty' rounds. These are used to slow potential brute-force attacks and to randomize the final encryption. After these 111 rounds, there are four more rounds from which the 32-bit key is constructed. This key will be used to decrypt the import table and relocations.

The relocation table is represented in a simpler form than normal relocations from PE executables. In Rustock.C, relocations are an encrypted table of addresses that need to be fixed with the base address of the module.

Imports are encrypted in a similar way to relocations. Each imported function is represented as a nine-byte structure:

```
DWORD relativeAddress;
DWORD checksum;
BYTE unknown;
```

To rebuild the import table, we need to match checksum values with the names of functions. Imported functions are

called through another function that checks for standard software breakpoints (0xCC) and debug breakpoint registers (dr0, dr1, dr2, dr3) at the beginning of the imported function.

The Rustock.C protector also incorporates a few anti-debugging tricks:

- the clearing of debug registers
- the setting of empty functions for all IDT entries
- memory checksums

Technical details on the protector, including keys and code snippets have been published elsewhere [2].

DRIVER INFECTOR

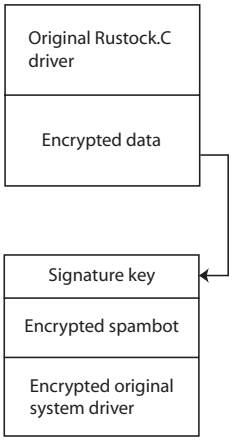


Figure 1: Infected driver structure.

Rustock.C is a driver infector, which means that after the first infection it is not dependent on any other file in order to work. The infected driver has a very simple structure, as shown in Figure 1.

The infected driver is almost identical to the original Rustock.C driver except for the last section and a few values in the PE header. In the last section we can see the encrypted structure with a spambot and the original driver. In fact, the code responsible for searching for that structure in Rustock.C allows the structure to be placed anywhere in the driver. The signature and key structure is rather easy to verify: it is 16 bytes (four dwords) long. The first dword is used as a decryption key and the next three values are used to validate the signature:

```
dword01 = decryption key
dword02 = dword01 - 0x747517C7
dword03 = dword01 ^ 0x945133B7
dword04 = dword01 - 0x0FCFD0AC
```

Data is decrypted with a 'xor-based' algorithm:

```
DWORD* data = addr_of_sig + 0x94;
for (i = 0; i < size; i++)
{
   data[i] ^= dword01;
   dword01 += 0x945133B7;
}
```

At the beginning of the decrypted buffer we have three variables:

```
DWORD offset;   //
DWORD size;     // x3
BYTE key;       //
```

The offset is relative to the beginning of the signature. The key is a one-byte value used for XOR encryption. The first structure describes botdll.dll (the spambot module injected into winlogon or services). Botdll.dll is encrypted with a one-byte XOR and compressed with aPLib. The second structure describes the original driver in a similar way to the first one, with the exception of compression. The original driver is just XORed with 'key', and after decryption mapped into memory at the base address of the infected driver. This is the reason why the rootkit body is copied to a new memory buffer during the unpacking stage.

SELF DEFENCE

Rustock.C uses several techniques to protect itself:

- Timer1 checks KdDebuggerEnabled
- Timer2 searches the memory space of all loaded drivers for the following strings:
  - 'NTICE'
  - 'Syser'
  - 'BPLOAD'
  - 'BPLoad'
  - 'ISO_S_'
- The rootkit memory is cleared in case of bugcheck (KeRegisterBugCheckCallback)
- Inline hooks are set on the functions following the functions from the file system driver IRP table.
  In Ntfs.sys:
  - NtfsFsdCreate
  - NtfsFastQueryStdInfo
  - NtfsFsdClose
  - NtfsFsdDirectoryControl
  - NtfsFsdDispatchWait
  - NtfsFsdRead
  - NtfsFsdSetInformation
  - NtfsFsdWrite

  File system hooks are responsible for hiding the rootkit: any attempt to read the infected driver causes on-the-fly disinfection and returns data from the original driver, while the driver remains infected. Also, the size of the driver can be seen from the original file.
- The inline hook on KiFastCallEntry is used to hook some functions from the ServiceDescriptorTable:
  - ZwQuerySystemInformation
  - ZwCreateThread
  - ZwTerminateThread
  - ZwResumeThread
  - ZwOpenThread
  - ZwReadVirtualMemory
  - ZwWriteVirtualMemory
  - ZwProtectVirtualMemory
  - ZwDuplicateObject

- ZwDelayExecution
- ZwTerminateProcess
- ZwCreateUserProcess (*Vista* only)
- ZwCreateThreadEx (*Vista* only)

These hooks are used to protect and hide botdll.dll in winlogon.exe (or services.exe on *Windows Vista*). ZwQuerySystemInformation is called with special parameters and used to access functions from the rootkit (ring 3 to ring 0 communication).

- Infection can easily migrate to another driver and disinfect the current infected file. Infected drivers must be in the following registry path: '\Registry\Machine\System\CurrentControlSet\Control\SafeBoot\Minimal'.
- Firewall bypassing techniques are employed (a few hooks on tcpip.sys, ndis.sys, wanarp.sys).

CONCLUSION

Analysis of Rustock.C would be much easier without the advanced code obfuscation (218 KB of obfuscated code versus 70 KB of clear, optimized code). In the future, we will probably see rootkits with private kernel-mode code virtualizers (similar to commercial products like *VMProtect* or *Code Virtualizer*) becoming more popular. This version of Rustock.C was used as a part of a spam botnet, but the architecture of the rootkit allows it to do anything (password stealing, phishing attacks, DDoS and so on). The botdll.dll file is appended like a plug-in that can be easily changed to another spam-sending module [3] or anything you want. Who knows, maybe there is another variant of Rustock.C in the wild...

REFERENCES & FURTHER READING

[1] http://www.rootkit.com/newsread.php?newsid=879.

[2] Kwiatek, L. Rustock.C – kernel mode protector. http://www.eset.com/threat-center/blog/?p=127.

[3] Shevchenko, S. http://blog.threatexpert.com/2008/06/new-rustock-switches-to-hotmail.html.

[4] Shevchenko, S. Rustock.C – unpacking a nested doll. http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html.

[5] Florio, E.; Pathak, P. Raising the bar: Rustock and advances in rootkits. Virus Bulletin, September 2006.

[6] Molenkamp, S.; O'Dea, H. Have you got anything without spam in it? Proceedings of the Virus Bulletin Conference, September 2007.

[7] Rusakoff, V. http://www.drweb.com/upload/6c5e138f917290cb99224a8f8226354f_1210062403_DDOCUMENTSArticales_PRDrWEB_RustockC_eng.pdf.

FEATURE 1

THE CASE FOR AV FOR LINUX: LINUX/RST-B

Billy McCourt
Sophos, UK

In February researchers at *SophosLabs* noted that Linux/Rst-B seemed to be very common on hacked *Linux* boxes [1]. The prevalence of this particular virus is not due to ingenious spreading mechanisms or *Linux* users swapping binaries, it is due to a proliferation of infected hacking tools. The fact that the virus replicates equally well on older and newer kernels will have added to its longevity – a characteristic that isn't always found in other *Linux* viruses.

LINUX/RST-B

We became interested in Linux/Rst-B when we noticed that around 70% of executable files downloaded to one of our honeypots were infected. Underneath the Linux/Rst-B infection were various tools such as flooders, SSH scanners and, more often than not, an IRC bot.

A particularly interesting feature of Linux/Rst-B is that it attempts to download a page from a specific IP address if it is executed as root. The *Ethereal* screenshot in Figure 1 shows the request being made to 207.66.xxx.xxx/~telcom69/gov.php.

This call-home technique provides the opportunity to assess the number of Linux/Rst-B root-compromised *Linux* boxes in the real world. The call home IP address falls under the control of *Accretive Networks* [2], who kindly agreed to assist us with our research.

DATA TRACKING

Since the beginning of May, we have had the call-home IP address hooked up to a web server and connection attempts to the specific URL have been logged. From this data, we can cross-reference the infected IP address with WHOIS data to find out details such as the country and company of an infected host. The data presented in this article is based on roughly five weeks' worth of logs.

One of the first sets of statistics that we generated was the number of infections by country. We take a single instance of each IP address that has called home and look up which country it came from:

Country	Unique infected IPs
USA	1,271
China	622
Germany	428
Brazil	389
Taiwan	264
Korea	247
France	240
Italy	212
India	209
Poland	176

Table 1: Number of infected IPs by country.

This data helps to show that this is a global problem. When these statistics were generated there were IP addresses from over 125 different countries calling home.

Figure 2 highlights that Europe is pretty badly hit. Each red marker represents a single IP address.

Another way to look at the data is to examine the frequency of each IP address calling home. Table 2 shows the most

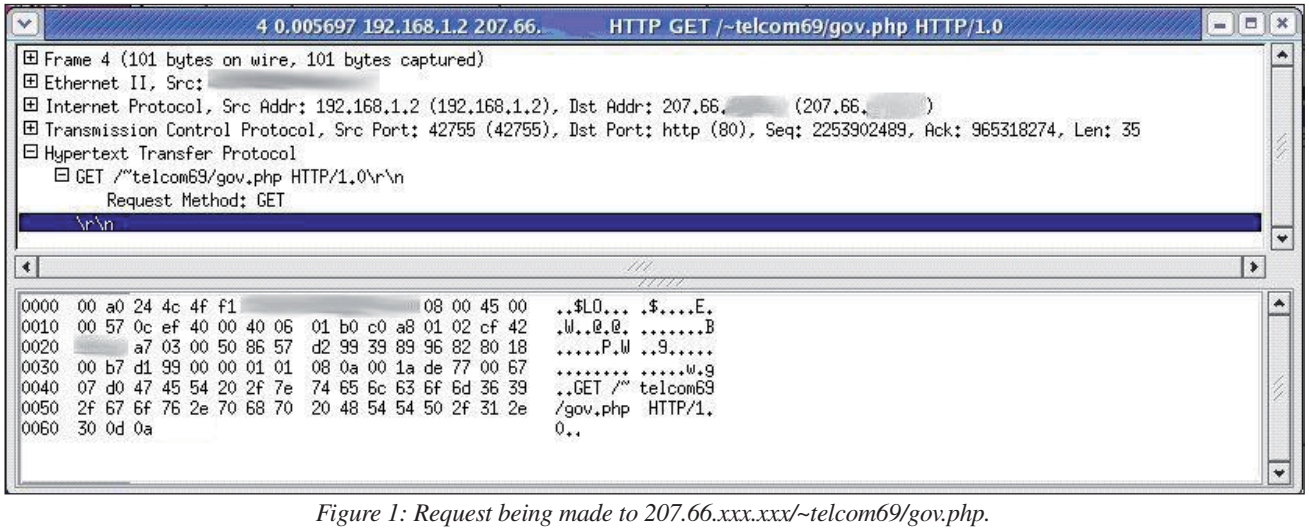


Figure 1: Request being made to 207.66.xxx.xxx/~telcom69/gov.php.

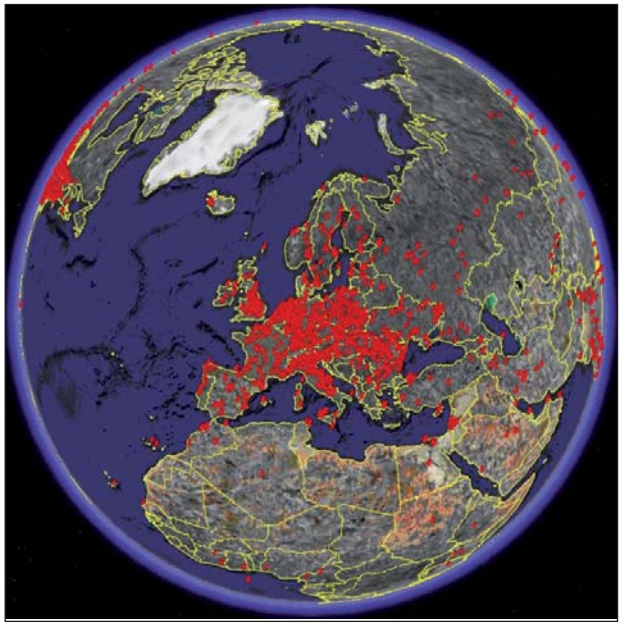


Figure 2: Location of infected IP addresses.

IP address ID	Country	Count
62.93.xxx.xxx	Germany	21,877
62.93.xxx.xxx	Germany	6,861
216.147.xxx.xxx	USA	5,498
75.26.xxx.xxx	USA	1,748
206.191.xxx.xxx	Canada	838
62.141.xxx.xxx	Germany	749
66.175.xxx.xxx	USA	649
88.146.xxx.xxx	Czech Republic	505
59.175.xxx.xxx	China	381
65.163.xxx.xxx	USA	152

Table 2: The most common IP addresses calling home.

common IP addresses calling home. This is an interesting result since it allows us to monitor activity tied to specific hosts. The most common call home attempts were made by computers in Germany. (Note that the first two IP addresses were from the same provider so could really be considered as a single IP address with a total of 28,748 hits.)

It would be nice to assume that these figures are the number of infected machines but it is clearly not that straightforward (due to computers behind NAT gateways etc. where many computers will be represented by a single IP address). Also, whilst a server that is never turned off will only ever call home once, a computer that is rebooted daily will call home after each reboot (assuming appropriate binaries have been infected, but this is a fair assumption if the virus has been executed as root).

Germany therefore may simply have more *Linux* computers being used as workstations and being rebooted frequently. However, even if we assume that every machine is booted up at least once a day, this still suggests that there are over 750 root-infected machines sitting behind two IP addresses alone.

It is also important to remember that we can only gather statistics for root-compromised computers. Our honeypots show that hackers are happy to gain access to standard user accounts (we don't allow root to SSH in) – only a tiny percentage of attackers have downloaded and executed a root exploit before downloading their other tools. From this we can safely assume that the actual number of infected *Linux* boxes is far higher than our results suggest.

AV FOR LINUX?

Hopefully every *Linux* AV scanner is able to detect Linux/Rst-B. It has been around for over six years and, according to our research, it is the virus you are most likely to encounter as a *Linux* user. Simply running an on-access scanner would prevent most hacking attempts from achieving anything destructive. Whilst on-access scanners don't address any underlying security issues (weak passwords, vulnerable web applications etc.) they should at least make you aware of hacking attempts without major damage being done.

Unfortunately, it is probably only script-kiddie-level hackers that use hacking tools infected with Linux/Rst-B. Hackers with financial motivation will no doubt be more meticulous with their choice of tools, providing more of a challenge for AV vendors to detect proactively.

We chose to investigate this particular virus partly due to its call-home feature (it gives a fairly accurate picture of real-world infections), but also since it is a real, in-the-wild, *Linux* threat. The longevity of these infections indicates that system administrators are not even running on-demand scans or file integrity checkers, despite appropriate tools being readily available on many common distributions.

It doesn't take much searching to find a *Linux* zealot claiming that malware is only a *Windows* problem – hopefully these figures will make users reconsider their approach to *Linux* security.

REFERENCES

[1] Botnets, a free tool and 6 years of Linux/Rst-B. http://www.sophos.com/security/blog/2008/02/1062.html.

[2] Accretive Networks. http://www.accretive-networks.net/.

FEATURE 2

IMPROVING HEURISTICS

Newaz Rafiq, Yida Mao
Zheng Group, Paretologic, Canada

With proven accuracy, predictability, performance and scalability, heuristic detection can provide valuable assistance to help security analysts in achieving zero-day malware detection. In this article we will discuss a novel heuristic detection technique with two major advantages:

- A consistently high level of accuracy in malware prediction.
- A high level of adaptability to meet the challenge of new malware.

MODEL

Our approach starts with a model that resembles the behaviour of our security analysts.

To make a prediction about a sample we need to extract features from it, just as security analysts collect features from the sample executables. Analysts have prior knowledge of malware features. They know which features characterize malicious behaviour and which indicate non-malicious files. They decide whether a sample is malicious or not based on their prior knowledge of its features. But some of the features will be new to the analysts, in which case they upgrade their prior knowledge by adding details of the new features. Our system works in exactly the same way. Figure 1 shows the model on which our automatic file classification system is based. As an automated heuristic approach alone cannot be relied on to give 100% accurate detection, a manual check is incorporated before committing any new features to a knowledge base.

FEATURE EXTRACTION

Features can be extracted from the static and run-time behaviours of malware samples. We are able to extract hundreds of features from each executable; some of the most notable ones are described here:

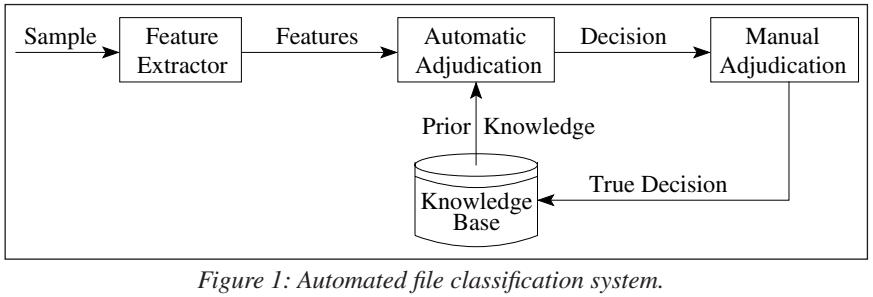


Figure 1: Automated file classification system.

File size

File size has been shown to be an important feature both in our investigations and in other studies [1]. In our initial experiments we divided executables into three groups based on their file size:

- Group 1: executables whose file size was smaller than 1 MB.
- Group 2: executables whose file size was smaller than 5 MB and greater than or equal to 1 MB.
- Group 3: executables whose file size was greater than or equal to 5 MB.

After normalizing the counts in each group, we arrived at the results shown in Table 1.

Group	Malware (%)	Non-malware (%)
1	53	47
2	58	42
3	3	97

Table 1: File size statistics.

According to Table 1, samples contained in groups 1 and 2 have an approximately equal chance of being malicious or non-malicious, thus the file size does not reveal any useful information for malware detection. However, executables belonging to group 3 (file size >5 MB) are significantly more likely to be non-malicious than malicious.

Obfuscation

In our investigations we divided the executables into two groups: obfuscated and non-obfuscated. Obfuscation can be achieved by packing the full sample or a portion of the sample binary, by reordering instructions, and so on. We found that approximately 60% of recent malware is obfuscated. We determined that if an executable is obfuscated, there is a greater than 95% probability that it is malware.

Sections

An executable consists of sections, such as header, text, code and so on. There are generally fewer sections in malicious files than in non-malicious ones. In our analysis, more than 70% of the malware samples consisted of two or three sections, while more than 70% of non-malicious files consisted of four or five sections. In further analysis focusing

on section names, we found that over 80% of malicious programs used unconventional section names, whereas only 3% of non-malicious programs used unconventional names. We also found that some executables used duplicate section names, although this was very rare (only 4%). If there is a duplicate section name, then there is a more than 95% probability that the executable is malware. We found that use of the resource section (.rsrc) was a good indicator of a sample being malicious (with more than 70% probability), the presence of read-only data (.rdata) meant that the sample had a greater than 70% chance of being non-malicious, and the presence of import data (.idata) was also a good indicator of the sample being non-malicious (with more than 80% probability).

Anomaly

Another notable feature relates to peculiarities in the executable structure – for example, some sections in the executable may not be aligned properly. In our analysis, more than 78% of malware revealed an anomaly in the executable structure, while only 5% of non-malicious samples had an anomaly in their structure. If an anomaly exists, there is a more than 93% chance that the sample is malicious.

BHOs

Browser Helper Objects (BHOs) are program modules (DLLs) designed as plug-ins to provide added functionality for *Microsoft*'s *Internet Explorer* web browser [2]. BHOs have access to all the events and properties of a web-browsing session [3]. This means they give developers almost complete control over *Internet Explorer* functionality. For malware writers this is a compelling reason to use BHOs.

According to our analysis, if an executable uses a BHO, it can likely be classified as malware with 98% probability.

Services

Services are employed to enable long-running executable applications to run in their own *Windows* session [4]. These services can be started automatically when the computer boots, can be paused and restarted, and do not require a user interface. Services start when the *Windows* operating system is booted and they run constantly in the background as long as *Windows* is running. Services can run for a specific user account that is different from the logged-on user or the default computer account.

According to our analysis, if an executable runs as a service, it can likely be classified as malware with 98% probability.

Imports

As part of our investigations we also calculated statistics relating to the importing of DLL files. For example, if an executable imports system32.dll, then the sample has a more than 77% chance of being malware and if it imports kernel32.dll, then the sample has a more than 67% chance of being malware.

FEATURE SELECTION

The accuracy of malware detection depends heavily on the selected features on which predictions are made [5]. Figure 2 shows our experimental results using two different feature selection algorithms. From Figure 2 we can conclude:

- An increase in the number of features does not guarantee better detection.
- A feature selection algorithm should be chosen carefully.

To understand how feature selection helps in the malware detection process, assume that we have 500 items, of which half are malicious and half are non-malicious. These will be used to train our system. Also assume that we have detected three features: A, B, and C, for each of the 500 samples.

From our statistical analysis, we obtain the information content of each feature, as shown in Table 2.

In our model, we assign samples a 'likelihood' score. The closer the likelihood score is to one the more likely it is to be malware, and the closer the score is to zero the more likely it is non-malicious.

Feature	A	B	C
Information	0.10	0.90	0.80

Table 2: Information content of three features.

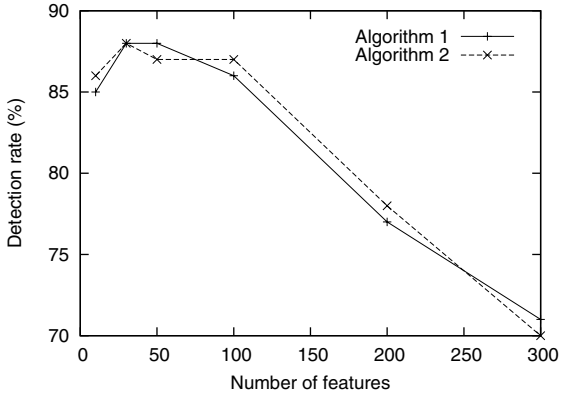


Figure 2: Detection rate as the number of features varies.

Now assume that an executable X has two features: A and C. The likelihood scores for X according to the features selected are given in Table 3.

Table 2 indicates that more information can be drawn from feature C than from feature A. This is also reflected in Table 3. If the feature selection algorithm selects A, then the likelihood score for X is 0.49, which is inconclusive. A similar score is achieved when two features, A and C, are selected for the adjudication process. But if feature C alone is selected the likelihood score is 0.88, which tells us that X is malware.

Feature	A	B	C	A,C
Likelihood score	0.49	0.10	0.88	0.43

Table 3: Likelihood scores for X according to selected features.

For this reason, feature selection is very important for malware detection. We have devised a few simple and time-efficient techniques to select the most informative features that produce a high accuracy of malware predictability. Some of these have been published in our previous work [6].

AUTOMATIC DECISION MAKING

There are many classification algorithms at our disposal. Currently we are using the naive-Bayes classification algorithm as it is both accurate and simple to implement. The simplified algorithm (assuming that there are only two classes: malware and non-malware) is given in Equation (1).

$$P(c|\mathrm{x}) = \frac{P(\mathrm{x}|c)}{P(\mathrm{x}|c) + P(\mathrm{x}|1-c)} \quad (1)$$

Where $\mathrm{x} = [x_1, x_2, \cdots, x_n]$ is an array of selected features from an executable, $P(c|\mathrm{x})$ is the a posteriori probability that the executable with feature set x is in class c, and $P(\mathrm{x}|c)$ is the probability of x occurring in class c.

EVALUATION OF OUR SYSTEM

To evaluate our system, we use the following quantities:

- True positive (TP): the number of malicious files classified as malware.
- True negative (TN): the number of non-malicious files classified as non-malware.
- False positive (FP): the number of non-malicious files classified as malware.
- False negative (FN): the number of malicious files classified as non-malware.
- True positive rate (TPR):

$$\mathrm{TPR} = \frac{\mathrm{TP} \times 100\%}{\mathrm{TP} + \mathrm{FN}} \quad (2)$$

- False positive rate (FPR):

$$\mathrm{FPR} = \frac{\mathrm{FP} \times 100\%}{\mathrm{FP} + \mathrm{TN}} \quad (3)$$

- False negative rate (FNR):

$$\mathrm{FNR} = \frac{\mathrm{FN} \times 100\%}{\mathrm{FN} + \mathrm{TP}} = 100\% - \mathrm{TPR} \quad (4)$$

- Detection rate (DTR):

$$\mathrm{DTR} = \frac{(\mathrm{TP} + \mathrm{TN}) \times 100\%}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad (5)$$

FINE-TUNING OF PARAMETERS

K-fold cross validation is one way to determine the characteristics of an algorithm. In this technique, the data set is divided into k subsets. One of the k subsets is used as the test set and the other $k-1$ subsets are merged together to form a training set. The advantage of this technique is that each sample contributes to the system performance.

We fine-tuned several parameters using the cross-validation technique, but we describe only one of them here: number of features.

To begin, we used around 7,000 known executables (54% of which were malware) to train our system and to fine-tune the initial system parameters. We varied the number of features from five to 30 and plotted the results as shown in Figure 3.

As can be seen in Figure 3, our detection algorithm produces the best DTR when the number of features is 15, the best FPR when the number of features is 20, and the best FNR when the number of features is 10. For this reason, we experimented with our algorithm using newly detected malware samples when the number of features was 15. The results are described in the following section.

EXPERIMENTAL RESULT

We used one group of non-malware and 28 released malware groups that had been detected by our analysis team in recent months. Each group contained around 150 to 300 samples. We plotted the results of our experiment in Figure 4. A smooth, dashed curve shows the recognition

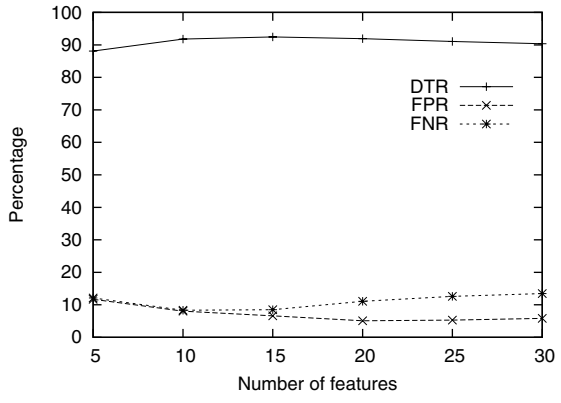


Figure 3: Detection rate as the number of features varies.

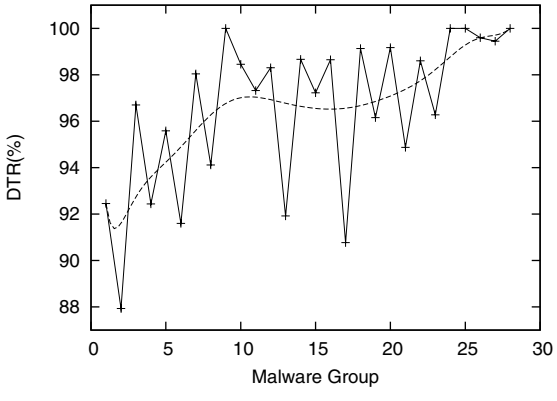


Figure 4: Detection rate across malware groups.

pattern. In almost all cases, the malware recognition rate is above 90%. As the automatic decision-making system is trained using more malware samples, the system utilizes more features and accuracy continues to rise to 100%. Our system is currently recognizing non-malware with more than 90% accuracy.

CASE STUDY

To gain an understanding of why our system is not 100% accurate, we have referenced the features of two malicious and two non-malicious samples in this section. We consider only those notable features that were described earlier. The features shown in bold are malware-characterizing features and the rest are non-malware-characterizing features.

Malware sample 1:	**number of sections = 2**, no resource usage.
Malware sample 2:	**kernel32.dll**, **anomaly**, no. of sections = 5, import data.
Non-malware sample 1:	**kernel32.dll**, **user32.dll**, **anomaly**, no. of sections = 5, read-only data.
Non-malware sample 2:	**kernel32.dll**, **unconventional name**, **anomaly**, **obfuscation**, import data, read-only data.

From the above information we can conclude that each malware sample has some malware-characterizing features. However, non-malware-characterizing features overpower the effect of malware-characterizing features. The same is true for non-malware. This means we are very unlikely to achieve 100% detection. However, by using diverse features and a more interesting feature selection algorithm we can attempt to achieve a close to perfect detection rate.

CONCLUSION

The main features of our automatic file classification technique are as follows:

- The ability to extract hundreds of features.
- An intelligent feature selection algorithm.
- The ability to fine-tune system parameters.
- The option to update the knowledge base easily.

We are consistently getting more than 90% accuracy detection of malware. The FPR of our system is around 10% and we are trying to reduce this by extracting new features and by developing a new feature selection algorithm.

REFERENCES

[1] Lu, B. A deeper look at malware – the whole story. Proceedings of the 17th Virus Bulletin International Conference, 2007, pp.9–17.

[2] http://en.wikipedia.org/wiki/Browser_Helper_Object.

[3] http://www.spywareinfo.com/articles/bho/.

[4] Introduction to Windows service applications. http://msdn2.microsoft.com/en-us/library/d56de412(VS.80).aspx.

[5] Goodman, S.; Hunter, A. Feature extraction algorithms for pattern classification. Proceedings of Ninth International Conference on Artificial Neural Networks, vol. 2, 1999, pp.738–742.

[6] Rafiq, A. N. M. E.; Mao, Y. A novel approach for automatic adjudication of new malware. Proceedings of The 12th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2008 (to be published).

COMPARATIVE REVIEW

WINDOWS XP SERVICE PACK 3

John Hawes

This month the VB100 test schedule rolled around once again to the *Windows XP* test – which was expected to be the most heavily subscribed of the year. However, a handful of withdrawals and no-shows meant that the crowd of submissions fell mercifully short of the 40 or so it had threatened to reach, but still promised to keep me busy throughout the test period. A new batch of test systems was ordered in time for this review – but unfortunately, half the shipment didn't arrive until well into the testing period, which actually slowed testing down rather than streamlining it. Hoping that most of the products – by now fairly familiar to me – would move on and off the test bench at a reasonable rate, a sprinkling of new names piqued both interest and apprehension, as did news that many of the regulars would be submitting heavily updated or redesigned versions. Some major updates to the zoo test sets, part of an ongoing programme of improvements, also added a new zest to this month's test.

PLATFORM AND TEST SETS

As testing for this comparative got underway, something of a milestone in the history of the *Windows XP* platform was reached – on 30 June, most versions of the operating system ceased to be sold via most OEM and retail channels. Licensing will continue to be available for 'System Builders' until January 2009, and in April official support for the platform will be downgraded to an 'extended' period set to continue until 2014. These first steps towards putting the platform out to pasture seem somewhat premature, given its continuing popularity and massive market penetration.

With its slicker, more advanced successor *Windows Vista* now well past its launch stage and settled in as the default (and in many cases only available) operating system for new PCs, *Windows XP* has maintained its dominance as the platform of choice for the majority of PC users. Looking at a selection of studies of platform usage, *XP*'s figures are declining very slowly, currently estimated as being in use on around 75% of systems while *Vista* has crept up to 15%. Many businesses continue to run *XP* on their workers' desktops, even where this entails removing *Vista* from new purchases. At this rate, *XP* looks set still to be the most widely used *Windows* version when the next new release, the successor to *Vista* currently going by the title 'Windows 7', hits the shelves – currently scheduled for around two years' time.

Adding further to the longevity of *XP* is the latest service pack, released a few months ago and added to the Automatic Update system during July. The update contains a number of new features, many of which are related to security, authentication and encryption, but for the majority of users is expected to make little obvious impact. In the weeks following initial release of the service pack, a number of issues were spotted arising from clashes between various aspects of the update and a selection of third-party anti-malware and security products, but most were quickly resolved. This test should see products at the top of their game, on a mature and stable platform, but as usual there is no knowing just how the range of updates will affect the products during the in-depth grilling applied on the *VB* test bench.

The toughness of this month's test was kept to a minimum thanks to an early deadline (intended to allow adequate time to deal with the anticipated glut of entries), which meant that the release of the May 2008 WildList narrowly missed the cut-off date for this month's test. The test sets were frozen on 20 June, using the April WildList for the core certification set, with the product submissions taken and frozen on 24 June.

The false positive set saw its usual expansion with new files and packages, and the other test sets were also extended somewhat, most notably the polymorphic set which saw several new items introduced in fairly limited numbers. This will be added to over the next few months as further generations of samples are replicated and verified.

The legacy set of older and more obscure items was left out of this test, something which has been planned for some time. Interest in such items continues to fluctuate, with a surprising number of macro and even DOS viruses still cropping up on the prevalence reports we gather, and this set may occasionally be resurrected for server tests where it has more relevance. In its place is a new set of trojans, an introductory selection of several thousand samples gathered over the course of the last six months or so. This move heralds a planned expansion in this direction for the *VB* sets, and we hope to have further improvements in the upcoming tests.

With an entirely new set of samples to measure detection against, a new platform on new hardware and a selection of new products, I expected the month of testing to be eventful, so I quickly got down to the lab and started testing.

Agnitum Outpost Security Suite Pro 6.0.2296.253.0490

ItW	100.00%	**Polymorphic**	77.32%
ItW (o/a)	100.00%	**Trojans**	84.22%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Agnitum's suite was reviewed in depth a few months ago (see *VB*, January 2008, p.17) and remains little changed on the surface. The installation process is rather protracted, both in terms of the selections required of the user and in the time taken to perform the installation, with a reboot required at the end to get things going. The complexity of the installation process is explained by the wide range of security extras, in particular the firewall for which *Agnitum* is renowned. The anti-malware component, supported by the *VirusBuster* scanning engine, receives minimal attention in the interface design. Configuration is fairly limited, particularly for the on-access scanner, and the layout of the manual scanning system a little fiddly, but the default setup and the few available options proved ample for most of my needs.

The product ran smoothly and with rock-solid stability, racking up some reasonable if not superb scanning speeds, decent coverage of the trojan test set and no issues at all in the WildList or clean sets, thus easily qualifying for a VB100 award.

Ahnlab V3 Internet Security 7.0 Platinum Enterprise 7.6.3.1

ItW	99.99%	**Polymorphic**	92.86%
ItW (o/a)	N/A	**Trojans**	84.34%
Worms & bots	99.81%	**File infectors**	97.64%
False positives	0		

Ahnlab's offering is another full suite, boasting a range of modules including anti-virus, anti-spyware, anti-hacking (which comprises a personal firewall and intrusion prevention elements), privacy control and email protection. The setup and installation process is much less complex than might be expected however, with no reboot required, and protection is up and running very quickly. A prompt requesting approval of the activities of svchost.exe pops up even before the installation is complete. Whether such a prompt would help the majority of users, who would be unlikely to understand its implications and may well simply click 'allow' without further thought, is perhaps somewhat questionable, but it does indicate a thoroughness of protection available to those with the understanding to apply it properly.

Configuration was rather limited and the layout a little confusing, with some options held in a central location while others appeared on specific sections for each module, and again the system for setting up a scan was somewhat awkward. Scanning speeds were pretty unexceptionable, but measurements were hampered by several crashes during the running of the speed tests, requiring them to be restarted.

Worse, while running the on-access detection tests the system crashed completely, with the famous blue screen putting in a rare appearance. Several repeat attempts brought similar results. On contacting the developers, it emerged that an engine update may have introduced issues with the handling of polymorphic items, thus causing the crashes. Having been unable to complete the on-access component of the test, *Ahnlab* does not qualify for a VB100 award on this occasion.

Alwil avast! 4.8.1214

ItW	100.00%	**Polymorphic**	88.78%
ItW (o/a)	100.00%	**Trojans**	97.66%
Worms & bots	99.48%	**File infectors**	96.06%
False positives	0		

Alwil's ever-popular *avast!* seemed much the same as ever, although apparently a new suite offering has recently been added to the company's line-up (something I hope to have a closer look at in the near future). For now the traditional design continues to frustrate somewhat while providing ample control and configuration for those who can find it. The installation was simple but required a reboot of the system, with the option to launch a scan immediately on restart.

Default settings are fairly limited in depth, with the on-demand scanner ignoring files with extensions not expected to be used by malware, although the on-access component checks further in depth and was able to spot the EICAR test file despite a random extension. Archives were likewise ignored in the default settings but covered flawlessly when requested. Speeds were splendid, remaining fairly good even with more paranoid settings, and detection rates were also excellent, including very impressive coverage of the new trojan set. With nothing in the WildList set missed and no false positives, *Alwil* adds another VB100 award to its tally.

ArcaBit ArcaVir 08.06.3218.4

ItW	95.80%	**Polymorphic**	94.16%
ItW (o/a)	95.80%	**Trojans**	76.12%
Worms & bots	99.78%	**File infectors**	98.62%
False positives	10		

ArcaBit was unfamiliar to me prior to this review, but it has some history in VB comparative testing with two entries in 2005, coming very close to achieving VB100 certification (see *VB*, February 2005, p.12 and *VB*, June 2005, p.11). The company is based in Warsaw, Poland, and provides a full

On-access detection	WildList		Worms and bots		File infectors		Polymorphic		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.91%	8	99.21%	317	77.32%	347	84.22%		
Ahnlab V3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
Alwil avast!	0	100.00%	6	99.48%	6	96.06%	322	88.78%	51	97.66%		
ArcaBit ArcaVir	182	95.80%	3	99.78%	6	98.62%	55	94.16%	525	76.12%	10	2
AVG Internet Security	0	100.00%	1	99.94%	1	99.21%	52	89.95%	58	97.36%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	38	98.27%		
BitDefender AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	116	94.75%	3	
Bullguard	2	99.92%	12	99.22%	2	98.95%	0	100.00%	96	95.62%	2	
CA AntiVirus + AntiSpyware	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
CA eTrust	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
eEye Blink Professional	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	238	89.20%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	92	95.54%	1854	15.73%		
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	0	100.00%	90	95.65%	250	88.63%		
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	30	98.55%	129	94.15%		
F-Secure Protection Services	0	100.00%	0	100.00%	0	100.00%	30	98.55%	129	94.15%		
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	21	99.04%		
K7 Total Security	0	100.00%	5	99.61%	5	97.32%	1072	64.74%	455	79.33%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	30	98.55%	137	93.79%		
Kingsoft Internet Security	0	100.00%	15	98.97%	87	81.89%	2009	42.15%	662	69.91%	1	
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	341	84.52%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	0	100.00%	90	95.65%	106	95.17%		
Norman Security Suite	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
NWI Virus Chaser	12	98.27%	0	100.00%	0	100.00%	90	95.65%	93	95.77%		2
PC Tools AntiVirus	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		
PC Tools Spyware Doctor	0	100.00%	2	99.91%	8	99.21%	313	77.70%	407	81.52%		
Proland Protector Plus	162	99.53%	5	99.48%	59	90.79%	1722	46.38%	1973	10.30%		
Quick Heal AntiVirus	0	100.00%	53	93.15%	10	98.03%	908	81.51%	1465	33.40%		
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	90	95.65%	102	95.38%		
Rising Antivirus	0	100.00%	2	99.81%	41	94.33%	1302	52.19%	292	86.74%		
Sophos Endpoint Security & Control	0	100.00%	0	100.00%	0	100.00%	90	95.65%	46	97.93%		33
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	90	95.65%	38	98.29%		
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	561	87.72%	40	98.20%		
VirusBuster Professional	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		2
Webroot AntiVirus with AntiSpyware	0	100.00%	4	99.48%	0	100.00%	107	95.06%	50	97.75%		

range of products including support for a range of Unix and *Linux* platforms, servers, mobile devices and an online scanner. The product submitted for testing includes a firewall, mail scanning and anti-spam, as well as some extras including registry monitoring, web scanning and a 'Care' module, all of which are disabled in a default installation but can be enabled at will. The setup process is thus rather lengthy, and requires a reboot at the end, but it is clearly laid out and looks very slick and professional.

The product itself is similarly impressive, with a clear and brightly coloured interface which was very easy to navigate. There was an unexpected lag during the setting up of manual scans, with the 'browse' button taking up to a minute to respond and present the filesystem for browsing, but otherwise things went smoothly, with decent scanning times and pretty good detection. This did not quite carry far enough however, as several of the highly complex variants of W32/Virut, which have been causing problems for a wide range of products for some months now, were not fully covered. This skews the results table somewhat, as the seemingly large number of misses in fact only represents a small number of unique viruses, so the percentage is a better indicator of performance than the raw number of missed files.

A smattering of false positives pushed a VB100 award further out of reach this time, but *ArcaBit* seems likely to reach the required standard in the very near future.

AVG Internet Security 8.0.131

ItW	100.00%	**Polymorphic**	89.95%
ItW (o/a)	100.00%	**Trojans**	98.47%
Worms & bots	99.94%	**File infectors**	99.21%
False positives	0		

Another suite, again reviewed in these pages fairly recently (see *VB*, March 2008, p.18), *AVG*'s *Internet Security* offers a splendidly fast and easy installation process, with everything up and running within a couple of minutes with no hard thinking or even a reboot required. Once the initial install is complete, however, a series of further setup phases are necessary, including options to install a *Yahoo!* toolbar and to set the browser to default to using *Yahoo!* for searches, a firewall configuration wizard, and several other steps.

With this stage complete things moved on very quickly, the product providing a clear and logical interface with no surprises. An oddity cropped up in the on-access side of testing, when the option to enable scanning of archives seemed to have little or no effect. Speeds were a little sluggish but detection rates excellent, with very little missed anywhere and no false positives either. With the WildList fully covered, *AVG* picks up another VB100 award.

Avira AntiVir 8.1.0.582

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.27%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

AntiVir presented a similarly straightforward and zippy installation process, again with no reboot and this time with no further requirements of the user. The familiar interface has its quirks but is easily navigated, with a few touches here and there either newly added or simply not noticed before, including some very funky slider controls.

A few times after running speed tests the 'Luke Filewalker' scanner screen seemed to linger rather longer than expected before closing down, but never for more than 10 seconds, and scanning speeds were extremely impressive. Detection rates were even closer to perfection, and without a hint of a false positive, and barely anything missed, *Avira* comfortably wins another VB100 award.

BitDefender AntiVirus 2008 11.0.16

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.75%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	4		

BitDefender's installation process takes a little time, with a blank setup window lingering on screen for 30 seconds or so before things get underway, followed by another lull as the *Windows Installer* prepares itself for action. The standard set of options follows, and once the installer proper is kicked off things move pretty speedily to completion. Prompts to enter a licence code and to reboot the system then appear simultaneously.

After the reboot the interface is simple and straightforward, but plenty of fine-tuning options are available in an advanced configuration area. Initial attempts to run on-demand scans proved a little troublesome, as requests returned strange messages claiming the scan could not be carried out, but a second restart of the system put a stop to these anomalies. From then on testing ran smoothly and quickly, with good scanning speeds and top-notch detection levels. WildList detection was flawless and the other sets not far off, but a small cluster of false positives put paid to *BitDefender*'s hopes of a VB100 award this month.

Bullguard 8.0.0.7

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	99.92%	**Trojans**	95.62%
Worms & bots	100.00%	**File infectors**	98.95%
False positives	4		

The *Bullguard* installation process was snappier, taking little more than a minute all told, with a reboot required at the end. This was followed by a registration process which asked for the user's email address and connected to base to report back – a six-day 'grace period' is allowed where this is not possible.

The interface is very simple and novice-friendly, offering basic controls for anti-virus, anti-spyware and a firewall. Little in-depth configuration was provided, but the defaults seemed sensible and more than adequate for my needs. Speeds and detection rates closely followed the example set by the parent *BitDefender* product, but a couple of misses of samples in the WildList set on access, along with those few false positives were enough to spoil things for *Bullguard* this time round.

On-demand detection	WildList		Worms and bots		File infectors		Polymorphic		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.91%	8	99.21%	317	77.32%	347	84.22%		
Ahnlab V3	2	99.99%	3	99.81%	8	97.64%	526	92.86%	345	84.34%		
Alwil avast!	0	100.00%	6	99.48%	6	96.06%	322	88.78%	51	97.66%		
ArcaBit ArcaVir	182	95.80%	3	99.78%	6	98.62%	55	94.16%	525	76.12%	10	2
AVG Internet Security	0	100.00%	1	99.94%	1	99.21%	52	89.95%	34	98.47%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	38	98.27%		
BitDefender AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	116	94.75%	4	
Bullguard	0	100.00%	0	100.00%	2	98.95%	0	100.00%	96	95.62%	4	
CA AntiVirus + AntiSpyware	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
CA eTrust	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
eEye Blink Professional	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	48	97.84%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	92	95.54%	1854	15.73%		
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	0	100.00%	90	95.65%	230	89.53%		
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	30	98.55%	117	94.66%		
F-Secure Protection Services	0	100.00%	0	100.00%	0	100.00%	30	98.55%	117	94.66%		
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.76%		
K7 Total Security	0	100.00%	5	99.61%	5	97.32%	883	68.95%	455	79.33%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	30	98.55%	72	96.73%		
Kingsoft Internet Security	0	100.00%	15	98.97%	87	81.89%	2009	42.15%	634	71.20%	1	
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	341	84.52%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	0	100.00%	90	95.65%	106	95.17%		
Norman Security Suite	0	100.00%	0	100.00%	7	99.15%	767	76.96%	128	94.18%		
NWI Virus Chaser	12	98.27%	0	100.00%	0	100.00%	90	95.65%	93	95.77%		2
PC Tools AntiVirus	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		
PC Tools Spyware Doctor	0	100.00%	2	99.91%	8	99.21%	313	77.70%	404	81.64%		
Proland Protector Plus	6	99.99%	5	99.48%	56	92.76%	1722	46.38%	1969	10.48%		
Quick Heal AntiVirus	0	100.00%	53	93.15%	10	98.03%	908	81.51%	1465	33.40%		
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	90	95.65%	102	95.38%		
Rising Antivirus	0	100.00%	2	99.81%	41	94.33%	1302	52.19%	268	87.82%		
Sophos Endpoint Security & Control	0	100.00%	0	100.00%	0	100.00%	90	95.65%	46	97.93%		33
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	90	95.65%	38	98.29%		
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	561	87.72%	40	98.20%		
VirusBuster Professional	0	100.00%	2	99.91%	8	99.21%	313	77.70%	362	83.56%		3
Webroot AntiVirus with AntiSpyware	0	100.00%	4	99.48%	0	100.00%	107	95.06%	48	97.81%		

CA AntiVirus + AntiSpyware 9.0.0.171

ItW	100.00%	**Polymorphic**	95.37%
ItW (o/a)	100.00%	**Trojans**	53.86%
Worms & bots	100.00%	**File infectors**	99.84%
False positives	1		

CA's home-user product is simple and speedy to set up, zipping through the standard options, EULAs and file copying in around a minute and a half; after this come options to install a *Yahoo!* toolbar and to set the browser to use *Yahoo!* for searching. Both of these options are checked by default and must be deselected if not required. After this, a reboot is needed.

Once again, to aid the less knowledgeable user and keep things simple, configuration is barely provided, but everything seemed to work pretty well. Scanning speeds were most impressive, and detection pretty solid, although a little weak in the new trojans set.

With the WildList covered without any problems, just a false positive in the clean set upset *CA*'s chances of an award for this product, and didn't bode well for the hopes of the company's corporate version.

CA eTrust 8.1.637.0

ItW	100.00%	**Polymorphic**	95.37%
ItW (o/a)	100.00%	**Trojans**	53.86%
Worms & bots	100.00%	**File infectors**	99.84%
False positives	1		

Setup of *eTrust* is a little more time-consuming, with EULAs in triplicate which must be scrolled through to the bitter end before they can be acknowledged, and a screen requesting a considerable amount of personal information to be filled in, again followed by a reboot.

The interface provided has always proved something of a bugbear during VB100 testing, but seemed a little faster and more responsive this time, perhaps thanks to the new, more powerful test hardware. There was still the occasional longueur as a screen prepared itself, and log viewing proved as awkward as ever. There was also an occasional problem with scans deactivating themselves while the interface presented a dialog box demanding credentials, although exactly what kind of credentials was not clear and simply cancelling out and reopening the interface got around this.

Once scanning was properly underway however, speeds were incredible as usual and detection rates again decent, with less thorough coverage of the trojans but no issues in the WildList. As expected, the same false positive put paid to *CA*'s chances of coming away with a VB100 award for either of the company's products.

eEye Digital Security Blink Professional 4.0.1

ItW	100.00%	**Polymorphic**	67.12%
ItW (o/a)	100.00%	**Trojans**	93.43%
Worms & bots	100.00%	**File infectors**	99.15%
False positives	0		

Initial installation of *eEye*'s *Blink* was simple and fast, but a few more steps had to be completed after the file copying, including licensing, a configuration wizard which could be cancelled to stick with the defaults, and offers to connect to the web to update and register the product. There followed a period of a minute or so while it settled in before the interface could be accessed.

The configuration is fairly in-depth, but lacks a 'block only' choice for the on-access scanner, meaning I had to let it destroy the test collection as it went through, but speeds were good enough for this not to matter much. Scanning of executables on demand was a little slower, thanks to the use of *Norman*'s sandbox technology to look for bad behaviours, but this attitude paid off with slightly better detection levels both for trojans and polymorphic viruses on demand, where the sandbox is used more deeply. There were no issues in the WildList in either mode, and no false positives either, meaning *eEye* can add another VB100 award to its growing collection.

ESET NOD32 Antivirus 3.0.667.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.84%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

ESET's installer, these days adorned with the rather groovy robot that has become the company's talisman, runs through a fairly standard set of options, with the whole thing running through from zero to protected in less than a minute and no reboot required.

With a splendid depth of options available in the advanced pages, more than plenty for the most demanding user, a few tweaks had everything just so and testing powered through in excellent time. A small issue appeared after scanning the full infected test sets in a single run on demand, in which the GUI appeared to hang and ceased to respond. Shutting it down with the task manager and restarting it soon put a stop to this however, and on-access scanning continued throughout this hiccup without issues. Detection rates were near perfect, and false positives absent, thus another VB100 award is added to *ESET*'s record tally.

Fortinet FortiClient 3.0.475

ItW	100.00%	**Polymorphic**	95.54%
ItW (o/a)	100.00%	**Trojans**	15.73%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The setup of *FortiClient* took a little longer, with a few more options needing to be set and a few lingering periods of waiting for activities to complete, but again no reboot was needed to activate the protection. The interface presented a familiar look, but seemed to be lacking the usual wealth of modules, perhaps indicating a pared-down version which would explain the less complex than usual setup process. Configuration is provided in great depth, but the defaults were pretty much just as I needed them and little

needed adjusting. Scanning speeds were very good, and detection rates generally superb, although performance in the trojans set was pretty disappointing. However, in the core WildList set there were no issues, and without false positives either *Fortinet* also notches up another VB100 award.

Frisk F-PROT Antivirus 6.0.9.1

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	89.53%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Frisk's desktop product provided one of the fastest setup processes of all, being completed in little more than 30 seconds, but did require a reboot, prior to which I judiciously dropped in the updates provided.

The product itself is one of the most basic, with barely any options available even for on-demand scans, which merrily deleted or cleaned files as it tripped through the test sets. This seemed to have little impact on scanning speeds however, which were pretty impressive, and detection rates were also solid, although one of the new batch of polymorphic viruses was not fully covered. With no false positives and no issues in the WildList, *Frisk* comfortably qualifies for a VB100 award.

F-Secure Internet Security 2009 9.00.146

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	94.66%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

F-Secure joins the growing group of vendors submitting multiple products, its *Internet Security Suite* being first up. The installation took a little time, including an automatic and unstoppable update attempt, and was followed by a reboot to complete the setup. Once up and running, the design was pretty familiar, little changed from the company's previous offerings, on the surface at least.

This meant a splendid array of tools and plenty of options available under the hood, providing excellent protection if not the best scanning speeds. Logging remains an issue, with records of completed scans rarely displayed in their entirety – HTML pages varied wildly in length but always missed off large amounts of detail, rendering data gathering somewhat difficult. Resorting to deleting files and seeing what was left behind showed the expected excellent coverage, with no problems in the WildList or clean sets and precious little missed elsewhere; a VB100 award is duly granted.

F-Secure Protection Services for Consumers

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	94.66%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

F-Secure's second offering is a customizable version of the company's suite designed for redistribution by ISPs wanting to provide branded protection to their customers. The setup and interface closely match the standard suite, with the basic components of anti-malware, web shield, spam filter and parental controls all available.

Speeds and detection rates also closely mirror the sister product, and the nasty logging was also in evidence. Quickly bypassing this showed the same results, granting *F-Secure* a second VB100 award this month.

G DATA AntiVirus 18.9.1.9

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.76%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The rather large installer file for *G DATA*'s product ran through its business pretty quickly and simply, requiring a system reboot to complete. Once up and running, a few changes were noted in the interface. These were most apparent in some changed wording in many of the options, and represented a number of small improvements to a thoroughly well-designed and usable tool.

G DATA also goes for a multi-engine approach, hence the large installer and slightly slower scanning speeds, but this is more than made up for by the superb thoroughness and excellent detection. Very little was missed, even in the new test set of trojans, particularly in the more thorough on-demand scans, and with no false positive issues and nothing missed in the WildList set, *G DATA* storms its way to another VB100 award.

On-demand throughput (MB/s)	Archive files - default		Archive files - all files		Binaries & system files - default		Binaries & system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - all files	
	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)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
Agnitum Outpost	942	3.21	942	3.21	357	10.23	357	10.23	102	17.56	102	17.56	85	10.88	85	10.88
Ahnlab V3	476	6.35	476	6.35	682	5.36	682	5.36	94	19.06	94	19.06	59	15.68	59	15.68
Alwil avast!	32	94.52	628	4.82	218	16.76	259	14.11	36	49.77	79	22.68	28	33.04	56	16.52
ArcaBit ArcaVir	351	8.62	351	8.62	315	11.60	315	11.60	38	47.15	38	47.15	66	14.02	66	14.02
AVG Internet Security	1497	2.02	1784	1.70	375	9.74	380	9.61	478	3.75	486	3.69	42	22.03	143	6.47
Avira AntiVir	329	9.19	367	8.24	112	32.62	114	32.05	41	43.70	51	35.13	33	28.04	45	20.56
BitDefender AntiVirus	335	9.03	1203	2.51	520	7.03	556	6.57	67	26.74	73	24.54	85	10.88	89	10.40
Bullguard	1193	2.54	1193	2.54	578	6.32	578	6.32	74	24.21	74	24.21	93	9.95	93	9.95
CA AntiVirus + AntiSpyware	404	7.49	404	7.49	94	38.87	94	38.87	42	42.66	42	42.66	35	26.43	35	26.43
CA eTrust	207	14.61	207	14.61	82	44.56	82	44.56	23	77.90	23	77.90	28	33.04	28	33.04
eEye Blink Professional	511	5.92	511	5.92	1749	2.09	1749	2.09	55	32.58	55	32.58	149	6.21	149	6.21
ESET NOD32 Antivirus	841	3.60	841	3.60	553	6.61	553	6.61	39	45.94	39	45.94	48	19.27	48	19.27
Fortinet FortiClient	271	11.16	271	11.16	499	7.32	499	7.32	36	49.77	36	49.77	51	18.14	51	18.14
Frisk F-PROT Antivirus	259	11.68	259	11.68	432	8.46	432	8.46	39	45.94	39	45.94	36	25.70	36	25.70
F-Secure Internet Security	1303	2.32	1620	1.87	306	11.94	313	11.67	43	41.67	99	18.10	30	30.84	91	10.17
F-Secure Protection Services	1322	2.29	1681	1.80	310	11.79	313	11.67	43	41.67	97	18.47	30	30.84	108	8.57
G DATA AntiVirus	1415	2.14	1415	2.14	424	8.62	424	8.62	122	14.69	122	14.69	90	10.28	90	10.28
K7 Total Security	196	15.43	N/A	N/A	247	14.79	247	14.79	35	51.19	35	51.19	38	24.35	38	24.35
Kaspersky Anti-Virus	582	5.20	582	5.20	164	22.28	164	22.28	47	38.12	47	38.12	34	27.21	34	27.21
Kingsoft Internet Security	168	18.00	N/A	N/A	1541	2.37	1541	2.37	548	3.27	548	3.27	1019	0.91	1019	0.91
McAfee VirusScan	50	60.49	778	3.89	753	4.85	746	4.90	76	23.57	73	24.54	101	9.16	99	9.35
MWTI eScan Internet Security	1376	2.20	1376	2.20	885	4.13	885	4.13	858	2.09	858	2.09	883	1.05	883	1.05
Norman Security Suite	532	5.69	532	5.69	1753	2.08	1753	2.08	56	31.99	56	31.99	139	6.66	139	6.66
NWI Virus Chaser	1332	2.27	1332	2.27	665	5.49	665	5.49	132	13.57	132	13.57	136	6.80	136	6.80
PC Tools AntiVirus	458	6.60	N/A	N/A	276	13.24	276	13.24	67	26.74	67	26.74	73	12.67	73	12.67
PC Tools Spyware Doctor	976	3.10	976	3.10	611	5.98	611	5.98	82	21.85	82	21.85	91	10.17	91	10.17
Proland Protector Plus	250	12.10	N/A	N/A	133	27.47	133	27.47	63	28.44	63	28.44	88	10.51	88	10.51
Quick Heal AntiVirus	153	19.77	342	8.84	65	56.21	65	56.21	50	35.83	53	33.80	37	25.01	45	20.56
Redstone Redprotect	1221	2.48	1221	2.48	427	8.56	427	8.56	302	5.93	302	5.93	313	2.96	313	2.96
Rising Antivirus	926	3.27	926	3.27	555	6.58	555	6.58	80	22.40	80	22.40	91	10.17	91	10.17
Sophos Endpoint Security & Control	47	64.35	831	3.64	305	11.98	323	11.31	47	38.12	68	26.35	35	26.43	87	10.63
Symantec Endpoint Protection	390	7.76	402	7.52	256	14.27	269	13.58	77	23.27	75	23.89	77	12.02	75	12.34
Trustport Antivirus	504	6.00	504	6.00	488	7.49	488	7.49	113	15.86	113	15.86	295	3.14	295	3.14
VirusBuster Professional	20	151.23	977	3.10	299	12.22	321	11.38	58	30.89	90	19.91	26	35.58	65	14.23
Webroot AntiVirus with AntiSpyware	834	3.63	834	3.63	1859	1.97	1859	1.97	91	19.69	91	19.69	63	14.69	63	14.69

K7 Total Security 9.5.0469

ItW	100.00%	**Polymorphic**	68.95%
ItW (o/a)	100.00%	**Trojans**	79.33%
Worms & bots	99.61%	**File infectors**	97.32%
False positives	0		

Unlike most AV installers, which simply warn users of potential problems if installing over existing protection software, *K7*'s installer includes a check for possible conflicting products, along with the usual steps. Nevertheless this is all done with remarkable speed. A reboot is required, which is followed by a friendly welcome splash screen.

The suite includes a firewall and anti-spam module as well as the anti-malware component. The interface is pleasantly laid out with a reasonable level of configuration available, and runs stably with impressive speeds. Detection rates were also impressive, with only some of the more obscure items in the polymorphic set causing any problems and the new trojan set was covered pretty well. The WildList was also well handled and without false positives *K7* nobly achieves a second VB100 award.

Kaspersky Anti-Virus 2009 8.0.0.337

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	96.73%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Kaspersky's latest version ups the ante a little, with a further sheen of glitz and slickness added to its already exemplary design and a selection of extra goodies dropped in. The installation is unexceptionable, taking a few minutes to run through a standard range of setup options and do the actual business, which is followed by a reboot.

With the expected excellent depth of configuration available this proved unproblematic, speeds were pretty good even using more thorough settings, and detection rates very strong. With the WildList covered effortlessly and the only alert raised on the clean sets being a warning that a few files in the archive were password protected and thus could not be guaranteed to be clean, *Kaspersky* ably earns another VB100 award.

Kingsoft Internet Security 2008.2.22.11

ItW	100.00%	**Polymorphic**	42.15%
ItW (o/a)	100.00%	**Trojans**	71.20%
Worms & bots	98.97%	**File infectors**	81.89%
False positives	1		

Kingsoft's products have had an uneven ride in recent months, with some successes and some problems. This occasion proved much the same. The installation process was pretty straightforward, and no reboot was required despite the product including a firewall. This was fortunate as several installations were needed.

The first few runs showed remarkably low detection rates, with large numbers of items missed despite having been picked up by the product on previous occasions. Although consistent in themselves, some kind of problem was suspected when compared with the product's earlier performances. A second attempt produced the same results, but on a third install, with the on-access test slowed down considerably, things picked up remarkably and the WildList was covered completely, with detection considerably less thorough elsewhere. The difficult question of whether this patchy performance merited a VB100 award was thankfully skirted, when a single file in one of the clean sets was mislabelled as malware, denying *Kingsoft* the award this time.

McAfee VirusScan Enterprise 8.5.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	84.52%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

McAfee's corporate product is one of few to have remained virtually unchanged in the two years since I took on the *VB* testing role, and I am thankful for it. The simple, unflashy setup is always clear, stable and thorough. The setup process proved as straightforward and worry-free as ever, and was completed in excellent time with no reboot required. The interface itself has a serious, business-like air about it, and provides all the fine-tuning options one would expect from an enterprise-class product.

Scanning speeds were very good and detection at its usual excellent level, with coverage of the new trojan set a little less complete than I might have expected but still more than decent. With no issues in the WildList or the clean sets, *McAfee* also takes away a VB100 award.

MWTI eScan Internet Security

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	95.17%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The anti-malware component of *MicroWorld*'s *eScan* is based on the *Kaspersky* engine, but with numerous additions of *MicroWorld*'s own the setup process takes its time running through multiple stages of configuration and installation. After several minutes it was all ready to go however, without the need for a reboot.

The interface has a blocky, somewhat retro look and proved a little slow to respond on occasion. Configuration seemed pretty thorough, but on one occasion the product reverted to deleting infected files despite being asked not to. This minor quibble aside, detection was as excellent as I expected, speeds a little on the slow side, but without false positives or WildList issues another VB100 award is easily earned.

Norman Security Suite 7.00

ItW	100.00%	**Polymorphic**	76.96%
ItW (o/a)	100.00%	**Trojans**	94.18%
Worms & bots	100.00%	**File infectors**	99.15%
False positives	0		

I had been looking forward to getting my hands on *Norman*'s new suite product, having had a few minor issues with the design of the company's previous product. Setup was pretty simple and speedy, including the offer of a 'Screensaver Scanner' which would run a scan automatically when the machine was not in use (more on which later). It also suggested that a reboot might be required, but this proved not to be the case.

My first look at the new interface was both pleasing and confusing. It took some time to show itself, but once up and running looked slick and cool and a little minimalist. In some cases this proved to be because elements took some time to render, or occasionally even failed to materialize at all. Configuration options were either less in-depth than I had hoped or simply so elusive that I didn't manage to find them. Occasionally buttons proved unresponsive and the whole interface froze or shut itself down from time to time.

The problems with the interface proved to have little effect on the level of protection provided, which proved stable and

File access lag time (s/MB)	Archive files - default		Archive files - all files		Binaries & system files - default		Binaries & system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - all files	
	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)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
Agnitum Outpost	60	0.02	N/A	N/A	470	0.13	N/A	N/A	190	0.10	N/A	N/A	178	0.17	N/A	N/A
Ahnlab V3	82	0.03	N/A	N/A	446	0.12	N/A	N/A	62	0.02	N/A	N/A	74	0.06	N/A	N/A
Alwil avast!	246	0.08	821	0.27	331	0.09	347	0.09	155	0.08	174	0.09	63	0.05	92	0.08
ArcaBit ArcaVir	78	0.03	N/A	N/A	327	0.09	N/A	N/A	32	0.01	N/A	N/A	24	0.01	N/A	N/A
AVG Internet Security	145	0.05	N/A	N/A	512	0.14	513	0.14	126	0.06	139	0.07	33	0.02	103	0.09
Avira AntiVir	34	0.01	305	0.10	127	0.03	124	0.03	48	0.02	61	0.02	30	0.01	57	0.04
BitDefender AntiVirus	312	0.10	861	0.28	527	0.14	559	0.15	85	0.04	94	0.04	105	0.10	109	0.10
Bullguard	350	0.12	350	0.12	580	0.16	N/A	N/A	36	0.01	N/A	N/A	19	0.00	N/A	N/A
CA AntiVirus + AntiSpyware	29	0.01	N/A	N/A	106	0.03	106	0.03	51	0.02	51	0.02	44	0.03	44	0.03
CA eTrust	24	0.01	N/A	N/A	96	0.02	96	0.02	50	0.02	50	0.02	43	0.03	43	0.03
eEye Blink Professional	60	0.02	N/A	N/A	295	0.08	295	0.08	68	0.03	68	0.03	117	0.11	117	0.11
ESET NOD32 Antivirus	11	0.00	N/A	N/A	65	0.01	65	0.01	48	0.02	48	0.02	43	0.03	43	0.03
Fortinet FortiClient	223	0.07	223	0.07	416	0.11	416	0.11	39	0.01	39	0.01	66	0.05	66	0.05
Frisk F-PROT Antivirus	71	0.02	N/A	N/A	465	0.12	465	0.12	48	0.02	48	0.02	42	0.03	42	0.03
F-Secure Internet Security	35	0.01	1461	0.48	276	0.07	465	0.12	63	0.03	177	0.09	41	0.03	150	0.14
F-Secure Protection Services	35	0.01	1474	0.49	266	0.07	771	0.21	61	0.02	181	0.09	39	0.02	153	0.15
G DATA AntiVirus	226	0.07	1256	0.41	408	0.11	510	0.14	135	0.07	227	0.12	124	0.12	153	0.15
K7 Total Security	52	0.02	N/A	N/A	250	0.07	350	0.09	49	0.02	49	0.02	50	0.04	50	0.04
Kaspersky Anti-Virus	23	0.01	76	0.02	152	0.04	154	0.04	75	0.03	87	0.04	52	0.04	69	0.06
Kingsoft Internet Security	82	0.03	N/A	N/A	1549	0.42	1549	0.42	553	0.30	553	0.30	1046	1.11	1046	1.11
McAfee VirusScan	40	0.01	254	0.08	367	0.10	355	0.09	67	0.03	63	0.03	84	0.07	84	0.07
MWTI eScan Internet Security	996	0.33	996	0.33	275	0.07	275	0.07	91	0.04	91	0.04	94	0.08	94	0.08
Norman Security Suite	47	0.01	N/A	N/A	313	0.08	313	0.08	70	0.03	70	0.03	112	0.10	112	0.10
NWI Virus Chaser	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PC Tools AntiVirus	45	0.01	N/A	N/A	25	0.00	25	0.00	219	0.11	219	0.11	149	0.14	149	0.14
PC Tools Spyware Doctor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Proland Protector Plus	18	0.01	N/A	N/A	126	0.03	N/A	N/A	38	0.01	N/A	N/A	21	0.00	N/A	N/A
Quick Heal AntiVirus	14	0.00	N/A	N/A	67	0.01	N/A	N/A	46	0.02	N/A	N/A	24	0.01	N/A	N/A
Redstone Redprotect	37	0.01	N/A	N/A	266	0.07	266	0.07	147	0.07	147	0.07	144	0.14	144	0.14
Rising Antivirus	66	0.02	511	0.17	278	0.07	578	0.15	93	0.04	91	0.04	105	0.10	101	0.09
Sophos Endpoint Security & Control	36	0.01	785	0.26	307	0.08	322	0.08	48	0.02	62	0.02	46	0.03	77	0.06
Symantec Endpoint Protection	27	0.01	N/A	N/A	199	0.05	199	0.05	55	0.02	55	0.02	49	0.03	49	0.03
Trustport Antivirus	501	0.17	501	0.17	512	0.14	512	0.14	125	0.06	125	0.06	186	0.18	186	0.18
VirusBuster Professional	33	0.01	N/A	N/A	279	0.07	286	0.07	42	0.01	65	0.03	28	0.01	59	0.05
Webroot AntiVirus with AntiSpyware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

reliable. On-demand scanning was a little awkward, particularly in the speed tests as, looking away to another test system as it ran, I returned to find the screensaver had activated, thus stopping my requested scan and starting the default full system probe. With this deactivated, things moved on nicely, with good speeds and decent detection, including full WildList coverage and no false positive issues. *Norman*'s protection, if not its GUI, earns the company a VB100 award.

NWI Virus Chaser 5.0b

ItW	98.27%	**Polymorphic**	95.65%
ItW (o/a)	98.27%	**Trojans**	95.77%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

NWI has been absent from the test for some time, but a return to the test bench offered a chance to see how the company's product has progressed. An initial surprise was the use of an 'InstallShiend Wizard' (*sic*) to operate the installation, but this proved remarkably fast if not well proof-read, getting protection fully operational in under 20 seconds, with judicious clicking of 'next'.

The main interface remains much as I remembered it from earlier tests, its most notable quirk being a prominent set of options to configure the colour and decoration of the interface. Other configuration proved limited, and on-access scanning was not activated on simple file access, meaning the tests had to be carried out by copying files to the system. This skirted the on-access speed test, but on-demand speeds were decent and system slowdown was not noticeable. On occasion the interface froze or shut down, apparently due to unusually large logs, a situation unlikely to occur in the real world, but overall detection proved pretty impressive. A few items in the clean sets were alerted on as possible dangers in the wrong hands, but false positives were absent. The trojan set was not the product's strongest point, and in the WildList set a few of the most recent items were also missed, keeping the VB100 award just out of *NWI*'s grasp.

PC Tools AntiVirus 2008 5.0.0.14

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	82.69%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Archive scanning		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
Agnitum Outpost	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Ahnlab V3	OD	X	9	X	9	9	X	9	X	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast!	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
ArcaBit ArcaVir	OD	2	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	√	√
AVG Internet Security	OD	X	√	X	X	√	X	√	√	X
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
BitDefender AntiVirus	OD	X/√	X/√	√	X/√	X/√	X/8	1/√	X/8	√
	OA	X/√	X/√	√	X/√	X/√	X/8	1/√	X/8	√
Bullguard	OD	√	√	√	√	√	8	√	8	√
	OA	X	√	X	X	√	X	√	8	X
CA AntiVirus + AntiSpyware	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	X	√
CA eTrust	OD	X	√	√	√	√	√	√	X	√
	OA	X	X	1	X	X	X	1	X	√
eEye Blink Professional	OD	X	X	1	1	X	8	2	X	√
	OA	X	X	X	X	X	X	X	X	√
ESET NOD32 Antivirus	OD	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	4	√	√
	OA	X	√	√	√	√	√	4	√	√
Frisk F-PROT Antivirus	OD	1	√	√	√	√	√	√	√	√
	OA	1	X	2	X	X	X	2	2	√
F-Secure Internet Security	OD	X/√	5	5	5	5	2	5	5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
F-Secure Protection Services	OD	X/√	5	5	5	5	2	5	5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
G DATA AntiVirus	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	8/√	8/√	4/√	√
K7 Total Security	OD	X	1	1	1	1	X	1	X	√
	OA	X	X	X	X	X	X	X	X	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/4	X/4	X/4	X/4	X/5	X	X	X	√
Kingsoft Internet Security	OD	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
MWTI eScan Internet Security	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Security Suite	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
NWI Virus Chaser	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	4	√	9	X
PC Tools AntiVirus	OD	X	X	X	X	X	X	X	X	√
	OA	2	2	2	X	2	1	2	2	√
PC Tools Spyware Doctor	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Proland Protector Plus	OD	X	√	√	X	X	X	√	X	√
	OA	X	X	X/2	X	X	X	X/2	X	X/√
Quick Heal AntiVirus	OD	X/2	X/5	2/5	X	X/5	X/1	2/5	X	√
	OA	X	X	X	X	X	X	X	X	X
Redstone Redprotect	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Rising Antivirus	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X/√
Sophos Endpoint Security & Control	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	OD	X	3/√	3/√	3/√	3/√	1/5	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	√
Trustport Antivirus	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	√	X	√	√	√	√	√
VirusBuster Professional	OD	2	√	X/√	X	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot AntiVirus with AntiSpyware	OD	X	√	X	√	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	√

Key:

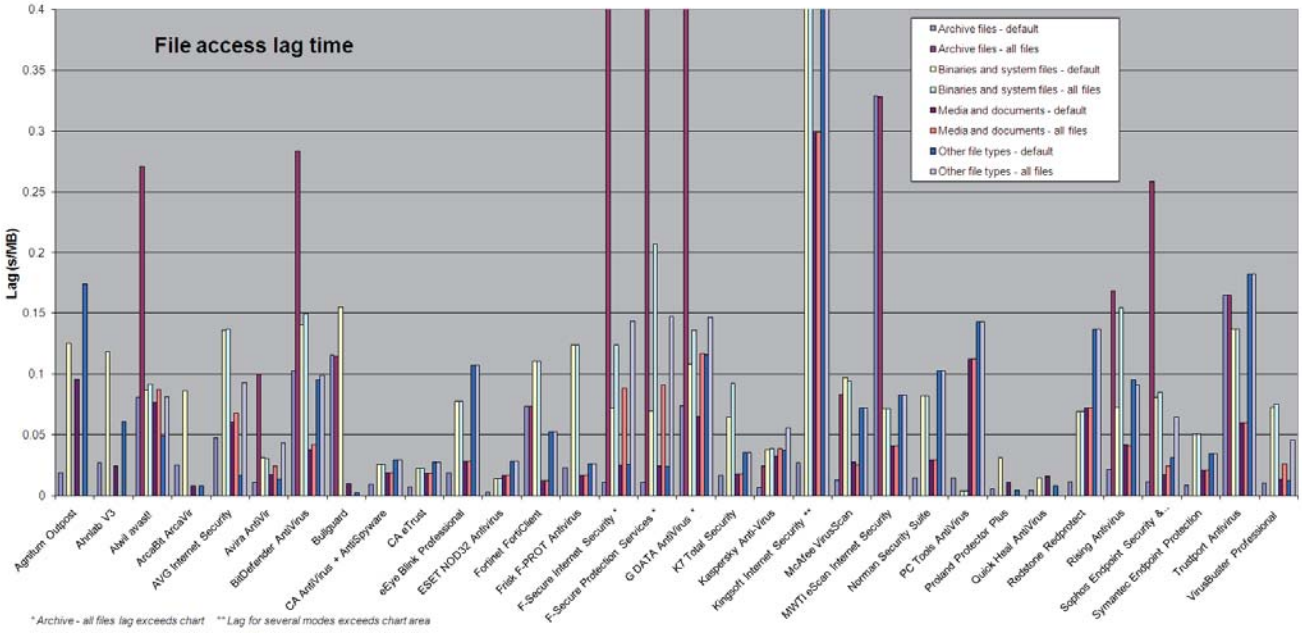
X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

[1-9] - Archives scanned to limited depth

X/√ - Default settings/thorough settings

*Executable file with randomly chosen extension



PC Tools products have produced many oddities in the past, and I approached them this month with my usual trepidation. The plain anti-virus product usually presents the fewest issues, and this time was no exception. Installing was fairly straightforward, with the product offering to install *Google* toolbars for me, and navigating the colourful, novice-friendly interface proved no problem. However, there were frequent lags moving from one page to another and configuration was minimal at best.

Scanning was completed fairly quickly, although the on-access behaviour seemed rather strange. Files were clearly being checked on simple opening, and scan times for most sets were rather slow, but executables seemed to be ignored entirely, hence the unusually fast time for this set.

Testing was thus performed by copying files to the systems and running scans with disinfection enabled, analysing remaining files for changes. As expected, final results showed fairly solid detection rates. False positives were absent, and the WildList covered in full, and thus *PC Tools AntiVirus* receives a VB100 award.

PC Tools Spyware Doctor 6.0.0.354f

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	81.64%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Spyware Doctor is pretty similar to its sister product, but a little more tricky to configure and with even longer and more regular freezes, lags in accessing screens and other annoyances. Scanning behaviour seemed even more erratic, but generally items being copied to the system or scanned seemed eventually to be removed or disinfected, although this often took some time and seemed likely to leave the system at risk for a spell. With logging proving too vague and unreliable to give an accurate indication of what was happening, checking remaining files for changes was resorted to once again.

Once gathered, results proved to be along the same lines as for the plain anti-virus product, and thus *Spyware Doctor* also earns a VB100 award for its developers.

Proland Protector Plus 2008 8.0.C03

ItW	99.99%	**Polymorphic**	46.38%
ItW (o/a)	99.53%	**Trojans**	10.48%
Worms & bots	99.48%	**File infectors**	92.76%
False positives	0		

Proland is an occasional entrant in VB100 testing, known for its very compact, lightweight product. The 10 MB installer powered through its business in eyebrow-raising time, and no reboot was required to get things going.

A nice, clear, simple interface provided easy access to the required controls, although in-depth configuration was

minimal, and the speed tests zipped through at superb speed. False positives were absent, but detection was less than splendid, particularly in the trojan set and with polymorphic items in on-access mode. These polymorphic problems extended into the WildList set, where a few W32/Virut samples were missed in on-demand mode too, thus denying *Proland* a VB100 award for the time being.

Quick Heal AntiVirus Lite 9.50

ItW	100.00%	**Polymorphic**	81.51%
ItW (o/a)	100.00%	**Trojans**	33.40%
Worms & bots	93.15%	**File infectors**	98.03%
False positives	0		

Similarly small and lightweight, *Quick Heal*'s installation is also exceptionally speedy and completed in little over 30 seconds, without the need for a reboot.

The interface, glitzed up a little from previous versions, proved a little sluggish to respond on occasions, but scanning speeds and overheads were as excellent as ever. Detection across all test sets was reasonable, with false positives absent in the clean set after several such issues in recent tests. The WildList was handled without problems, and *Quick Heal* regains its VB100 certified status.

Redstone Redprotect 1.6.1.0

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	95.38%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Redstone's product implements the strong protection of the *Kaspersky* engine, with the .NET framework required for the front end. This added somewhat to the installation time, which was pretty fast once the framework was in place and requested no reboot. However, the product seemed not to have been started at the end of the process, so the system was restarted manually to ensure everything was in place.

Designed to be managed remotely, *Redprotect* has little by way of user configuration, simply a set of options accessible via the system tray icon to run manual scans and updates. A simple configuration tool is made available for testing purposes, basically adjusting registry entries which would otherwise be controlled by the remote manager. This proved just about enough for my needs, although the options to activate archive scanning in the on-access mode seemed not to function. Speeds in both modes were not super fast, and one of the on-demand scans of a subset of the clean collection repeatedly crashed out, but things were completed eventually and the somewhat awkward multiple logs gathered, linked up and parsed.

The results showed the excellent detection expected of the engine, an absence of false positives and flawless coverage of the WildList, earning *Redstone* a VB100 award.

Rising Antivirus 20.47.22

ItW	100.00%	**Polymorphic**	52.19%
ItW (o/a)	100.00%	**Trojans**	87.82%
Worms & bots	99.81%	**File infectors**	94.33%
False positives	0		

Rising's product had one of the most complex installation processes, running speedily but with a multitude of questions and options put before the user. Once done with, and after the required reboot, the interface is smooth and efficient-looking but on occasion slow to respond, as is the system as a whole, perhaps thanks to the cartoon lion placed on the desktop, constantly performing acrobatics, striking poses and so on, seemingly unrelated to the activities of the product.

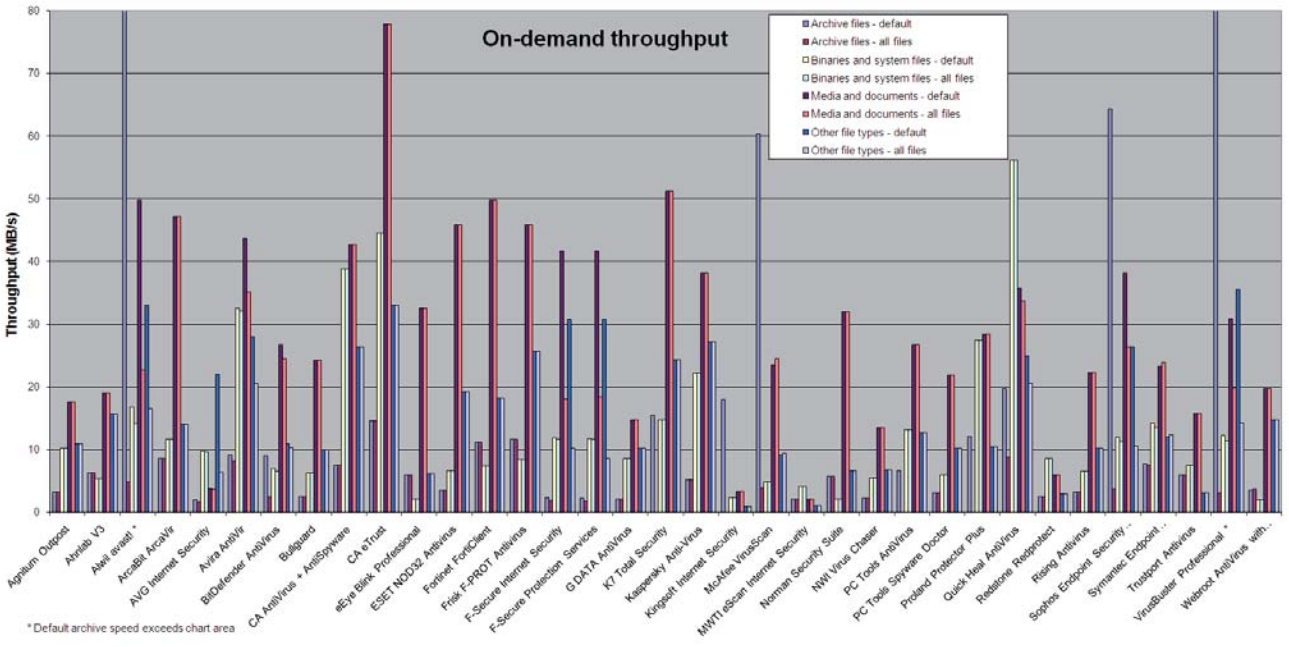
Despite this scanning speeds were reasonable, as was detection across the sets, and false positives were absent. Some initial worries that some samples of W32/Looked (aka Viking) were being missed on access proved to be a one-off, with everything on the WildList detected flawlessly on a second attempt, and *Rising* becomes the proud winner of its first VB100 award.

Sophos Endpoint Security & Control 8

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	97.93%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Sophos's latest product-naming scheme seems to reflect a marketing move rather than the product under test here, which remains much as normal. The installation is straightforward and includes the offer of a firewall, and also the removal of any 'third-party software'. It all ran through in under a minute and needed no reboot.

As an enterprise-focused product *Sophos* provides the most in-depth configuration anyone could ask for, all of which is



easily accessible. Speeds were good and detection excellent; a VB100 award is earned with ease.

Symantec Endpoint Protection 11.0.2000.1567

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	98.29%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Like *Sophos*, *Symantec* also included the dreaded 'endpoint' euphemism in its product title, but its business-grade product is a little more bright, shiny and, well, less business-like. The installation took a few minutes, including the offer of some readmes and guides in PDF format. In the colourful interface, configuration is not hugely complex, much of this presumably being left to an admin with a management tool. One thing proved vital for my testing needs though: the option to up the priority of scanning, as an initial attempt at scanning the infected sets would have taken, by my estimation, around 13 days to complete (the fastest time for another product was seven minutes). This sluggishness can presumably be explained by various bits of logging and side-scanning being carried out when a detection is spotted, as scanning of the clean sets was pretty fast. Detection rates were splendid, false positives absent, and *Symantec* thus earns another VB100 award.

Trustport Antivirus 2.8.0.3003

ItW	100.00%	**Polymorphic**	87.72%
ItW (o/a)	100.00%	**Trojans**	98.20%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The *Trustport* installer runs very quickly, the process completed in under a minute, with no unexpected options to break the chain of 'next's and no reboot required.

The layout of the product is a little odd, having no true main interface but instead several configuration pages and scanning tools accessible from the system tray icon. This system proved perfectly usable however, and provided ample controls for the product. The number of engines used by the product has varied considerably of late, but was down to a mere two this time, clearly a wise decision as scanning times were not as slow as they have been in the past while detection rates remained excellent. With not much missed and no false positives, *Trustport* also earns a VB100 award.

VirusBuster Professional 5.3.121

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	83.56%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

VirusBuster is a challenger for the fastest installation process, with its simple system which starts with a simple *WinZip* dialog and completes, after a standard set of choices, around 30 seconds later with no reboot required.

The interface is much as it has been for some time, a tried and trusted thing which, while occasionally a little awkward to navigate, provides plenty of configuration in stable and reliable style. The protection offered is similarly solid, with more than decent detection rates and very decent speeds. No issues in the WildList or clean sets means that *VirusBuster* earns a VB100 award.

Webroot AntiVirus with AntiSpyware 5.5.7.124

ItW	100.00%	**Polymorphic**	95.06%
ItW (o/a)	100.00%	**Trojans**	97.81%
Worms & bots	99.48%	**File infectors**	100.00%
False positives	0		

This product starts out as the traditional *SpySweeper* anti-spyware tool, before a few judicious additions – including the *Sophos* anti-virus engine – convert it, name and all, into a full anti-malware product. The install process is fairly straightforward and fast, complicated by the lack of web connection and need to manually doctor some sections, but things are soon up and running after a reboot.

The interface provides rather confusing access to a very limited configuration setup, and seemed even more sluggish in its response times than usual, especially when running on-demand scans. On-access detection is only sparked by copying files to the system, and seems to allow writing and then to remove the file when it gets round to it, in some cases quite some time later. Actually executing files seems to be blocked a little more promptly, but it still left me rather nervous.

This system meant on-access speeds could not be measured, but the machine seemed to be rather slow, and under heavy load the interface froze regularly – on occasion the whole system, but in most cases recovered without intervention, patience allowing. Logging was a little odd, in many cases failing to record any data on files removed or cleaned, so detection rates had to be measured by comparing checksums of remaining files. After this arduous process the expected solid detection was shown, including full WildList coverage and no false positives, and a VB100 award is duly granted.

CONCLUSIONS

This was another bumper test, with its usual crop of issues. Passes were plentiful, with a few false positive issues and a few products having problems with WildList samples. In particular the W32/Virut strains continue to fox products after several months on the WildList, during which time they have been consistent high-flyers in *VB*'s prevalence charts. The new trojan set proved informative, although as expected most AV labs managed to keep pretty much on top of *VB*'s sample-gathering and validation process. We anticipate removing most of the files used here from future test sets, using a rolling system to keep the set as up to date as possible, so hopefully some patterns of strength and weakness should begin to emerge over time.

The biggest issues this time around were with interface design and stability. A remarkable number of professionally made and presumably professionally tested products presented problems with their interfaces freezing, crashing, or being unbearably slow to respond, and in some cases this instability ran over to the protection offered and even brought down the entire test system. Whether any of these issues are influenced by the addition of the recent service pack remains to be investigated in post-test analysis. Software stability is pretty vital, particularly in security software, and a shaky interface will swiftly lose the trust of users even if the protection behind the scenes remains up and running. It never fails to astound me that products should reach external testers, and presumably also users, with such serious issues as have been seen in some this month.

This test marks something of the end of an era. For many years the VB100 has been a solo effort, carried out entirely by a single tester beavering away on his own in an empty test lab. In time for the next test (barring unforeseen problems), there will be two pairs of hands on the keyboards and two pairs of eyes on the screens. For me, this should mean the end of the long hours and late nights required, while for our readers it will mean more value and information from our tests, thanks to there being more time to devote to expansion, devising and implementing new tests and keeping sample sets broader and more up to date. For competing vendors, of course, this will mean stiffer challenges and tougher criticisms of failure, but then, not everyone can be a winner.

Technical details:

All products were tested on identical systems with *AMD Athlon64* X2 Dual Core 5200+ processors, 2 GB RAM, dual 80 GB and 400 GB hard drives, running *Microsoft Windows XP Professional* (32-bit) with Service Pack 3.

END NOTES & NEWS

Black Hat USA 2008 takes place 2–7 August 2008 in Las Vegas, NV, USA. See http://www.blackhat.com/.

COSAC 2008, the 15th International Computer Security Forum, will take place 21–25 September 2008 in Naas, Republic of Ireland. For details see http://www.cosac.net/.

VB2008 will take place 1–3 October 2008 in Ottawa, Canada. Presentations will cover subjects including: sample sharing, anti-malware testing, automated analysis, rootkits, spam and botnet tracking techniques, corporate policy, business risk and more. Register online at http://www.virusbtn.com/conference/vb2008.

SecTor 2008 takes place 7–8 October 2008 in Toronto, Canada. The conference is an annual IT security education event created by the founders of North American IT security usergroup TASK. For more information see http://sector.ca/.

The 3rd International Conference on Malicious and Unwanted Software (Malware '08) will be held 7–8 October 2008 in Alexandria, VA, USA. The main focus for the conference will be 'the scalability problem'. For more details see http://isiom.wssrl.org/.

Black Hat Japan 2008 takes place 7–10 October 2008 in Tokyo, Japan. Training will take place 7–8 October, with the Black Hat Briefings taking place 9–10 October. For full details see http://www.blackhat.com/.

Net Focus UK 2008 takes place 8–9 October 2008 in Brighton, UK. The event deals with issues of security, personnel, compliance, data privacy, business risk, e-commerce risk and more. For details see https://www.baptie.com/events/show.asp?e=160&xyzzy=2.

The third APWG eCrime Researchers Summit will be held 15–16 October 2008 in Atlanta, GA, USA. eCrime '08 will bring together academic researchers, security practitioners and law enforcement representatives to discuss all aspects of electronic crime and ways to combat it. See http://www.antiphishing.org/ecrimeresearch/.

The SecureLondon Workshop on Computer Forensics will be held 21 October 2008 in London, UK. For further information see https://www.isc2.org/cgi-bin/events/information.cgi?event=58.

RSA Europe 2008 will take place 27–29 October 2008 in London, UK. This year the conference celebrates the influence of Alan Mathison Turing, British cryptographer, mathematician, logician, biologist and 'the father of modern computer science'. For full details see http://www.rsaconference.com/2008/Europe/.

Hack in the Box Security Conference 2008 takes place 27–30 October 2008 in Kuala Lumpur, Malaysia. This year's event will see new hands-on sessions designed to give attendees a closer and deeper understanding of various security issues from physical security bypass methods to the security of RFID and other wireless-based technologies. For more information see http://conference.hackinthebox.org/.

Hacker Halted Malaysia 2008 takes place 3–6 November 2008 in Selangor, Malaysia. For more information see http://www.hackerhalted.com/malaysia.

CSI 2008 takes place 15–21 November 2008 in National Harbor, MD, USA. Online registration will be available soon at http://www.csiannual.com/.

The 2nd Annual Chief Security Officer Summit will take place 8–10 December 2008 in Geneva, Switzerland. For details see http://www.mistieurope.com/.

ACSAC 24 (the Applied Computer Security Associates' Annual Computer Security Conference) will be held 8–12 December 2008 in Anaheim, CA, USA. For details see http://www.acsac.org/.

AVAR 2008 will be held 10–12 December 2008 in New Delhi, India. The 11th Association of anti-Virus Asia Researchers International Conference will be hosted by Quick Heal Technologies Pvt. See http://www.aavar.org/avar2008/index.htm.

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/

vbSpam supplement

CONTENTS

S1 **NEWS & EVENTS**

S1 **FEATURE**
Evading CAPTCHA

NEWS & EVENTS

PROLIFIC SPAMMER JAILED

A man who sent more than 50,000 spam emails an hour and who has been a known spammer since 1999 has been sentenced to nearly four years in jail after pleading guilty to charges of fraud, spamming and tax evasion.

Robert Soloway was arrested 14 months ago on a total of 35 charges that included mail fraud, wire fraud, aggravated identity theft and money laundering. Prosecutors had been hoping for a stiffer sentence and had requested he be sent to prison for nine years, taking into account both the scale of his spamming operations and the fact that he had previously been investigated for spamming activities – in 1999 he told Californian authorities he was sorry for his actions and would end his spamming career, but instead just moved his operations to a different state and continued spamming.

Once again Soloway made an attempt at an apology, saying 'I take full responsibility for everything I've done. I am sorry for all the people that got the emails ... I am very embarrassed and ashamed.' However, an apology is pretty hard to swallow when it comes from someone who has spent much of the last nine years boasting about his spamming techniques, failing to comply with court orders that banned him from spamming and dodging the millions of dollars in fines and compensation he was ordered to pay by the civil courts. *VB* hopes he enjoys his time in jail.

EVENTS

CEAS 2008 will take place 21–22 August 2008 in Mountain View, CA, USA. For more information about the event see http://www.ceas.cc/2008/.

The 14th general meeting of the Messaging Anti-Abuse Working Group (MAAWG) will be held in Harbour Beach, FL, USA, 22–24 September 2008. See http://www.maawg.org/.

FEATURE

EVADING CAPTCHA

Martin Overton
Independent researcher, UK

'Evading CAPTCHA' may sound like a theme for a spy or war story, but this has nothing to do with spies or traditional conflicts in war zones. In this article I will cover the use of CAPTCHAs and how cybercriminals are trying to evade them so that they can create bogus accounts on web services such as *Google Mail*, *Yahoo! Mail* and *Microsoft Live Hotmail*.

The following is a brief description of a CAPTCHA [1]:

> 'The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University. At the time, they developed the first CAPTCHA to be used by *Yahoo* ... A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text ... but current computer programs can't.'

Figure 1: Example CAPTCHA (actually a reCAPTCHA [2]).

Figure 1 shows an example of the distorted text displayed in a CAPTCHA.

If you have created webmail or similar accounts at *Yahoo! Mail*, *Google Mail* or *Microsoft Live Hotmail* you will have had to solve a CAPTCHA to complete the sign-up form and prove that you are a human and not a machine. Many websites also use CAPTCHAs for forum sign-ups, feedback forms, etc. The idea is to make it too difficult or time consuming for the bad guys and girls to bother filling in sign-up and feedback/contact forms and to stop them from automating the process using bots and botnets. Love them or hate them, CAPTCHAs have their place in web security.

Spammers, scammers and malware authors have started to move to the likes of the *Google Mail*, *Yahoo! Mail* and *Microsoft Live Hotmail* web mail services to try and improve the chances of their output bypassing anti-spam defences.

This is because anti-spam defences are now in place almost everywhere, as even home users have finally woken up to the spam problem (commercial organizations, academia and government departments have mostly been on the ball for quite a few years).

But why are the cybercriminals bothering to use these web mail systems? Simply because anti-spam defences such as Domain Keys (aka DKIM) [3] are used by both *Yahoo! Mail* and *Google Mail* to prove that emails have originated from their systems; this in turn gives any email sent via their systems extra credibility and makes them less likely to be filtered as spam at the receiving server.

Microsoft Live Hotmail uses a similar technique known as Sender ID [4], which is heavily based on SPF. This, like DKIM, is seen to add credibility to emails and make them less likely to be flagged as spam.

Now do you see why the bad guys and girls are interested in CAPTCHA-evading/solving techniques and tools?

ATTACK, ATTACK

So what sort of techniques can be used to evade or beat CAPTCHA-based sign-ups?

The types of attack that have been shown to work include computer character recognition (OCR or shape matching and object recognition) [5], social engineering (humans) and bots as well as mixtures of these attack vectors. So, let us have a look at each of these methods. We will start with the easiest and most effective, which almost certainly has the highest accuracy rate: social engineering.

STRIPTEASE!

At the end of October 2007[1] we saw a very interesting technique being used to try to make unsuspecting users help the criminals evade or beat CAPTCHAs. This was called Troj/CAPTCHA-A (*Sophos*). The following is a brief explanation of how it works [6].

> 'The Troj/CAPTCHA-A Trojan horse poses as a sexy game, offering increasingly saucy photographs of a blonde model called Melissa in exchange for the user correctly unscrambling an image. The obfuscated image is a CAPTCHA used by websites to ensure that requests are being made by a human being and not a bot ... every time a CAPTCHA is entered correctly Melissa donates another item of clothing to charity.'

This particular CAPTCHA attack was aimed squarely at breaking those used by *Yahoo! Mail.* Figure 2 shows a series of screenshots from Troj/CAPTCHA-A.

[1] Most anti-malware descriptions show that this was first discovered on 1 November, a few claim that it was 31 October.

Figure 2: Troj/CAPTCHA/A screenshots (courtesy of Sophos).

Not surprisingly, this trojan-assisted attack worked quite well as it used one of the key social-engineering hooks: sex.

However, it isn't the only way that the bad guys and girls encourage humans to solve CAPTCHAs for them, they also use another common social-engineering hook: greed. Yes, they simply *pay* people to solve them!

Websense found a document [7] that appears to instruct workers on the art of solving CAPTCHAs. It states (translated from Russian):

> 'If you are unable to recognize a picture or it is not loaded (picture appears black, empty picture), just press Enter. Do not enter random characters! If there is a delay in downloading images, exit from your account, refresh the page and go again.'

It is not known how much the person gets paid for each CAPTCHA solved [8], but the original document does state 'No more than one payout per day. Minimum balance to be paid out is $3'.

To those of us in the developed and wealthy parts of the world the level of payments being offered seems a pittance, however many of those who live in the poorer parts of the world would see this as a golden opportunity to be grasped with both hands. It is not known whether those who run this service actually pay out, and if they do, how.

THE RISE OF THE MACHINES

It was suggested by some researchers earlier this year [9] that bots and botnets are now being used successfully to break the CAPTCHAs used by *Google Mail* (aka *Gmail*):

> '*Gmail* is being targeted in recent spammer tactics. Spammers in these attacks managed to create bots that are capable of signing up and creating random *Gmail* accounts for spamming purposes.'

However, the research seems to indicate that the attacks on *Google Mail* require the use of several bots – a sort of tag-team wrestling approach:

> 'The *Gmail* signing process involves two botted hosts (or CAPTCHA breaking hosts) ... On average, only one in every five CAPTCHA breaking requests are successfully including both algorithms used by the bot, approximating a success rate of 20%.'

It isn't just *Google Mail* that has been targeted using bots, both *Yahoo! Mail* and *Microsoft Live Hotmail* [10] have also been attacked successfully by using bots to solve their CAPTCHAs.

According to *Websense*, this is how the *Microsoft Live Hotmail* account sign-up is automated using a single bot:

> 'First, the bot is observed to request the *Live Mail* registration page and it begins filling in the necessary form fields (as any ordinary user would be required to) with random data. When it comes to the CAPTCHA verification test, the bot sends the CAPTCHA image to its CAPTCHA breaking service for the text in the image.
>
> '...on average, one in every three CAPTCHA breaking requests succeeds – setting the bot's success rate at around 30–35%.'

This is quite an amazing success rate for something that a computer is not supposed to be able to do.

However, I don't believe that the current success rates using bots and botnets are completely accurate I suspect, as do others, that this is more of a cyborg-based [11] attack, with the work using both bots and humans to defeat automated account sign-ups and CAPTCHA solving. The report from *Websense* on bots being used to solve *Google Mail* CAPTCHAs seems to confirm my suspicions.

HOW BIG A PROBLEM IS THIS REALLY?

An article which appeared in *The Register* in March 2008 [12] stated:

> 'An analysis of spam trends in February 2008 by net security firm *MessageLabs* revealed that 4.6 per cent of all spam originates from web mail-based services.
>
> 'The proportion of spam from *Gmail* increased two-fold from 1.3 per cent in January to 2.6 per cent in February, most of which spamvertised skin-flick websites. *Yahoo! Mail* was the most abused web mail service, responsible for sending 88.7 per cent of all web mail-based spam.'

This shows that the problem is still quite small (4.6%) when compared with global spam quantities. Unfortunately I suspect that the use of webmail services may well take over from the current almost exclusive use of botnets to send spam. However, the criminals will need to come up with some more efficient ways of evading or solving CAPTCHAs first.

CONCLUSIONS

Is the CAPTCHA still useful? Yes, and more complex and harder-to-defeat systems have been developed, including 3D [13] and image-recognition [14] (rather than text-based) varieties.

It seems that spammers are intent on continuing their assault on our inboxes, offering things as diverse as university degrees and penny stocks to pills and potions to make various body parts larger or firmer.

The funny thing is that this market would soon collapse and become financially non-viable if the 11 per cent of recipients [15] (or 22 per cent of British consumers [16]) who currently buy the items advertised in spam would just stop doing so. (Yes, I know, that is about as likely to happen as world peace.)

Until then those that push spam will continue to look for ways to ensure – or at least improve the chances – that their 'crud' will end up in inboxes all over the world.

Repeat after me: '*I will not buy from spam*'.

REFERENCES

[1] http://www.captcha.net/.

[2] http://recaptcha.net/learnmore.html.

[3] http://en.wikipedia.org/wiki/DomainKeys.

[4] http://en.wikipedia.org/wiki/SenderID.

[5] http://www.cs.sfu.ca/~mori/research/gimpy/.

[6] http://www.sophos.com/security/blog/2007/11/737.html.

[7] http://securitylabs.websense.com/content/Blogs/2919.aspx.

[8] http://bits.blogs.nytimes.com/2008/03/13/breaking-google-captchas-for-3-a-day/index.html?ref=technology.

[9] http://securitylabs.websense.com/content/Blogs/2919.aspx.

[10] http://securitylabs.websense.com/content/Blogs/2907.aspx.

[11] http://en.wikipedia.org/wiki/Cyborg.

[12] http://www.theregister.co.uk/2008/03/14/captcha_serfs/.

[13] http://spamfizzle.com/CAPTCHA.aspx.

[14] http://research.microsoft.com/asirra/.

[15] http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=165701785.

[16] http://www.theregister.co.uk/2004/12/10/spam_buyers_survey_bsa/.