

virus

BULLETIN

Fighting malware and spam

CONTENTS

- 2 **COMMENT**
IE 6 – 5 – 4 – 3 – 2 – 1
- 3 **NEWS**
No mail for Alisons, Alberts, Algernons...
Old breach rears its head
- 3 **VIRUS PREVALENCE TABLE**
- TECHNICAL FEATURES**
- 4 Defeating mTANs for profit – part two
- 11 Hiding in plain sight
- CONFERENCE REPORTS**
- 14 Phighting cybercrime together
- 16 RSA 2011 conference review
- 20 **FEATURE**
Sender authentication – practical implementations
- 25 **COMPARATIVE REVIEW**
VB100 comparative review on Windows XP SP3
- 81 **END NOTES & NEWS**

IN THIS ISSUE

COUNTDOWN TO ZERO?

With 34.5% of the market share in China, Gabor Szappanos fears that IE 6 – the browser with 473 publicly known unpatched vulnerabilities – will not disappear any time soon.

page 2

MEETING OF MINDS

Martijn Grooten and Jeannette Jarvis report on two important security industry events: the first APWG eCrime Researchers Sync-Up and the 20th annual RSA conference.

pages 14 and 16

VB100 ON WINDOWS XP

With a staggering 69 products on this month's VB100 test bench, the VB lab team hoped to see plenty of reliability and stability. But, while the majority of products were well behaved, the team was woefully disappointed by a handful of unruly participants. John Hawes has all the details.

page 25





'...the outlook is alarming when you consider the browser's local prevalence in China, which peaks at 34.5%.'

Gabor Szappanos, VirusBuster

IE 6 – 5 – 4 – 3 – 2 – 1

2001 was a memorable year for me. I started working at *VirusBuster* and thus officially joined the AV industry. I got my first cell phone. I bought my first car (a used one, but who cared?). I moved to a new apartment, which was largely due to the fact that my son had just been born. I also bought a new home PC. 2001 was also the year that *Microsoft* released *Internet Explorer (IE) 6*.

Over a decade has passed since then. My company has moved office twice. I have switched cell phone four times. I have replaced my home PC three times. I've moved to a new apartment, and I've applied several hotfixes and replaced the engine of my car.

Unlike all these other elements in my life, *IE 6* has prevailed. On releasing *IE 9* – three major versions away from our title piece – *Microsoft* launched a website¹ tracking the astonishingly high prevalence of this elderly web browser (according to data collected by *Net Applications* it accounted for 12% of the market share overall in February 2011). It's not only that the overall prevalence of the browser is high, but the outlook is alarming when you consider the browser's local prevalence in China, which peaks at 34.5%.

What could be behind this phenomenon? One would expect that in the 21st century – which is all about increasingly rapid change, especially in IT – users would

¹<http://ie6countdown.com/>

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Web Developer: Paul Hettler

Consulting Editors:

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, USA*

upgrade their operating system (or at least the major applications) every few years. However, nothing could be further from the truth.

At the root of the problem is a combination of *Windows XP* and *Windows Update*. *XP* came with *IE 6* preinstalled, and was a very successful operating system – more successful than its successor, and this is one major part of the problem. Although a fair number of *IE* updates were released, the *XP* service packs did not include the installers for them. One could install them with automatic update or by visiting the *Windows Update* website, but both of these required a genuine, non-pirated OS version, as with *Windows XP* came the debut of *Windows Genuine Advantage*. And herein lies the other part of the problem. The most popular operating system in China is *Windows XP*, with 81.8% of the market share. According to several sources, the software piracy rate in China is around 80%, so it is little surprise that over a third of web browsers (or operating systems) have not been upgraded. Manual download and installation of the updates is possible, but beyond the capabilities of most computer users. The situation is not helped by the fact that many websites in China are optimized for and tested only on *IE 6*, thus forcing users to stick with the old version.

Taking all these facts into consideration, I am afraid that *IE 6* will not disappear any time soon. The target population must be served by enabling *Internet Explorer* upgrades (and critical OS vulnerability fixes) regardless of licence, or even by a final wrap-up installer of *XP*.

But is it really a problem we should care about? Why bother if one third of Chinese web browsers are as old as an entry-level single malt whisky?

According to *Wikipedia*², *IE 6* has 473 publicly known unpatched vulnerabilities (i.e. these will never be fixed). All other versions and browsers have just 94 combined. In other words, *IE 6* has five times more open vulnerabilities than all the other browsers put together. One other thing has also changed since 2001. Back then, the primary distribution media for malware was email. Nowadays, the primary intrusion media are drive-by exploits introduced during web browsing – and this is what makes using this dinosaur of a browser so dangerous. Failing to upgrade the browser leaves the most vulnerable entrance to the computing system the least protected.

Before you ask, my son is fine. He's the only thing in my inventory list from 2001 that keeps improving.

²http://en.wikipedia.org/w/index.php?title=Comparison_of_web_browsers&oldid=421471109#Vulnerabilities

NEWS

NO MAIL FOR ALISONS, ALBERTS, ALGERNONS...

McAfee customers whose email address begins with the letter 'A' may have found their inboxes unexpectedly quiet earlier this month when a flawed update script in the *MX Logic* managed email filtering service (acquired by *McAfee* in 2009) prevented them from receiving mail. According to *McAfee*, temporary account verification issues were experienced by users with non-alphanumeric email addresses and aliases up to the letter 'A'. The issue was identified and fixed within 12 hours.

This is not the first time an innocent letter has caused problems and red faces for a security firm – in 2003, *Trend Micro* quarantined the letter 'P', when a bug in an update for email security product *eManager* quarantined all incoming mail containing the letter 'P' (see *VB*, June 2003, p.3).

OLD BREACH REARS ITS HEAD

The potential long-lasting effects of a security breach were highlighted earlier this month when a small Illinois-based bank revealed that customers' payment card information had been compromised at card processor *Heartland Payment Systems* – which suffered a breach back in 2008.

It is thought that, more than two years after the breach, crooks are still working their way through the stolen card details. While many of the cards will no longer be active after such a long period of time (either because they have expired or because they have been cancelled), the flip side is that if a credit card has gone for two years without any signs of fraudulent activity, banks and retailers are likely to assume that it hasn't been stolen – thus making it easier for the criminals to defraud.

The news comes just days after email marketing firm *Epsilon* admitted that hackers had obtained access to its customer data. The Dallas-based company claims that the data breach affected only around 2% of its clients and that the information obtained was limited to email addresses and/or customer names only. However, a growing list of companies is known to have had their customer lists stolen. Among the victims are *Hilton Honors*, *Walgreens*, *Disney Destinations*, *Marks and Spencer*, *Capital One*, *TiVo*, *JPMorgan Chase* and *Citibank*.

Even if the hackers did only obtain names and email addresses, these companies' customers will now be at increased risk of phishing – and with the crooks able to personalize their emails, the phishes will be harder to spot than generic ones. Most of the affected companies have warned their customers to be on the alert for phishing attempts.

Prevalence Table – February 2011^[1]

Malware	Type	%
Autorun	Worm	9.13%
VB	Worm	7.43%
Conficker/Downadup	Worm	5.75%
Agent	Trojan	5.00%
FakeAlert/Renos	Rogue AV	4.53%
Exploit-misc	Exploit	3.86%
Adware-misc	Adware	3.68%
Downloader-misc	Trojan	3.49%
Delf	Trojan	2.89%
OnlineGames	Trojan	2.81%
Injector	Trojan	2.66%
Sality	Virus	2.35%
Heuristic/generic	Virus/worm	2.17%
StartPage	Trojan	2.09%
Kryptik	Trojan	2.06%
Small	Trojan	1.77%
Heuristic/generic	Misc	1.54%
Autolt	Trojan	1.50%
Hupigon	Trojan	1.49%
Zbot	Trojan	1.46%
Dropper-misc	Trojan	1.40%
Heuristic/generic	Trojan	1.40%
Crack/Keygen	PU	1.33%
Iframe	Exploit	1.28%
Alureon	Trojan	1.27%
PDF	Exploit	1.20%
Bifrose/Pakes	Trojan	1.18%
Virtumonde/Vundo	Trojan	1.12%
Tanatos	Worm	1.10%
Virut	Virus	1.07%
PCCClient	Trojan	0.89%
Hoax	PU	0.81%
Others ^[2]		18.28%
Total		100.00%

^[1]Figures compiled from desktop-level detections.

^[2]Readers are reminded that a complete listing is posted at <http://www.virusbtn.com/Prevalence/>.

TECHNICAL FEATURE 1

DEFEATING mTANS FOR PROFIT – PART TWO

Axelle Apvrille, Kyle Yang
Fortinet

Until recently, malware on mobile devices had not been used for organized crime involving large amounts of money. This changed when the infamous Zeus gang, known for targeting online banking, started to show a clear interest in infecting mobile devices and released a new version of their bot to propagate a trojan for mobile phones.

This two-part series (based on a paper presented at ShmooCon 2011) presents an in-depth analysis of the Zitmo trojan. Last month [1] we presented some background information on Zeus and mobile malware and looked at how the attack behind Zitmo works. In this article we will present our reverse engineering of Zitmo and attempt to draw lessons from the attack, as well as suggesting methods for circumventing it.

1. ZITMO FOR SYMBIAN

The Zitmo package consists of a few resource files and an executable named NokiaUpdate.exe. The resource files are typical to *Symbian* applications – such as the resource in c:\private\101f875a\import, which is used to automatically restart an executable after the phone reboots – and are of little interest for the purpose of reverse engineering. NokiaUpdate.exe is more interesting, however. The .exe file centralizes all malicious functionalities in a single daemon, and this is what we analyse.

1.1 Initial tasks

The first time NokiaUpdate.exe is run after installation it sends an SMS to +44778148xxxx with the text ‘App installed ok’. Both the text and the phone number are hard coded, hence easily locatable in the malware’s strings¹. To ensure that no SMS will be sent the next time the .exe file is run, the file c:\20022B8E\firststart.dat is created and used as a flag. The presence of the file indicates that the trojan has already been launched; if it is absent, an SMS should be sent.

During the first start-up, the trojan also creates an SQL database (c:\20022B8E\Numbers.db) containing three tables: tbl contact, tbl phone number and tbl history, as depicted in Tables 1–3. The contact table lists contacts to spy on. Only the first column, the index, is used by Zitmo. The other columns probably refer to the name descriptions

¹ As for most *Symbian OS 9* executables, NokiaUpdate.exe must first be uncompressed before searching for strings.

index 32-bit integer	name 16-bit Unicode	descr 16-bit Unicode	pb_contact_id 32-bit int
1	Not used	Not used	Not used
2	Not used	Not used	Not used

Table 1: Example of contact table.

contact id 32-bit int	phone number 16-bit Unicode
1	0611111111
2	1234567890

Table 2: Example of phone number table.

event id 8-bit int	pn id 32-bit int	date type	description 16-bit Unicode	contact info 16-bit Unicode	contact id 32-bit int
1		27-10-2010			2

Table 3: Example of history table.

of the contacts and their indexes in the phone’s address book (if listed there). The phone number table sets the relationship between contact indexes and their phone numbers. The contact id column corresponds to the index column of the contact table. Finally, the history table stores events related to those contacts such as incoming calls.

1.2 Listening to incoming SMS messages

Once the initial set-up is complete, the trojan listens for incoming SMS messages. To do so, it uses the technique described in [2], i.e. it opens and binds a socket to the SMS channel. The *Symbian* APIs provide several ways to open SMS sockets, such as receiving anything (ESmsAddrRecvAny), receiving messages that start with a special prefix (ESmsAddrMatchText), or using a special port (ESmsAddrApplication8BitPort) to receive messages. Since opening an SMS socket to receive all messages is not possible because the phone’s built-in applications are already using this method, the trojan uses ESmsAddrMatchText but with a special trick (see Figure 1): it specifies that the incoming messages to receive must begin with nothing. This method works and actually receives all incoming SMSs. Note this trick has also been explained in [3].

In this article, ARM assembly listings are all taken from Zitmo. They use the following convention: functions beginning with ‘NokiaUpdate’ have been named and reverse engineered by us, functions beginning with ‘ZN’ have

automatically been resolved by *IDA Pro*: they correspond to standard *Symbian* API calls. Other functions, starting with 'sub', are usually not very relevant and have not been reversed. Lines starting with a semicolon are comments.

```

; Open socket RSocket::Open(RSocketServ &,uint,uint,uint)
BL _ZN7RSocket4OpenER11RSocketServjjj
STR R0, [R11,#errcode] ; store the return code
LDR R3, [R11,#errcode]
CMP R3, #0 ; if return code != KErrNone
BNE loc_7C90DAF8 ; jump to this location if error
SUB R0, R11, #0x54
BL _ZN8TSmsAddrC1Ev ; TSmsAddr::TSmsAddr(void)
SUB R0, R11, #0x54
MOV R1, #4 ; ESmsAddrMatchText
; set socket family with SetSmsAddrFamily =
ESmsAddrMatchText
NL _ZN8TSmsAddr16SetSmsAddrFamilyE14TSmsAddrFamily
SUB R0, R11, #0x54
SUB R3, R11, #0x24
MOV R1, R3 ; _L8("")
; set text to match to _L8("")
BL _ZN8TSmsAddr12SetTextMatchERK6TDesC8
    
```

Figure 1: Assembly code to intercept all incoming SMS messages.

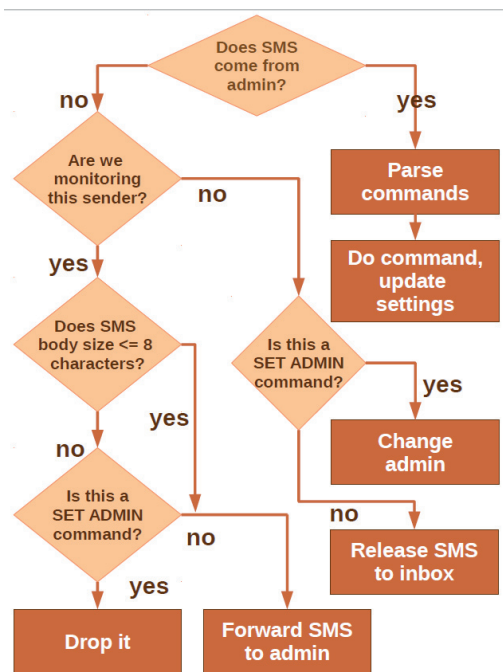


Figure 2: How Zitmo processes incoming SMS messages.

Each time the mobile phone receives an SMS, the trojan's socket intercepts it (before it reaches the phone's inbox). It reads its content in the socket (RSmsSocketReadStream class in the API) and processes it.

An explanation of SMS processing is illustrated in Figure 2. The trojan checks who has sent the incoming SMS. There are three cases:

1. Sender is monitored. If the SMS comes from a phone number the trojan is configured to monitor (i.e. if the phone number is specifically mentioned in the trojan's phone number table, or if the trojan is configured to monitor all incoming numbers), the SMS is diverted to the administrator's phone number (see Figure 3). The victim will never see this SMS in his inbox.
2. Sender is administrator. In this case, the trojan parses the message body for a known command and processes it.
3. Sender is neither monitored nor administrator. This happens when the victim receives an SMS from somebody the malicious gang does not care about (in which case the SMS is released to the victim's inbox – the fact that the victim receives some SMS messages helps reduce suspicion) or, in other cases, when the administrator's phone number changes. In this case, the administrator can send a SET ADMIN command from the new administrator phone. In fact, we believe this is a flaw in the trojan's protocol and will explain later how we have abused it. Note that the SET ADMIN command is the only one a non-administrator can send.

1.3 Remote SMS commands

Zitmo implements 10 different commands: ON, OFF, SET ADMIN, ADD SENDER ALL, ADD SENDER xx, REM

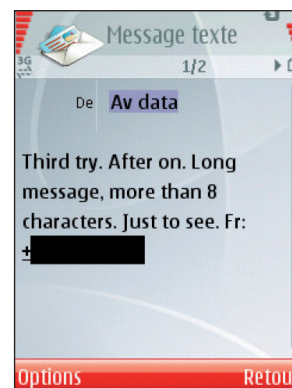


Figure 3: SMS intercepted by Zitmo and forwarded to the administrator (lab test phone).

SENDER ALL, REM SENDER xx, SET SENDER xx, BLOCK ON, BLOCK OFF. All of these have been described either in [3, 4] or in our previous work [5]. What hasn't been explained yet is how the trojan recognizes the commands in the SMS and processes them.

Basically, the trojan reads the SMS body, converts it to upper case and counts the number of spaces in order to work out the number of words in it. If there are no spaces, the only likely commands are ON or OFF. If there is one space, the only possible commands are BLOCK ON or BLOCK OFF etc. (see Figure 4). This is rather a strange way to recognize commands, and is perhaps copied from a more sophisticated library.

Once the trojan knows which command it is dealing with, it must react. Its immediate action always consists of updating its settings and/or updating the contact and phone number tables (ADD SENDER, REM SENDER and SET SENDER commands). Later, the effective behaviour of the trojan relies only on those two parameters.

The trojan's settings are dumped in c:\20022B8E\settings2.dat. The format of the file is the following:

1. The first byte represents the state of the trojan: 0 if it is off, 1 if it is on (enabled).

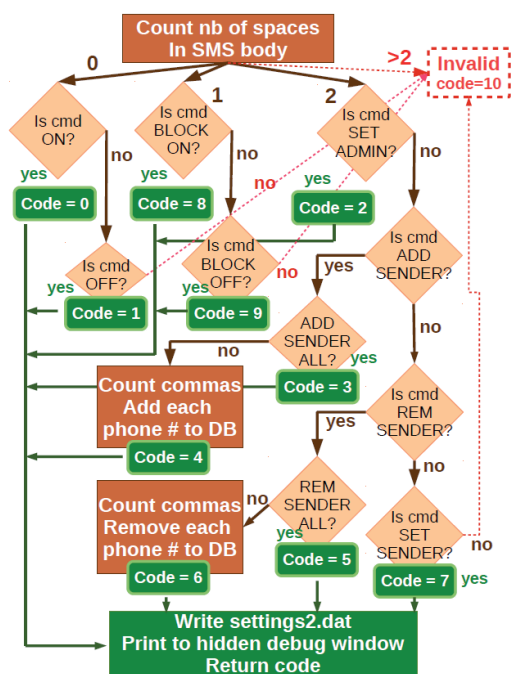


Figure 4: How Zitmo parses SMS commands.

```
00000000 00 01 00 34 2b 34 34 37 37 38 31 34 38 x x x |...4+44778148xxxx|
00000010 x |x|
```

Figure 5: Zitmo's initial settings file.

2. The second byte represents the monitoring case: 0 to monitor phone numbers specified in the table, and 1 to monitor any numbers (in the case of ADD SENDER ALL).
3. The third byte represents the blocking state: 0 if calls must not be blocked and 1 if they must be blocked (BLOCK ON/OFF).
4. The remaining bytes correspond to the externalized 16-bit Unicode string object (TDesC16) for the administrator's phone number.

For example, the settings of Figure 5 correspond to a disabled trojan (OFF), configured to steal any incoming SMS messages (ADD SENDER ALL) and let incoming calls go through (BLOCK OFF). The administrator's phone number is +44778148xxxx.

For the ADD SENDER, REM SENDER and SET SENDER commands, the trojan also updates the contact and phone number tables with the phone numbers specified in the rest of the command. For example, ADD SENDER 1234567890 creates a new row in the contact table for index 2 (see Table 1). In the phone number table, a new row is added too, and index 2 is mapped to phone number 1234567890 (see Table 2). The other columns are not used in Zitmo.

1.4 SMS actions

In the end, there are only three different outcomes for an SMS received by the trojan: release the SMS to the victim's inbox, divert it to the administrator's phone number or just drop it. This is how the trojan does it:

- Releasing the SMS actually consists of creating a new SMS message in the phone's inbox. To do this, the trojan first switches to the inbox entry (SwitchCurrentEntryL specifying the inbox KMsvGlobalInboxIndex-EntryIdValue – see Figure 6).

In *Symbian*, each entry (CMsvEntry object) consists of generic information (e.g. subject, date) held in a TMsvEntry object, and message-type specific data (e.g. headers, body) in a CMsvStore object [6]. So the trojan first copies the generic information to the entry and then marks the change (CMsvEntry::ChangeL).

Then, it copies the SMS headers and body to the entry's store. It must make sure the header is marked as an SMS to deliver (ESmsDeliver – see Figure 7) so that it appears as a message coming from the sender (and not to the sender).

```

; switch to entry: CBaseMtm::SwitchCurrentEntryL(long)
LDR R0, [R3,#0x34]
MOV R1, 0x1002 ; KMsVGlobalInboxIndexEntryIdValue
BL _ZN8CBaseMtm19SwitchCurrentEntryLEl

```

Figure 6: Code to switch to global inbox entry.

```

; CSmsHeader::NewL(CSmsPDU::TSmsPDUType,CEditableText &)
MOV R0, #0 ; ESmsDeliver
LDR R1, [R11,#var_80]
BL _ZN10CSmsHeader4NewLEN7CSmsPDU11TSmsPDUTypeER13CEditableText
...
LDR R0, [R11,#cmsvstore]
BL _ZN9CMsvStore7CommitLEv ; CMsvStore::CommitL(void)

```

Figure 7: Setting SMS as 'to deliver'.

```

; Copy original body in TDes16
LDR R3, [R11,#var_18]
ADD R0, R3, #0xC0
LDR R1, [R11,#incomingmstext]
BL _ZN6TDes164CopyERK7TDesC16
; Point to " Fr:"
SUB R0, R11, #0x84
LDR R1, =aFr ; " Fr:"
BL _ZN7TPtrC16C1EPKt ; TPtrC16::TPtrC16(ushort const*)
; Append " Fr:" to body
SUB R2, R11, #0x84
LDR R3, [R11,#var_18]
ADD R0, R3, #0xC0
MOV R1, R2
BL _ZN6TDes166AppendERK7TDesC16 ; TDes16::Append(TDesC16 const&)
; Append sender's phone number
LDR R3, [R11,#var_18]
ADD R0, R3, #0xC0
SUB R3, R11, #0x6C ; sender's phone number
MOV R1, R3
BL _ZN6TDes166AppendERK7TDesC16 ; TDes16::Append(TDesC16 const&)
...
; Send SMS
BL NokiaUpdate_CommitDraft

```

Figure 8: Adding the sender's phone number to the body of the SMS.

```

; RSocket::Ioctl(uint,TRequestStatus &,TDes8 *,uint)
MOV R1, #0x304 ; KIoctlReadMessageSucceeded
MOV R3, R12
BL _ZN7RSocket5IoctlEjR14TRequestStatusP5TDes8j

```

Figure 9: Call RSocket::Ioctl with KIoctlReadMessageSucceeded to indicate the message was processed correctly.

Finally, it commits the change (CommitL). Note also that if the message to release comes from a contact listed in the phone's address book, the trojan opens the address book, searches for the contact whose phone number matches the sender of the SMS, retrieves the contact's first and last name and writes this information in the inbox, instead of the phone number. This ensures, for instance, that the SMS appears to come from 'Axelle Apvrille' and not from '+336xxxxxx'.

- Diverting the SMS to the administrator's phone number is quite similar, except a new entry is created in the Drafts box. And, of course, the new SMS is created with the administrator as recipient, and the body is modified to include at the end the phone number of the original sender of the SMS (see the result in Figure 3: the original sender's phone number is mentioned after 'Fr:'). The trojan then marks this entry as changed (CMsvEntry::ChangeL – see Figure 8), sets the SMS service centre and finally sends it.
- Dropping the SMS (i.e. not displaying the SMS at all) basically consists of doing nothing with the SMS once it has been read. More precisely, the trojan reads the SMS from the SMS socket, processes it and decides it must be dropped, does not commit any new entry on the phone's message server, and makes sure it marks the socket message as successfully processed (as in the two other cases) – see Figure 9. It is important to mark the SMS PDU as successfully processed or it will reappear in the inbox on the next reboot.

1.5 Reverse engineering techniques

Symbian malware is typically reverse engineered using static code analysis. *IDA Pro* is particularly handy for Symbian because it supports ARM assembler and automatically resolves most Symbian API calls. Static code analysis represents a high percentage of our reverse engineering for Zitmo, but in addition, we have been able to use two other techniques:

1. Spoofing the administrator. As mentioned previously, the trojan's protocol to configure a new phone number for the administrator is flawed, because anybody can claim to be the new administrator, provided their phone number is not currently being monitored. So, for our experiments, we used two phones: one infected by the Zitmo malware, and the other one to act as the administrator (instead of the real Zeus gang). There are two ways to become the new administrator.

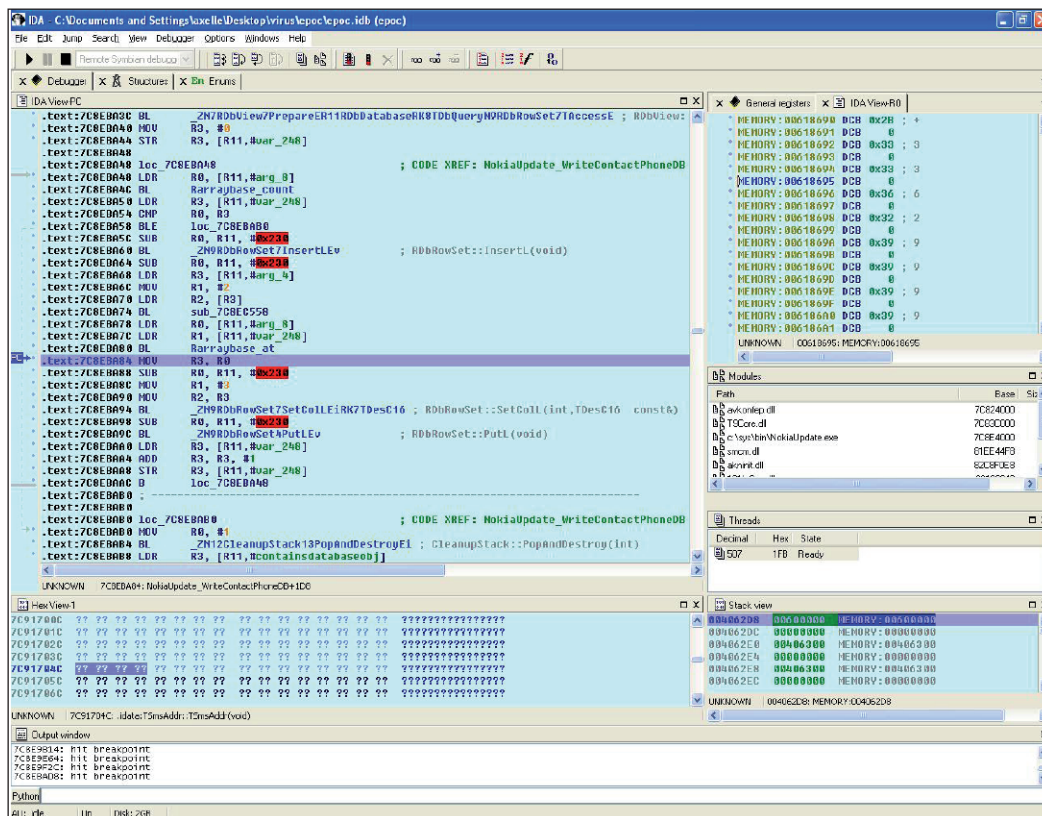


Figure 10: Screenshot of IDA Pro during a remote step debugging of the trojan. In this case, the function is adding a new row to the phone number table of the trojan.

The simplest way we found was to send a ‘set admin’ command (due to a bug in the trojan the command must be in lower case) with the phone number of our second phone. The more complicated way consisted of crafting a settings file with the new administrator’s phone number (for example, replacing the phone number at the end of the code in Figure 5). The settings file is located in a private, restricted directory though, so it is necessary first to install a hack on the phone [7] to access the directory.

Once we had set up our phone as the new administrator, it was much easier to understand the code of the trojan: set up remote debugging of the device, send a command by SMS and step through the assembly line by line. For example, in Figure 10, we are debugging, step by step, the function that adds a new contact to the trojan’s database for monitoring.

2. Unhiding the console window. Static analysis of the trojan reveals that it actually creates a text

editor window and writes debug information to it. Under normal circumstances, this debug window is not shown because the malware authors have hidden it: basically, this consists of setting the window as hidden (CApaWindowGroupName::SetHidden(ETrue)), and making sure the window stays in the background (RWindowTreeNode::SetOrdinalPosition to ECoeWinPriorityNeverAtFrom=-1000 or ECoeWinPriorityNormal=0). See [8] for more information. So, to show this debug window, we set breakpoints to the SetHidden and SetOrdinalPosition API calls, ran until we reached those breakpoints, and then each time we reached SetHidden, we modified ETrue (=1) to EFalse (=0) and each time we reached SetOrdinalPosition, we set the priorities to ECoeWinPriorityAlways-AtFront =1000 = 0x3e8. This caused the debug window to appear.

Figure 11 shows the debug window after the trojan has read its settings. First, there is the administrator’s phone number (blurred – a test

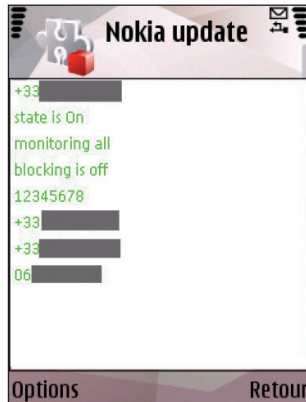


Figure 11: Zitmo's debug window dynamically sent to the foreground.

phone in our lab). Then we see the trojan is enabled, monitoring any incoming number, and incoming calls are not blocked. Finally, the last few phone numbers are those listed in the phone number table (partially blurred). We added those phone numbers to our test phone using the relevant ADD SENDER commands. They are ignored because the trojan is configured to monitor all incoming numbers.

2. SECURITY CONSIDERATIONS AND SOLUTIONS

Zitmo is quite worrying for two main reasons:

First, it is difficult to spot. Even security-aware users could fall into the trap and have their mobile phone infected. The only (weak) signs that something is amiss consist of 1. receiving an alleged certificate packaged as a *Symbian* package (.sis or .sisx) and not as a standard certificate (.p12 or .pfx), and 2. having an unknown application listed in the phone's Application Manager. The rest of the social engineering is quite plausible. Moreover, the trojan is signed by *Symbian*, which gives end-users a false sense of security.

In reality, the fact that the trojan went through the *Express Signed* program does not mean the application was reviewed. Only some (randomly selected) applications are reviewed, and Zitmo was not one of those. Obviously, a more thorough analysis of the packages undergoing the *Express Signed* program (e.g. the *Symbian* security capabilities they require, in-house testing etc.) might block more malware, but this has a financial cost nobody seems to be willing to pay. The *Apple Store* and the *Android Market* get the money from applications sales

– an interesting concept, although it does not make them technically immune to malware².

This issue is not simple to remedy with the current mobile framework. The most technically promising solutions we are aware of base malware detection on behaviour analysis [9, 10], on SMS sending profiles [11], or on matching rules combining security capabilities [12]. They should, however, be tested in real-life situations, and perhaps be combined with other approaches such as mobile anti-virus solutions or firewalls.

The second reason Zitmo gives us cause for concern is that it initiates on-demand two-factor authentication. In part one of this series [1], we explained that Zitmo gives cybercriminals the capability to authenticate whenever they want, using two different authentication factors.

Two-factor authentication is a good security measure, but only as long as the security of the systems in charge of each factor remains intact. In Zitmo's case this does not happen: from a compromised PC in charge of the first authentication factor, it manages to compromise the mobile phone which handles the second authentication factor. The insecurity of the PC leads to the insecurity of the mobile phone.

Hardware authentication tokens, such as SecurID tokens, are not a solution to this issue. These were defeated by prior versions of Zeus, because the one-time password they generate is entered on a compromised host (the PC). However, in that case, cybercriminals cannot initiate authentication on demand and must wait for the victim to do it.

We would recommend the use of a smartcard-based authentication: a smartcard reader (with its own keypad) is attached to the PC. To authenticate, the end-user must insert his smartcard into the reader and enter a valid PIN on the smartcard reader. This unlocks a private key stored on the smartcard. This key is used to sign an authentication challenge sent by the bank. The signing process is done by the smartcard itself. The authentication challenge is randomly generated and only valid for a given time frame.

In this scenario, the PIN cannot be eavesdropped because it is entered on an uncompromised and secure device, the smartcard reader. The smartcard reader cannot be infected by a trojan such as Zitmo because it usually does not support installation of any additional software. The signed authentication challenge cannot be replayed because it is valid only for a short time frame. The cybercriminals

²The *Android Market* has been known to distribute several pieces of spyware, which occasionally have been pulled out. The *Apple Store* has had fewer security issues so far, but it is often seen as so closed that it basically encourages end-users to jailbreak their devices and then download totally uncontrolled software.

cannot initiate the authentication because they need the victim to enter his PIN on the smartcard reader. The only vulnerability we foresee is race attacks, where the signed authentication challenge could be intercepted by the cybercriminals and sent to the bank by them before the victim. This protocol can probably be improved.

In the future, mobile phones could act as smartcard readers as long as their SIMs have the capability to store a keypair and the phone features a secure keyboard.

3. CONCLUSION

In this two-part series, we have shown how cybercriminals related to the Zeus gang have stolen online banking credentials, even in cases where the bank sends an mTAN to the end-user's mobile phone.

We have provided an in-depth analysis of the malicious mobile component, Zitmo, which infects *Symbian* mobile phones. We have explained how the trojan intercepts all incoming SMS messages. Using a disassembler tool with a *Symbian* remote debugger and configuring a sane phone to act as the attacker, we have stepped through Zitmo's malicious code and revealed the entire process of SMS interception and handling. This technique even succeeded in helping us display a debug window the malware authors had hidden.

We have also covered how the cybercriminals probably wrote Zitmo. During our research, we noticed a very similar piece of spyware and found that Zitmo was closely related to it, with a high percentage of identical routines and strings. So, the motivation, implementation and inspiration of Zitmo have all been explained. On a technical note, Zitmo's reverse engineering is fully completed. Future work should probably keep an eye on SpyEye, which is seen as a rising successor to Zeus. Some other aspects would also be worth investigating more closely, such as countermeasures or cybercriminality.

Research into countermeasures would mean testing solutions based on malicious behaviour detection, firewalling or anti-virus capabilities in real-life environments. Research could also be conducted on reviewing challenge-based authentication protocols and proving them formally against Zeus/Zitmo attacks. As for cybercriminality, several points are still unknown (or undisclosed), such as how many online bank accounts were stolen, how much the cybercriminals traded the accounts for, and to whom, and of course, the identity of the gang.

ACKNOWLEDGEMENTS

We thank Guillaume Lovet (*Fortinet*) for his technical and in-depth review, and Ludovic Apvrille (*Telecom*

ParisTech) for useful comments on the article structure. Finally, we thank David Barroso (*s21sec*) for kindly sharing information regarding Zeus and Zitmo.

REFERENCES

- [1] Apvrille, A.; Yang, K. Defeating mTANs for profit – part one. *Virus Bulletin*, March 2011, p.6. <http://www.virusbtn.com/pdf/magazine/2011/201103.pdf>.
- [2] Payu, S. Silent Receiving of SMS Messages. October 2008. http://symbian.devtricks.mobi/tricks/silent_receiving_of_sms_messages/.
- [3] Barroso, D. Zeus Mitmo: Man-in-the-mobile. September 2010. <http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>.
- [4] Tarasov, D. SMS Monitor User Manual. http://dtarasov.ru/smsmonitor_manual_en.html.
- [5] Apvrille, A. Zitmo Follow Up: From Spyware to Malware. September 2010. <http://blog.fortinet.com/zitmofollow-up-from-spyware-to-malware/>.
- [6] Campbell, I. *Symbian OS Communications Programming*. Symbian Press. John Wiley & Sons Ltd, 2nd edition, 2007.
- [7] BiNPDA. SecMan Security Manager v1.1, 2008. <http://free-mobilesoftware.mobilclub.org/software/QuickHackKit.php>.
- [8] Tarasov, D. Evil-coding Symbian. *xakep magazine*, 3, 2009. <http://www.xakep.ru/magazine/xa/123/096/1.asp> (in Russian).
- [9] Bose, A.; Hu, X.; Shin, K. G.; Park, T. Behavioral Detection of Malware on Mobile Handsets. 6th International Conference on Mobile Systems, Applications, and Services (MobiSys'08). June 2008.
- [10] Xie, L.; Zhang, X.; Seifert, J.-P.; Zhu, S. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices. 3rd ACM Conference on Wireless Network Security (WiSec'10). March 2010.
- [11] Yan, G.; Eidenbenz, S.; Galli, E. SMS-watchdog: Profiling social behaviors of SMS users for anomaly detection. RAID, volume 5758 of Lecture Notes in Computer Science, pp.202–223, 2009.
- [12] Enck, W.; Ongtang, M.; McDaniel, P. On Lightweight Mobile Phone Application Certification. 16th ACM Conference on Computer and Communications Security (CCS'09). November 2009.

TECHNICAL FEATURE 2

HIDING IN PLAIN SIGHT

Raul Alvarez
Fortinet, Canada

Malware uses various different encryption techniques, compression algorithms and stealth technologies to avoid detection by anti-virus scanners. Stealth technologies like rootkits are often used to hide malicious components from anti-virus scanners.

In this article we will look at another, lesser known, stealth technology. The alternate data stream (ADS) is an old *Windows* trick that can easily be exploited by malware authors to hide their files.

In this article, we will look at the early use of ADS in a proof-of-concept virus (StreamC), at how a folder can be infected (Rustock), and at ADS in use in the wild today (Joleee). We will also discuss the future of ADS in malware.

PART I: STREAM OF CONCEPT

Windows introduced ADS with the inception of NTFS in *Windows NT*. The NTFS file system is capable of supporting multiple streams of data: one file that is visible to the user, and several other files behind it. But one of the drawbacks is that we can't transfer such a file to a non-NTFS storage device (such as a USB flash drive) unless it is formatted as NTFS; attempting to move a file containing ADS to non-NTFS storage will result in only the primary file being copied, and the ADS will vanish into thin air.

The concept

Around the year 2000, a proof-of-concept virus – let's call it StreamC – was created with ADS, and at that time it only infected files in *Windows 2000*. It was evident from the early call to the `GetVersion` API, and a check on the AL register of whether the value is equal to 5, that the author's original intention was to infect files in *Windows 2000*.

Now, however, *Windows XP*, *Windows XP 64-Bit Edition*, *Windows Server 2003* and *Windows Server 2003 R2* can also be infected, since their version number also starts with 5.

Infection routine

Once it has ascertained that the OS can be infected, StreamC uses the `FindFirstFileA` and `FindNextFileA` APIs to search in the current directory for executable files (*.exe) to infect.

If, for instance, `calc.exe` is found, StreamC checks if the file is compressed by checking its attributes for the value `0x800`

(`FILE_ATTRIBUTE_COMPRESSED`). The malware will skip further processing of `calc.exe` if it is compressed, but otherwise it will proceed to compress the file using NTFS file compression via a call to the `DeviceIoControl` API. Using the `FSCTL_SET_COMPRESSION(0x9C040)` `IoControlCode` and `COMPRESSION_FORMAT_DEFAULT` value, `calc.exe` is compressed in a default NTFS compression format. Afterwards, `calc.exe` is copied to a temporary file.

While `calc.exe` is stored away securely in a temporary file, StreamC creates a copy of itself using the filename '`calc.exe`'. Afterwards, the temporary file is placed into the malware's memory space and copied as ADS – the `calc.exe:STR` stream contains the original contents of `calc.exe`.

Note that the ADS naming convention always uses a colon (:) to separate the names of the primary file and the alternate data stream:

<primary file name>:<alternate data stream name>

For example, `calc.exe:STR`.

Only two APIs are needed to create an alternate data stream: `CreateFileA` and `WriteFile`. After infecting all .exe files in the current folder, StreamC will display a message box (see Figure 1).



Figure 1: Message box displayed by StreamC.

Proof of companionship

StreamC can be categorized as a companion virus; in the old DOS days, companion viruses created a copy of the malware using a similar name to the existing executable file. For example, `calc.com` would be created as a companion virus for `calc.exe`, since .com files are executed before .exe files in the DOS environment. This is done simply by making a copy of the virus with a .com extension.

But StreamC does not create a .com version of itself; instead, it uses ADS technology to hide the original .exe file – StreamC is disguised as the original legitimate application.

Executing the original calc.exe

When an infected calc.exe is executed, StreamC’s infection routine is performed first, after which the original executable file will be run as a process. This is done by using, for example, calc.exe:STR as the ApplicationName of the CreateProcessA API.

```
CALL DWORD PTR SS:[EBP+8BB] kernel32.OpenEventA
TEST EAX,EAX
JNZ 1.00401DD9
LEA ESI,DWORD PTR SS:[EBP+57C] ASCII "{DC5E72A0-6D41-47e4-C56D-024587F4523B}"
PUSH ESI
CALL DWORD PTR SS:[EBP+8FF] kernel32.GlobalFindAtomA
TEST AX,AX
JNZ 1.00401DD9
PUSH ESI
CALL DWORD PTR SS:[EBP+8FB] kernel32.GlobalAddAtomA
```

Figure 2: Strings used by Rustock for infection checking.

PART II: HIDING THE HIDDEN

A variant of Rustock attempts to use a combination of a rootkit and ADS in an attempt to hide its code.

ADS in a folder

Given a file to infect, StreamC has shown us how simple it is to create an alternate data stream. A walk through Rustock’s code will explain how to create an ADS in a folder.

```
8D85 F5050000 LEA EAX,DWORD PTR SS:[EBP+5F5]
50 PUSH EAX ASCII ":lzx32.sys"
57 PUSH EDI ASCII "C:\WINDOWS\system32"
FF95 97080000 CALL DWORD PTR SS:[EBP+897] kernel32.lstrcata
89FE MOV ESI,EDI
6A 00 PUSH 0
57 PUSH EDI ASCII "C:\WINDOWS\system32;lzx32.sys"
FF95 C3080000 CALL DWORD PTR SS:[EBP+8C3] kernel32._lcreat
5B POP EBX
83F8 FF CMP EAX,-1
75 1A JNZ SHORT 1.00401CA2
C603 00 MOV BYTE PTR DS:[EBX],0
8D85 00060000 LEA EAX,DWORD PTR SS:[EBP+600]
50 PUSH EAX
57 PUSH EDI
FF95 97080000 CALL DWORD PTR SS:[EBP+897]
6A 00 PUSH 0
57 PUSH EDI
FF95 C3080000 CALL DWORD PTR SS:[EBP+8C3]
83F8 FF CMP EAX,-1
0F84 2E010000 JE 1.00401DD9
89C7 MOV EDI,EAX
8D85 03090000 LEA EAX,DWORD PTR SS:[EBP+903]
68 660A0100 PUSH 10A66
50 PUSH EAX
57 PUSH EDI
FF95 C7080000 CALL DWORD PTR SS:[EBP+8C7] kernel32._lwrite
57 PUSH EDI
FF95 A7080000 CALL DWORD PTR SS:[EBP+8A7] kernel32._lclose
```

Figure 3: Creating an ADS in a %system32% folder.

After a series of decryption routines, Rustock checks if the operating system is NT by looking at its version number – the same check as performed by StreamC. Then, Rustock checks for an event synchronization object, to avoid re-infection. If the event {DC5E72A0-6D41-47e4-C56D-024587F4523B} is not found, it proceeds to check for the existence of an atom¹ with the same event string name, otherwise, it creates one using the GlobalFindAtomA and GlobalAddAtomA APIs (see Figure 2).

Address	Value	ASCI	Comment
0006FD88	00401D0A	. @.	CALL to CreateServiceA from 1.00401D04
0006FD8C	00083E90	h .	hManager = 00083E90
0006FD90	0040213C	< @.	ServiceName = "pe386"
0006FD94	00402142	B @.	DisplayName = "Win23 lzx files loader"
0006FD98	00000010	...	DesiredAccess = SERVICE_START
0006FD9C	00000001	...	ServiceType = SERVICE_KERNEL_DRIVER
0006FDA0	00000001	...	StartType = SERVICE_SYSTEM_START
0006FDA4	00000000	ErrorControl = SERVICE_ERROR_IGNORE
0006FDA8	0006FEC0	âp .	BinaryPathName = "C:\WINDOWS\system32;lzx32.sys"
0006FDAC	00402159	Y @.	LoadOrderGroup = "Base"
0006FDB0	00000000	pTagId = NULL
0006FDB4	00000000	pDependencies = NULL
0006FDB8	00000000	ServiceStartName = NULL
0006FDBC	00000000	Password = NULL

Figure 4: CreateServiceA call for the rootkit functionality.

To create an ADS in a folder, Rustock uses the GetSystemDirectoryA API to generate the system folder’s path. ‘:lzx32.sys’ is now added to the folder’s name, followed by a call to the _lcreat API – to create, for example, ‘c:\windows\system32;lzx32.sys’ – and a call to the _lwrite API to write the malware code to the stream (see Figure 3).

In its simplicity, Rustock uses _lcreat and _lwrite to make a stream in a folder, but hiding using ADS is not enough. Rustock knows that it can easily be detected; hiding the code deeper using a rootkit is the next feasible step. By calling the OpenSCManagerA API, Rustock is now ready to launch its code as a service; a call to the CreateServiceA

API with SERVICE_KERNEL_DRIVER(0x00000001) ServiceType parameter ‘c:\windows\system32;lzx32.sys’ is now launched as a device driver (see Figure 4). Finally, a call to StartServiceA activates the driver.

The main rootkit functionality is to hide ‘c:\windows\system32;lzx32.sys’. By launching ‘lzx32.sys’ as a service, Rustock secures a dual layer of stealth technology for its code; an ADS and a rootkit, not to mention it is a stream in a folder.

¹ An atom is a 16-bit integer used to access the string in the atom table, a list of global strings.

PART III: A JOLEEE GOOD FELLOW

Is ADS still used by malware today? Yes, a prevalent worm known as Joleee is still in the wild at the time of writing; a recent variant of Joleee shows signs of ADS usage. We will explore how this malware survives in the wild and how it uses an old-style hiding capability.

Simply ADS

Joleee uses a Bredolab-style anti-debugging trick and employs an encryption algorithm to hide its API names. After decrypting and resolving the first batch of APIs, Joleee sets up some registry settings and then proceeds to create an ADS version of itself.

To create the ADS, StreamC and Rustock simply used a string for the filename, but for Joleee there is a considerable amount of preparation just to produce the filename itself.

First, it gets the path for the Windows directory using the GetWindowsDirectoryA API and stores the path, character by character, in its memory space. Next, it adds the string 'explorer.exe' manually, four characters at a time, followed by the strings ':userini' and '.exe'. By allocating a total of 631 bytes of code, Joleee generates the ADS name 'C:\windows\explorer.exe:userini.exe' and creates it using the CreateFileA API (see Figure 5).

After successfully creating 'C:\windows\explorer.exe:userini.exe', Joleee copies the content of the encrypted version of itself to its memory space – using the VirtualAlloc and ReadFile APIs – and writes the malcode to the newly opened ADS file using WriteFile.

Once the ADS version of Joleee is attached to explorer.exe, the malware continues with the rest of its malicious actions: it drops a copy of its encrypted version in the %system% folder and will attempt to delete itself from the current directory. It then proceeds to create a series of threads: for creating registry start-ups (see Figure 6), for downloading files, and for accessing SMTP domains.

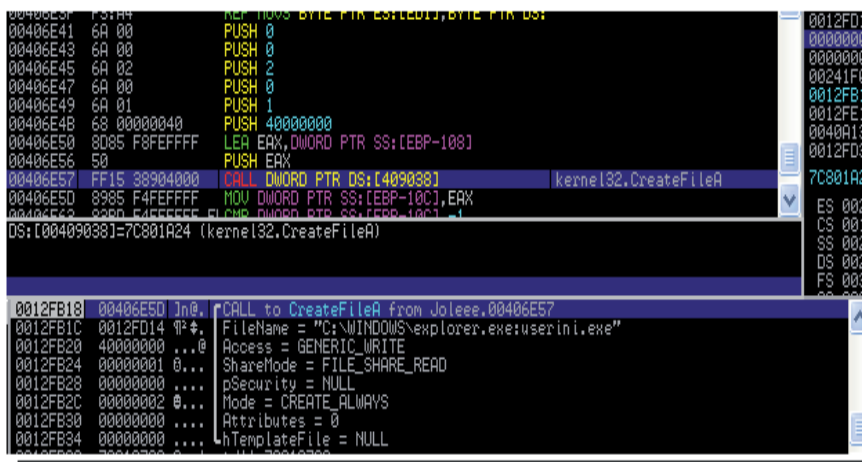


Figure 5: The call to the CreateFileA API to create 'C:\windows\explorer.exe:userini.exe'.

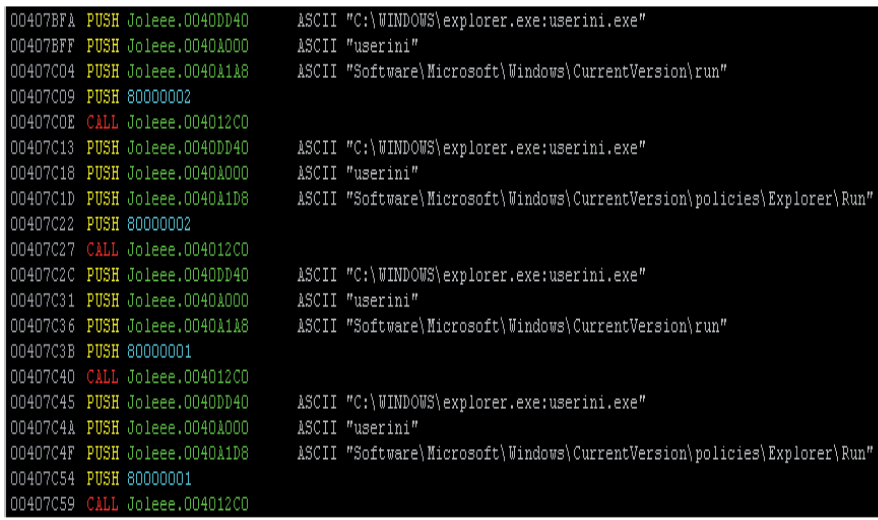


Figure 6: Some registry start-ups added by Joleee.

Survival in the wild

With a combination of spamming, decryption, anti-debugging tricks, and a touch of ADS, Joleee has all the ingredients needed to survive in the wild for long enough to add more tricks in future releases.

PART IV: FUTURE OF ADS MALWARE

You might think that ADS is an old technology and therefore not really a threat. Think again. We haven't seen the end of exploits using alternate data streams.

The following are some common examples of ADS in everyday computing that we might not be aware of:

- `:Zone.Identifier`. This is a stream generated by *Internet Explorer* and *Outlook* when saving files to the local disk from different security zones. In other words, whenever we download a file from the Internet, the `Zone.Identifier` ADS is added to the file.

Format: `<downloaded filename>:Zone.Identifier`

The usual content is:

```
[ZoneTransfer]
```

```
ZoneId=3
```

- `:encryptable`. This is an ADS attached to the `Thumbs.db` file, created when the Thumbnails view is selected in *Windows Explorer*. The file size is usually 0 (if it is not 0 this may be a sign that it has some malicious content).

Format: `Thumbs.db:encryptable`

- `:favicon`. Whenever you add a link to your 'Favorites' in *Internet Explorer* and the website has an icon, the icon will be saved as `:favicon`.

Format: `<linkname>.ulr:favicon`

`:Zone.Identifier`, `:encryptable` and `:favicon` are normal alternate data streams that reside on our computers. We don't usually notice their existence because they are harmless and mostly used simply to identify the base file to which they are attached. But, like any other files, it is possible for them to contain malicious code, dangerous URLs, encrypted commands, or updates for existing malware.

CONCLUSION

ADS may be an old trick, easy to use, and easy to detect, but it will remain in existence for a long while and it will only be a matter of time before malware writers start to use ADS in new malicious ways; we must remain vigilant. A great way to start looking for ADS in your computer is to use the *Streams* tool from the *Microsoft SysInternals* site [1]. Happy hunting!

REFERENCES

- [1] Streams. <http://technet.microsoft.com/en-us/sysinternals/bb897440>.
- [2] File Streams. [http://msdn.microsoft.com/en-us/library/aa364404\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364404(v=vs.85).aspx).

CONFERENCE REPORT 1

FIGHTING CYBERCRIME TOGETHER

Martijn Grooten

The first annual eCrime Researchers Sync-Up, organized by the Anti-Phishing Working Group (APWG) in conjunction with University College Dublin's Centre for Cybercrime Investigation, was described as 'a two-day exchange of presentations and discussions related to eCrime research in progress – and for networking of researchers within the disciplines that are defining the eCrime research field today'. However, when I first looked at the programme for the Sync-Up, I have to admit to thinking that it might be too much of an academic event.

I wasn't worried about my own presentation (on evaluating spam filters) not being academic enough – in fact, having spent some time in academia, I thought this would be a good opportunity to dust off my mathematical notations to make simple things look a little more complicated. Rather, cybercrime is a very serious issue and I didn't believe it would benefit greatly from being discussed on a purely academic level.

However, I needn't have been concerned – not only were the participating academics involved up to their elbows in the task of fighting online threats on a daily basis, but participants came from all areas of the field: from those dealing with user education, via those whose job it is to protect the users, to those involved in hunting down the cybercriminals and bringing them to justice. There were also representatives of perhaps the most prominent victims of online crime: financial institutions. In fact, many of the participants wore multiple hats.

NAMING AND MEASURING

The benefit of having such a broad range of participants became obvious during a discussion of the naming of malware families and botnets. When it was suggested that this was an exercise of little relevance in today's world of fast-changing threats (the naming practice dating from an era when just a handful of new samples were seen every day), a delegate who worked with law enforcement agencies stood up and said that, for them, naming and labelling is extremely important: these agencies frequently have to decide which are the most relevant threats and where they should dedicate their limited time and resources: Stuxnet, Rustock, Zeus or perhaps a gang of eBay fraudsters?

Having a good idea of which are the biggest threats, and which are linked, is essential for making such decisions. It

is thus important to have a good idea of the size of threats, from spam to botnets, and to represent these correctly. Presentations by *Trend Micro's* David Perry, APWG's Pat Cain and Randy Vaughn of Baylor University dealt with some aspects of the far from trivial task of threat measurement.

Indeed, a lack of resources is a constant struggle for those working in law enforcement and the current economic downturn and subsequent public sector cuts have not made things any easier. But, rather than bemoan the difficult nature of their jobs under such circumstances, participants discussed ways in which they could use resources more effectively and ways to convince both governments and the general public about the severity of these online threats.

The fact that online crime is a serious problem was demonstrated by data showing that, in the US, the amount of money lost per year through online crime is significantly greater than the amount lost through bank robberies. If nothing else, the data reinforced the idea that collaboration is needed to drive forward the fight against cybercrime – and a proposal to set up an 'eCrime Collaborative Research Center' was examined in a roundtable discussion.

PATCHER

For those, like me, who do not dissect malware and botnets on a daily basis, a presentation on the Patcher rootkit was particularly interesting. It certainly showed that phishing has evolved a great deal since the days when websites only vaguely resembled those of banks and victims were expected to fill in their credit card details, their social security number and their *PayPal* password.

Patcher 'patches' a number of *Windows* files in a near-undetectable way so that traffic between the user and their bank is intercepted and modified. Not only does the malware steal money from the user's account, it also hides these transactions and modifies the account balance whenever the user visits the bank's website.

TOOLS AND TECHNIQUES

With researchers digging so deep into the crooks' systems, it is easy to lose sight of the ethical principles guiding IT research, and this topic was addressed in a presentation by Erin Kenneally of *eLCHEMY Inc.*

But fighting cybercrime is not just about fighting specific gangs or detecting specific pieces of malware. Just as important in the fight against crime and the protection of users, is to detect and block the tools used by the crooks.

One example of such a tool is fast-flux DNS, where malicious domains point to constantly changing IP addresses to prevent detection and make the corresponding websites less vulnerable to actions against the hosts. Marc Vilanova, of *la Caixa*, described a method to track such networks, while other presentations dealt with IP reputation using network topology estimation and botnet detection and remediation.

Phishing is traditionally seen as a threat involving email and websites, and these subjects were discussed as well. A presentation by Richard Urbanski of *AIB* dealt with avoiding automated detection by using 'homoglyphs' (for instance by substituting the Cyrillic 'a' for the Latin 'a'), while Brendan Bowles, of University College Dublin, discussed language models to detect phishing.

EDUCATION

As demonstrated by recent examples of previously silenced botnets being resurrected, and disconnected spammers continuing to ply their trade, the only effective way to stop cybercriminals is to find them, arrest them and bring them to court. This is something that requires more than simple cooperation between researchers, industry experts and law enforcement agencies; it also requires significant technical knowledge among the latter group.

I was therefore particularly interested to learn that a number of universities – University College Dublin, host of the event, among them – have set up courses on cybercrime specifically for law enforcement. These courses are essential, not just to educate a new generation of police officers, but also to educate existing officers, for whom dealing with cybercrime has become an increasingly prominent part of their work, yet who often lack the knowledge required to deal with it.

CONCLUSION

There are many events dealing with the fight against cybercrime; indeed, in the same week as the APWG Sync-Up another anti-cybercrime event took place in London. It is important that these events are organized and that experts get plenty of opportunities to meet.

For an event to be successful, it is important not just for the talks to be of good quality, but also for there to be ample time for discussion. At the APWG Sync-Up there were plenty such opportunities for discussion, and I left Dublin not just with the pleasing feeling of having met many friendly and like-minded people, but also with fresh inspiration to continue my daily job.

CONFERENCE REPORT 2

RSA 2011 CONFERENCE REVIEW

Jeannette Jarvis

Independent researcher, USA

The 20th annual RSA Conference was held at the San Francisco Moscone Center in February.

The RSA conference began exclusively as a cryptography conference, taking its name from the three founders of the RSA algorithm: Ron Rivest, Adi Shamir and Leonard



Adleman. The theme of RSA 2011 was 'The Adventures of Alice & Bob'. Rivest first used these fictitious characters in 1978 to help explain the complex process of encryption. Later, Bruce Schneier – another institution in the cryptography world – added further characters, such as Mallory the Malicious Attacker and Eve the Eavesdropper, to help less technical professionals get a grasp of this deeply technical topic. Cartoons depicting these characters were played for entertainment throughout the conference week.

While the theme of the conference always reflects the world of cryptography, the event itself has evolved into a very comprehensive forum discussing the latest in security technologies, research, forensics, policies and regulations, trends, best practices, business concerns, and much more.

RSA generally attracts more than 12,000 attendees from around the world – delegates can choose between 14 presentation tracks, with over 250 speakers throughout the week. In keeping with the times, 'Cloud Security' was a new track added this year.

An exhibition runs alongside the conference, with over 330 exhibitors representing software, hardware, consulting, government and non-profit organizations.

The event also offers several keynote talks (17 this year) – many of which are given by representatives of the companies sponsoring the event.

THE KEYNOTES

In a talk entitled 'Collective Defense: Collaborating to Create a Safer Internet', *Microsoft's* Trustworthy Computing Corporate Vice President, Scott Charney, suggested that we apply public health models to the Internet. The worldwide health community has a solid programme in place for educating about health risks, coordinating efforts to detect diseases and vaccinations to

prevent diseases, and an international structure to respond when outbreaks occur. The application of such a model to Internet health would have enormous benefits, but would require sustained local and international collaboration.

Charney also focused on identity management. A shared and integrated domain creates huge problems when people and their activities are mingled. Anything we've ever done on the Internet is recordable and findable. Identity management is critical. We must build trusted stacks with strong identity management systems. As the threat world evolves, *Microsoft* continues to revise its Security Development Lifecycle (SDL).

RSA would not have been complete without hearing more about Stuxnet. And who better to offer that information than *Symantec's* President and CEO, Enrique Salem.

Symantec played a crucial role in the identification and analysis of Stuxnet. The worm exploited four zero-day vulnerabilities, and *Symantec* helped uncover three of them. The threat has moved the game from espionage to sabotage and used the first rule of the art of war: deception. Salem noted that we've been expecting this sort of sophisticated, elaborate attack for many years. Now it is here and it is more sophisticated, dangerous and prevalent than anything we have seen before.

While SCADA attacks are not new, they are a threat to our economy, prosperity and our lives. We now know what is possible. More targeted attacks are coming, with the most dangerous ones targeting critical infrastructure. Salem noted that every day there are over two million different attacks and it takes skill to figure out which are real threats and which can safely be afforded less attention.

Dr Michio Kaku provided delegates with an enlightening presentation on the future of computers. Some of the advancements he predicts are cars driving themselves, and a home office in your glasses (or contact lenses) – blink and you go online!

Dr Kaku predicts that in 10 years' time we will be able to identify people's faces, know their biographies and translate their languages, all with a pair of smart glasses. According to Kaku, our clothing will contain all our medical records and particles in our homes will be able to diagnose health issues. Ultimately, he indicated, the augmented reality we see in movies like *The Terminator* will be in our own reality very soon.

With the amount of personal information being added to the Internet there will be more headaches for those working in security. (And can you imagine the opportunity for exploits?) Kaku also believes that Silicon Valley will become a rust belt by 2020 due to overheating and quantum leakage – the two problems facing Moore's Law today.

‘Moore’s law will flatten out until physics can create quantum computers.’

Another popular keynote was ‘The Murder Room: Breaking the Coldest Cases’, presented by Michael Capuzzo, author of the book *The Murder Room*. Capuzzo discussed the crime-fighting Vidocq Society, along with two of its members: Bill Fleisher, a private investigator and former FBI agent, and Richard Walter, a forensic psychologist, who many consider to be the living Sherlock Holmes.

The Vidocq Society consists of forensic investigators, prosecutors, medical examiners, police officers, attorneys, and the world’s most successful detectives whose sole purpose is to solve cold-case murders. They are experts at decrypting crime scenes and mining data. These retired professionals use the skills they gained throughout their careers for the greater good. All their work is pro-bono with the belief that ‘virtue is its own reward’.

The Society’s success is due to having founded a network of the best of the best in criminal investigations. These are brilliant people who study invisible links, put puzzles together, keep track of what could seem like meaningless files, look for patterns, and think about the psychology of what motivates criminals. Their work closely maps to the anti-malware industry’s search for the bad guys on the Internet. Parallels exist in how the bad guys hide, their motives, and how they try to conceal their guilt. In fact, the Vidocq Society has been enlisted to create a system that uses the same subtypes employed in murder investigations to evaluate Internet stalking and other cybercrimes. They’ve been able to determine that, within 3.8 years, a fantasy-driven stalker will move from stalking on the Internet to attempting to kill the victim. As the Vidocq Society transfers its expertise to the cyber world, we should expect to hear more from them.

A panel entitled ‘Cyberwar, Cybersecurity, and the Challenges Ahead’ was led by James Lewis of the Center for Strategic and International Studies, with panel members: Michael Chertoff, Former United States Secretary of Homeland Security; Mike McConnell, *Booz Allen Hamilton*; and Bruce Schneier, *BT*.

The panel was asked why there is so much attention on cyber war. Schneier indicated that categorizing something as a



‘war’ is sexier than categorizing it as a cyber attack – it’s what sells and allows for bigger budgets. Overstating the threat is a good way to get people scared. These are big terms, and useful if you want to set up a cyber command. The panel’s consensus was that we are not engaged in cyber war – at risk of it, yes, but the situation now, while uncomfortable and dangerous, is not war.

The Russian denial of service attack against Georgia was brought up as an example of where we have observed an aspect of cyber war. Terrorists could be sophisticated enough to destroy major systems – when we are facing an attack, or one is under way, what can our governments do? We must create policies and procedures in advance.

With the entire globe riding on the same internet infrastructure we need to have better layers of defence. It was unanimously agreed that the solution was not a technology fix, but a framework model. Better legal and international policy is required, with a framework of rules, norms and laws.

We need more discussion, agreement, and treaties between nations. More countries need to talk with and trust each other so we can better deal with the cyber concerns together.

Arguably the most popular keynote was given by the former United States President, and founder of the William J. Clinton Foundation, Bill Clinton.

President Clinton is a very passionate speaker who talked about the challenges surrounding globalization and our interdependence on programs that do not focus on our core values. He spoke about the need to save our resources and focus on green technology to lessen our dependence on foreign oil.

Clinton said: ‘Throughout history, everything that has value is subject to being stolen or altered. Everyone in cyber security is like a modern day cop on a beat. You are dealing with human nature and an inevitable tendency to try to take advantage of whatever the latest object of value is.’

He also focused on the need to ensure that, as we invent new technologies, we have government policies in place and do our best to not repeat mistakes of the past.

INNOVATION SANDBOX

The ‘Innovation Sandbox’ is a forum in which new companies showcase their technologies and compete for the



title of ‘Most Innovative Company’. *Invincea* took home the 2011 title for its fully virtualized browser and PDF reader that seamlessly runs a virtual environment separately from the desktop operating system. This protects users against web-borne and PDF-embedded threats.

HIGHLIGHTS FROM THE TRACK SESSIONS

With so many talks to choose from, I decided to attend as many anti-malware industry presentations as I could.

Under ‘Hot Topics’ I found a panel entitled ‘The Digital Apocalypse: Fact or Fiction?’, which was moderated by John Pescatore of *Gartner*, with panellists: Dmitri Alperovitch, *McAfee*; Bob Dix, *Juniper Networks*; Mike Echols, *Salt River Project*; and Justin Peavey, *Omegeo*.

Key takeaways were that targeted attacks are politically motivated and are not sophisticated. Attacks are focused on integrity and availability, not on confidentiality, with the integrity attacks the most concerning. ‘An APT attacker wants you like a dog with a bone. It doesn’t matter how long it takes, they will keep trying.’

Another panel also proved interesting: ‘Breaking News! Up to the Minute Hacking Threats’ was moderated by investigative journalist Brian Krebs, with panellists: Eric Chien, *Symantec*; Wade Baker, *Verizon Business*; and Jeremiah Grossman, *WhiteHat Security*.

Grossman predicated that in 2012 every website will be vulnerable. *Verizon* has noted an upswing in customized malware and that organizations are simply not patching. Add that to the rise in zero-day threats and it is not a pretty picture. Today there is more visibility of new vulnerabilities, which helps to get the problems fixed sooner – software companies are generally providing fixes for vulnerabilities faster – but end-users are not installing them in a timely manner.

Krebs indicated that he is underwhelmed by mobile threats. New malware for *Android* is being seen at a rate of about one per week, but he predicted that *Windows Phone 7* will become a bigger target. Further discussion centred on browser security, with panellists asserting that if the browser is not secure, the web is not secure – and that innovation must focus on increasing browser security.

Kaspersky’s Roel Schouwenberg presented a paper entitled ‘Adobe – Evaluating the World’s Number One Most Exploited Software’. He reported that in 2010 Q1, 48% of exploits used PDFs. Although the number of exploits using PDFs decreased throughout the rest of 2010, *Adobe*’s model to protect against persistent threats is not good enough. *Adobe* needs to force updates by changing to an auto-update model similar to that of *Google Chrome* where

it is not possible to opt out. Schouwenberg applauded *Microsoft* as a ‘thought leader’. As the company has become more security-focused and its products more locked down, the bad guys have looked for other opportunities. Schouwenberg predicts that 2011 will be the year of Java – which has a big market and therefore will continue to be a big target.

‘The X Factor – Moving Threat Protection from Content to Context’ was a discussion moderated by Ambika Gadre of *Cisco Systems*, with panel members Mary Landesman, *Cisco Systems*, and Patrick Peterson, *Authentication Metrics* and *Cisco Systems*.

Spam volumes dropped dramatically in 2010 due to concerted botnet takedown efforts throughout the year. However, spam volume does not equate to risk level. A decrease in spam does not mean there is less risk of malicious email. (It doesn’t mean there is more risk either – risk stays about the same.) For example, December 2010 was the lowest point in terms of spam volume, yet a very successful attack was carried out against .gov and .mil workers via an email disguised as a greeting card from the White House. The email contained a link to view the greeting card, which actually led to a variant of the Zeus trojan. This particular variant harvested .PDF, .DOC and .XLS files from victim computers. In the short time the attack was live, attackers managed to accrue a few gigabytes’ worth of stolen data.

Over the last ten years, malware has evolved from being prank-driven to being profit-motivated. In the next ten years, we are likely to see more malware used as a sabotage tool for political and global economic gain.

We cannot afford to approach the problem passively. An active approach is required by all, including deep analysis of system logs and having the expertise to spot suspicious behaviour and deal with it appropriately.

The bad guys are looking for interesting people and have the ability to customize their attacks accordingly. End-users should understand how to recognize and report suspicious behaviour, whether encountered via email or on the web. Administrators should ensure they are providing active forensic analysis of their systems and that there are processes in place that empower security teams to take appropriate and timely action.

The ‘Advanced Persistent Threats: War Stories from the Front Lines’ panel was moderated by *McAfee*’s Dmitri Alperovitch, with panel members: Heather Adkins, *Google*; George Kurtz, *McAfee*; Kevin Mandia, *MANDIANT*; and Adam Meyers, *SRA International*.

The threats we see today are not always advanced, but they are persistent. Mandia commented that simply labelling

an attack 'APT' seems to get security professionals off the hook for not stopping it pre-attack. He also indicated that law firms and healthcare organizations appear to be the sectors that are least well prepared for these targeted attacks. Kurtz asserted that all major organizations currently have a hacker on their network and that it isn't hard to get past layer 8 (humans).

The panel recommended that IT officers create a social footprint of their executives and see who is trying to profile them and accessing their information. Who is pulling down their bios? Their whitepapers? This will provide an indication of who is being targeted, as well as who is doing the attacking. It is about behaviour detection – not just malware detection. Mandia commented that hackers are not targeting operating systems, but people. These people just happen to be using *Windows*.

Companies need to implement DHCP, DNS and web access logging. Whole packet capture is not always optimal, but logging and analysis of activity – both coming and going – must be provided. User involvement and user education is also critical.

Mikko Hyppönen, *F-Secure's* Chief Research Officer, presented a compelling talk, the highlight of which was the world premiere of a video documenting Mikko's recent trip to Pakistan to meet the authors of Brain, the first PC virus, on the 25th anniversary of its release. The authors of the virus, brothers Basit and Amjad Alvi, had posted their names and address within the code, and Mikko found that they were still operating a (legitimate) business from the same address today.

Brain was not intended to destroy data, and the brothers said that they regret seeing the destructive behaviour of today's malware. However, they said they believe that someone else would have written the first virus, had it not been them.

CONCLUDING REMARKS

I could go on describing more presentations and keynotes but there simply isn't enough room for all the content.

RSA is by far the best networking event across the security industry. Its attendees are a veritable *Who's Who* in the worldwide security community. You'll find everything from pre-conference training, deep technical content, peer-to-peer sessions and alliance summits, to working group meetings, professional development seminars, executive forums, and so much more. There is something here for everyone, including far too many social events that will have you hopping from one event to another every night. This is truly a conference not to be missed.

'Securing your Organization in the Age of Cybercrime'

A one-day seminar in association with the MCT Faculty of The Open University

- Are your systems *SECURE*?
- Is your organization's data at *RISK*?
- Are your users your greatest *THREAT*?
- What's the real *DANGER*?

Learn from top IT security experts about the latest threats, strategies and solutions for protecting your organization's data.

Book your place today to make sure your business is protected:

www.virusbtn.com/seminar
or call 01235 555139



SEMINAR
24 May 2011
Milton Keynes, UK



The Open
University

FEATURE

SENDER AUTHENTICATION – PRACTICAL IMPLEMENTATIONS

Terry Zink
Microsoft, USA

In my six-part series on sender authentication [1–6], I wrote about a number of topics: how SMTP works, email headers, SPF, SenderID and DKIM.

I mainly wrote about the theoretical constructions of the system and illustrated some considerations for mail receivers when they implement the technologies. But what about some practical realities? How well do these technologies work in real life? Can we use them to solve actual problems? The answer is yes, and that is the subject of this article.

THE REAL-LIFE WEAKNESSES OF SPF AND SENDERID

SPF and SenderID are two technologies that are very similar and accomplish similar things, but each has its weaknesses and strengths. Table 1 shows a comparison between the two technologies.

The weaknesses of SPF became apparent to me several years ago. The year was 2007. The mortgage financial crisis was still ahead of us, Rudy Giuliani and Hillary Clinton were their party front runners for the presidential nominations, and I was still a fledgling spam analyst. The years 2006 and 2007 were quite turbulent in the spam world. In 2006 we saw a major influx of image-only spam, and spam filters were caught scrambling to react to it because it was very effective in evading content filtering. This was also the time that botnets really hit their stride and we saw massive increases in the volume of spam hitting our inbound servers. Finally, in the summer of 2007, spam with PDF attachments was just emerging. It was short-lived, but it was still a new and creative spam technique that hadn't been seen previously.

I wasn't nearly as familiar with SPF at that time as I am now. I had only recently become a Program Manager at *Microsoft* and this meant that I would be exposed to an increasing number of customer escalations. This also meant that anything I couldn't speak confidently about would come back to haunt me.

In mid-2007, I was looped into an escalation for a new customer who was receiving a lot of phishing messages in which the attacker was spoofing the From: address. These messages were evading our filters and landing

Feature	SPF	SenderID
DNS records	v=spf1	v=spf2.0
Domain that it works on	Envelope sender (P1)	PRA (P2 – much more common) or envelope sender (much less common)
How does it treat SPF records	Works per normal	Treats it like a SenderID record if the SenderID record does not exist
How does it treat SenderID records	Ignores it	Works per normal
Strengths	<ul style="list-style-type: none"> - Can stop some phishing, good for some whitelisting - Can prevent backscatter by only sending bounces to messages that pass an SPF check - Can reject some messages in SMTP before accepting any data 	<ul style="list-style-type: none"> - Better at stopping phishing (or spoofing) that visually tricks the user - The PRA derives from actual Resent-* headers, and Sender and From headers; this makes validation on forwarded mail theoretically possible
Weaknesses	<ul style="list-style-type: none"> - Doesn't catch phishing when the P1 From is Neutral or None and the PRA is spoofed - Doesn't work on forwarded mail 	<ul style="list-style-type: none"> - Prone to false positives when mail is sent on behalf of another - Doesn't work on forwarded mail

Table 1: Comparison between SPF and SenderID.

in people's inboxes. Users were being fooled by the messages, clicking the links, and their workstations were being compromised. This was occurring regularly enough for the IT personnel of the company to escalate the matter to us¹.

At the time, I knew that SPF was an anti-spoofing technology but I didn't know much more beyond the basics so I did some research and learned a lot more. The spammer was sending mail from a domain with no SPF records in the 'P1 Mail From' and was spoofing the recipient's organization in the 'P2 From' address field. The result was that the recipients of the message were fooled into believing that it was from an internal sender because they recognized their 'own' domain as the sender.

For example, suppose that the organization receiving the mail was the government of Washington State²:

```
SMTP Mail From: alwknr@zebuzeze.com
P2 From: admin@wa.state.gov
To: tzink@wa.state.gov
Subject: Update your credentials
```

Dear recipient,

We are upgrading our security infrastructure. Please login to the following site and enter your credentials so it will update in our systems otherwise your account will be locked out.

<http://security.wa.state.gov/user/login>

Thanks for your co-operation in this regards.

Department of IT Security

Let's take this message apart and see what happened:

1. The state of Washington has published SPF records and tagged them with '-all', which means that receivers should Hard Fail any mail that purports to come from its servers but whose sending IP is not in its SPF record. This is something that a responsible organization does to prevent being spoofed and then delivered to someone's inbox.
2. Upon receipt of the message, the spam filter executes an SPF check on the email address in the 'P1 Mail From', which is the randomized `alwknr@zebuzeze.com`. The domain `zebuzeze.com` exists in DNS and has an A-record but does not publish SPF records. The spam filter checks it out

¹ This was the first instance I had seen of a spear phishing attack, although in retrospect it was probably less sinister than it sounds. A targeted spear phishing attack customizes everything, right down to the recipients. This attack spoofed the From: address, but nothing else in the message content was customized.

² The government of Washington State is not our customer, I use this as an example.

and the result is SPF None. It continues to pass it down to the rest of the filter.

3. The URL in the message is a newly created domain, and the message is sent from a new IP address that is part of a botnet but is not on any blocklists. It evades the spam filter's other reputation checks and ends up in the customer's inbox. This is a false negative.
4. The user sees the mail which appears to come from their own internal department, `admin@wa.state.gov`. Since it seems to come from a domain they recognize, they trust the message and decide to click on the link. The spammer has been clever enough to send the message in HTML format and the link in the message actually points to a spammer's domain. The user's computer has now become part of a botnet because they clicked on the link³.

If you only use SPF as part of your spam filter, then your filter will be prone to these types of attack. Whether spammers spoof your specific domain intentionally or are randomizing the domains in the senders, the fact is that SPF cannot prevent these emails from reaching your inbox.

I was left scratching my head. How could we combat these types of spam messages using content filtering? I started to investigate SPF and how it executes on the 'P1 From' address. The SPF documentation discourages the use of SPF on the 'P2 From' address because, while the P1 and P2 From addresses are often the same, *sometimes* they are not, and it is difficult to predict what will occur in the event that they are not the same. Will a spam filter flag legitimate messages as spam (i.e. generate false positives)? For example, suppose that the state of Washington wanted to send out a large mail campaign to residents of the state who had opted in to receive special announcements – e.g. about road repairs, government office closures, breaking news reports or results of legislative changes. Rather than sending these out themselves, the state might decide to use a marketing company, say, Big Communications, Inc. The marketing company wants the emails to look like they came from the state of Washington, but needs to avoid them being marked as spam.

Since SPF is the most common authentication technology, they would do something like the following:

³ One dismissive argument I hear regarding SPF's ability to prevent spoofing by Hard Failing spoofed addresses is that all a spammer has to do to circumvent it is to send mail from a slightly different account, say, `state.wa.gov.ghsataw.com`. This is true, and spammers do this. However, they also spoof the actual domains and they do this a lot. I have not measured which is more prolific, but the spoofing occurs so often that it is a legitimate scenario that requires a solution.

SMTP Mail From: tkgghsas@wa.state.gov@bigcommunications.com
 P2 From: communications@wa.state.gov
 To: tzink@wa.state.gov
 Subject: Latest results of bill 2101

Dear tzink@wa.state.gov,

The results of Bill 2101 are in! The legislature has voted to approve the use of \$2 million to the University of Diamondville to study the effects of weightlessness on tiny screws! This can have vast repercussions here in the future, everything from watch making to watch repair!

Stay tuned for more updates!

Washington State Department of Communications

Obviously, the contents of the mail above are entirely fictional and far fetched, and a government department might not outsource their communications. However, large corporations like *Microsoft* do. If an SPF check in the above example were performed on the 'P1 From' address, the result would be an SPF Pass. However, if it were performed on the 'P2 From' address – the one that is displayed in the mail client – the result would be an SPF Hard Fail. Many spam filters assign this a heavy weight and there is a good chance that the message would subsequently be marked as spam – the exact opposite of what is desired.

Thus, we are in a position where performing a standard SPF check leaves our recipients open to phishing attacks. Performing a modified SPF check on the 'P2 From' address (i.e. performing a SenderID check) has the very real possibility of marking legitimate messages as spam and generating false positives. What can we do? How can we get the best from SPF and SenderID (stopping phishing) while avoiding the worst of SPF and SenderID (false positives)?

COMBINING SPF AND SENDERID

While investigating these two technologies, I liked SenderID's ability to combat spoofing of the 'P2 From' address because that is what is displayed to the end-user. However, I could not stomach the idea of generating false positives.

The solution was to combine SPF and SenderID and perform *both* checks. They would not both be performed every time, but conditionally: a SenderID check would only be performed in the event that a standard SPF check returned a non-authoritative authentication result.

What do I mean by non-authoritative? Rather than the conventional Internet industry use of the term, I use it to refer to an assertion that we cannot say something for certain either one way or the other. To illustrate this, here are the results of an SPF check:

- **SPF Pass** – We can state with certainty that the sending IP of the message is permitted to send mail for that domain. It is explicitly stated in the SPF record published by that domain.
- **SPF Hard Fail** – We can state with certainty that the sending IP of the message is *not* permitted to send mail for that domain and should be treated with great suspicion.
- **SPF Soft Fail** – We can state with certainty, although a lot less of it, that the sending IP is *not* permitted to send mail for that domain.
- **SPF None** – We cannot state one way or the other whether the sending IP is permitted to send mail for the sending domain, and the result is ambiguous. This is what I mean by non-authoritative. We just don't know.
- **SPF Neutral** – Similar to SPF None, we don't know whether or not the IP is permitted to send mail for the sending domain. Again, it is ambiguous. Is it neutral because the sender forgot to include the IP in the SPF record, because the message is forwarded, or because the sender is forged? We can't assert either way.
- **SPF Temp Error, Perm Error** – The same as the above, we can't say one way or the other whether the sending IP is permitted to send mail for the domain.

The implementation we came up with was to send all messages in our pipeline through a standard SPF check. If the message returns Pass or Fail, then we know if the message is authenticated or spoofed. However, we don't know one way or the other if we get None, Neutral, Temp Error or Perm Error. If we get one of these results, *then* we perform a SenderID look up on the 'P2 From' address to see if that address is being spoofed – a SenderID check is conditional upon the result of an SPF check. Once that result comes back, appropriate action can be taken:

- Use the Hard or Soft Fail as weights in the spam filter.
- Use the other results with the same actions that you would take for the results of a regular SPF check.

The idea is that, since we didn't have an authentication answer the first time, we try it again a second time on a different field and see what the result is.

Let's return to our two previous examples and see how we can get the results we want while avoiding the results we don't want:

SMTP Mail From: alkwnr@zebuzez.com
 P2 From: admin@wa.state.gov
 To: tzink@wa.state.gov
 Subject: Update your credentials

1. Perform an SPF check on `alkwnr@zebuzez.com`. It returns SPF None. This is a non-authoritative result.
2. Perform a SenderID check on `admin@wa.state.gov`. It returns SPF Hard Fail.

We therefore interpret this as a spoofed message and treat it as such. Whereas before it was a false negative, now it is detected as spam.

What about our other example?

```
SMTP Mail From: tkgghsas=wa.state.gov@
bigcommunications.com
P2 From: communications@wa.state.gov
To: tzink@wa.state.gov
Subject: Latest results of bill 2101
```

In this case:

1. Perform an SPF check on `tkgghsas=wa.state.gov@bigcommunications.com`. It returns an SPF Pass.

We therefore interpret this message as authenticated and proceed with the rest of the filtering pipeline. No further authentication is performed. Whereas before this message was a true positive with SPF, and a false positive with SenderID, now it is back to being a true positive again.

NAMING THE FEATURE

After it was decided that this was the way we would address the spoofing issue, we had to come up with a name for the feature. It isn't SPF and it isn't SenderID, it's a combination of the two of them. Since the feature is designed to authenticate against the 'From:' field in an email message, we called it 'From Address Authentication'. It authenticates against the 'From:' address of an email message⁴.

We decided that this feature would not be enabled by default on all inbound mail hitting the network. Instead, it would be a custom spam filter action that was off by default. In order to get the benefit of this feature an organization would have to activate it manually.

ACTIONS

Next, we had to decide on an action to take in the event that a message received a Hard Fail with the second check. Spam filters usually use the results of an SPF check as a weight in their scoring engines. Some (like ours) allow users to enable an option to auto-reject all mail that Hard Fails a traditional SPF check. I don't typically recommend

⁴Technically speaking, SenderID authenticates against the PRA, which is either the Resent-Sender, Resent-From, Sender or From field. In the majority of cases, this is the From: field.

this because more legitimate mail than you might think fails SPF checks – although for certain organizations that are heavily spoofed it makes sense.

We had to decide whether we wanted a Hard Fail to be used as a weight in the engine or to automatically mark the message as spam. Experience had taught me that auto-marking anything that Hard Fails an SPF check as spam would be prone to false positives. My proposal was to use the failure of this feature as a weight in the engine by default, and then give users another option to mark anything that Hard Failed the check as spam. However, a colleague pointed out that this would over complicate things for users. For one, they would have to enable this option manually. Second, they would subsequently have to click another checkbox to mark a message as spam instead of using the Hard Fail as a weight in the spam evaluation. That was too much. Better to pick one action and give the user the on/off option than to make them do two things⁵.

I decided to go with the auto-mark-as-spam option in the event that a message performed a From Address Authentication and returned a Hard Fail. Simplifying the design was the best option even if it had the potential to cause false positives. All of the other results (Soft Fail, Neutral, etc.) have their own weights associated with them and used in the spam filter evaluation. By itself, Hard Fail can single-handedly mark a message as spam. Thus, if an organization selects this option and publishes SPF records, then a spammer will not be able to spoof the organization in either the 'P1 From' or 'P2 From' address. Those messages will be marked as spam and hidden from the end-user.

RESULTS

The feature was coded, tested and deployed into the production network within a couple of months. Yet, for all of the work we had put in and the research we had done, I was still nervous. All of the reading I had done that looked at performing SPF checks on the 'P2 From' address suggested that the results were potentially unreliable. Would we get false positives? Would there be a whole bunch of scenarios that I hadn't considered and lots of complaints pouring in? The best case scenario was that it solved the problem of spoofing for the original customer

⁵Years later, when researching choice architecture – the process of providing users with a list of options – I discovered that giving users fewer choices is better than giving them more. The reason is that the more options we are given, the more difficult it is to make a decision and the less likely we are to be happy with that decision. This seems counterintuitive, but in fact a simplified interface with fewer options helps people make decisions faster and to remain happier with their decisions.

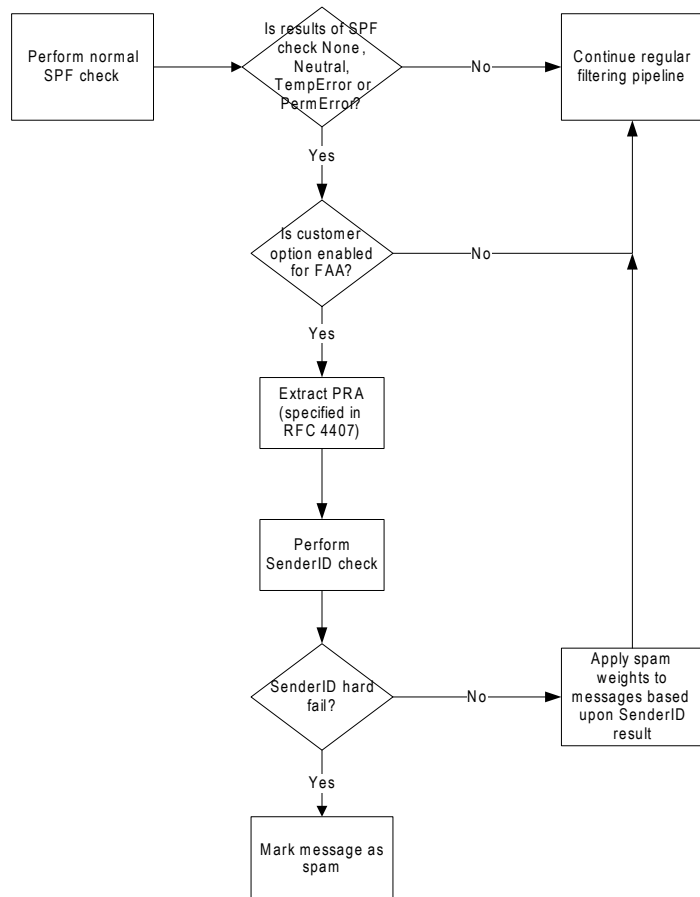


Figure 1: From address authentication in Forefront Online.

who had complained, that it was adopted by others and that no complaints came in. The worst case scenario was that piles of false positives occurred, the original customer complained and disabled the feature, phishing messages still came in and we would be back to square one.

As it turned out, it was the best case scenario. We solved the problem for the customer and stopped the phishing messages from hitting their inboxes. We didn't get false positive complaints from other people, and the feature was adopted by a number of other organizations as well. The feature worked exactly the way it was supposed to (how often does that happen in real life?). By getting creative with SenderID and SPF, we had managed to use them in a unique way that combined their strengths while avoiding their weaknesses.

CONCLUSION

SenderID and SPF each have their advantages and

weaknesses, but it is possible to use them together to create an effective anti-phishing mechanism that targets a specific case. Obviously, this is a special scenario. It doesn't solve the overall problem of phishing, which is still with us today; we even have an organization – the Anti-Phishing Working Group – that was formed in an effort to address the problem. Furthermore, this technique doesn't address the issue of when the phisher uses visually or phonetically similar domains to the one that's being spoofed (for example state.gov.wa.com.br), which don't publish SPF records but which look like a domain that the organization in question might use.

However, this solution does stop spammers who attempt to spoof either the 'P1 From' address or the 'P2 From' address when the targeted domain has published SPF and/or SenderID records. This scenario occurred so often that we were driven to come up with a response to it. It's true that SPF and SenderID each have their limitations, but it is equally true that they have their place in an anti-spam environment.

We have the evidence to prove it.

REFERENCES

- [1] Zink, T. What's the deal with sender authentication? Part 1. Virus Bulletin, June 2010, p.7. <http://www.virusbtn.com/pdf/magazine/2010/201006.pdf>.
- [2] Zink, T. What's the deal with sender authentication? Part 2. Virus Bulletin, July 2010, p.16. <http://www.virusbtn.com/pdf/magazine/2010/201007.pdf>.
- [3] Zink, T. What's the deal with sender authentication? Part 3. Virus Bulletin, August 2010, p.15. <http://www.virusbtn.com/pdf/magazine/2010/201008.pdf>.
- [4] Zink, T. What's the deal with sender authentication? Part 4. Virus Bulletin, September 2010, p.17. <http://www.virusbtn.com/pdf/magazine/2010/201009.pdf>.
- [5] Zink, T. What's the deal with sender authentication? Part 5. Virus Bulletin, December 2010, p.12. <http://www.virusbtn.com/pdf/magazine/2010/201012.pdf>.
- [6] Zink, T. What's the deal with sender authentication? Part 6. Virus Bulletin, January 2011, p.8. <http://www.virusbtn.com/pdf/magazine/2011/201101.pdf>.

COMPARATIVE REVIEW

VB100 COMPARATIVE REVIEW ON WINDOWS XP SP3

John Hawes

When *Windows XP* first came out, George W. Bush was still in his first year of presidency. The 9/11 attacks took place between the platform's release to manufacture and going on retail sale, as did the launch of the first generation *iPod*. *Wikipedia* was less than a year old, *Google* was just starting to turn a profit, while the likes of *Facebook*, *Skype*, *YouTube* and *World of Warcraft* were yet to come. Computers themselves were not too different from today of course, although the *Pentium 4* was the hottest chip on the block and *x64* was still a couple of years away. Skip forward almost a decade, and *XP* is still with us – not just hanging on by its fingertips but firmly remaining the most popular desktop platform (some estimates put it on over half of all desktop systems, and most agree that it runs on at least 40%). It is familiar, cheap, (comparatively) reliable and very popular. To most of the world's computer users, it's just the way computers work.

The operating system's popularity with users is, if anything, surpassed by its popularity with developers, so it was almost inevitable that we would be deluged with products of all shapes and sizes for this month's comparative, from the old and familiar to the new and scary. We knew there would be more than enough to keep us busy this month.

Of course, the platform's maturity and stability also mean there has been plenty of time for refinement and quality control, so we hoped that we might see a trend in products towards the sort of stability and reliability that has been woefully lacking in some quarters of late.

PLATFORM, TEST SETS AND SUBMISSIONS

Setting up *Windows XP* has become such a familiar and oft-repeated task that it requires very little effort these days. In fact, we simply recycled bare machine images from the last run on the platform a year ago, tweaking and adjusting them a little to make them more at home on our current hardware and network set-up, and re-recording the snapshots ready to start testing. As usual, no updates beyond the latest service pack were included, and additional software was kept to a minimum, with only some network drivers and a few basic tools such as archivers, document viewers and so on added to the basic operating system.

With the test machines ready good and early, test sets were compiled as early as possible too. The WildList set was synchronized with the January 2011 issue of the

WildList, released a few days before the test set deadline of 16 February. This meant a few new additions to the core certification set, the bulk of which were simple autorun worms and the like. Most interesting to us were a pair of new W32/Virut strains, which promised to tax the products, and as usual our automated replication system churned out several thousand confirmed working samples to add into the mix.

The deadline for product submission was 23 February, and as usual our RAP sets were built around that date, with three sets compiled from samples first seen in each of the three weeks before that date, and a fourth set from samples seen in the week that followed. We also put together entirely new sets of trojans, worms and bots, all gathered in the period between the closing of the test sets for the last comparative and the start of this month's RAP period. In total, after verification and classification to exclude less prevalent items, we included around 40,000 samples in the trojans set, 20,000 in the set of worms and bots, and a weekly average of 20,000 in the RAP sets.

The clean set saw a fairly substantial expansion, focusing on the sort of software most commonly used on home desktops. Music and video players, games and entertainment utilities dominated the extra 100,000 or so files added this month, while the retirement of some older and less relevant items from the set kept it at just under half a million unique files, weighing in at a hefty 125GB.

Some plans to revamp our speed sets were put on hold and those sets were left pretty much unchanged from the last few tests. However, a new performance test was put together, using samples once again selected for their appropriateness to the average home desktop situation. This new test was designed to reproduce a simple set of standard file operations, and by measuring how long they took to perform and what resources were used, to reflect the impact of security solutions on everyday activities. We selected at random several hundred music, video and still picture files, of various types and sizes, and placed them on a dedicated web server that was visible to the test machines. During the test, these files were downloaded, both individually and as simple zip archives, moved from one place to another, copied back again, extracted from archives and compressed into archives, then deleted. The time taken to complete these activities, as well as the amount of RAM and CPU time used during them, was measured and compared with baselines taken on unprotected systems. As with all our performance tests, each measure was taken several times and averaged, and care was taken to avoid compromising the data – for example, the download stage was run on only one test machine at a time to avoid possible network latency issues. We hope to expand on this selection of activities in future tests, possibly refining the selection of samples to

reflect the platforms used in each comparative, and perhaps also recording the data with greater granularity.

We had also hoped to run some trials of another new line of tests, looking at how well products handle the very latest threats and breaking somewhat with VB100 tradition by allowing both online updating and access to online resources such as real-time ‘cloud’ lookup systems. However, when the deadline day arrived and we were swamped with entrants, it was clear that we would not have the time to dedicate to this new set of tests, so they were put on hold until next time.

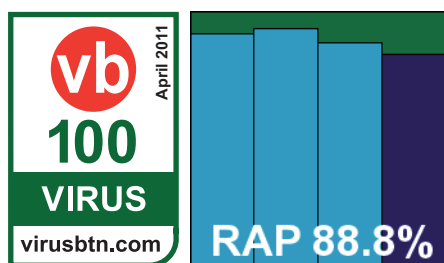
The final tally came in at 69 products – breaking all previous records once again. Several of these were entirely new names (indeed, a couple were unknown to the lab team until the deadline day itself). Meanwhile, all the regulars seemed to be present and correct, including a couple of big names that had been missing from the last few tests. With such a monster task ahead of us, there was not much we could do but get cracking, as usual crossing all available digits and praying to all available deities for as little grief as possible.

Agnitum Outpost Security Suite Professional 7.1

Version 3415.320.1247

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.57%
Worms & bots	96.89%	False positives	0

Agnitum kicks off this month’s comparative in its usual solid style. This is the full ‘Pro’ version of the suite solution, which



has recently been joined by a slightly pared-down free edition, still offering a good range of protection layers. The installer came as a 94MB executable, with the latest updates thoughtfully built in, and the set-up process followed the usual steps of language selection, EULA and so on; it took a couple of minutes to get through, and a reboot was needed to complete.

The GUI hasn’t changed much for a while, remaining clear and simple with not much in the way of fancy frills to get in the way of things. The product includes a comprehensive set of firewall, HIPS, web filtering and anti-spam components.

Configuration is not hugely in-depth (for the anti-malware component at least), but a good basic set of controls are provided. Testing ran smoothly, unhindered by unexpected behaviour or difficulties operating the solution. We were once again impressed by some judicious use of result caching to ensure items that had already been checked were not processed again, and this efficiency helped us keep the overall test time to well within the expected bounds (when planning our testing schedule we roughly allocate 24 hours to each product for full testing).

Scanning speeds and on-access lags were decent to start with, both speeding up hugely in the warm sets, and while RAM and CPU consumption were perhaps a little above average, impact on our new sets of standard activities was minimal.

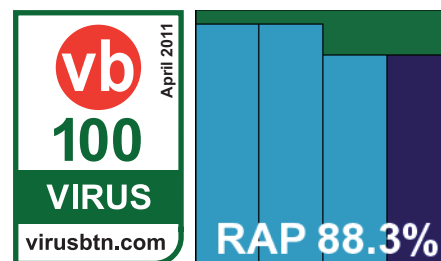
Detection rates were decent as ever, with solid scores in most areas, and the WildList caused no problems. The clean sets were also handled well, with only a single item labelled as adware, and a VB100 award is duly earned by *Agnitum*. This brings the company’s tally in the past two years to seven passes and one fail, with four tests not entered – all of the last six entries having resulted in passes.

AhnLab V3 Internet Security 8.0.4.6

Build 925; engine version 2011.02.23.31

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	94.05%
Worms & bots	98.35%	False positives	0

AhnLab is a pretty regular participant in our comparatives, and the company’s product is generally well behaved (the



occasional wobbly month notwithstanding). This month’s submission was a 155MB executable, including latest updates, and ran through its installation process fairly uneventfully. An option to apply a licence was declined in favour of a trial version, and we were also offered the choice of including a firewall – this was not enabled by default, so was ignored. The process completed in under a minute and needed no reboot.

The product is reasonably clean and efficient-looking, although some of the configuration was a little hard to find. Thankfully, past experience had taught us to search

thoroughly to make sure all configuration options were checked. Intrusion prevention and firewalling is provided in addition to the anti-malware component, and there are some extra tools as well. Testing ran through smoothly without any major problems – even the log viewer, which has caused some pain in the past, proved solid and stable.

Scanning speeds were not super fast, but lag times were low, with fairly low use of RAM too. CPU use was a little higher though, and the time taken to complete our set of tasks was around average.

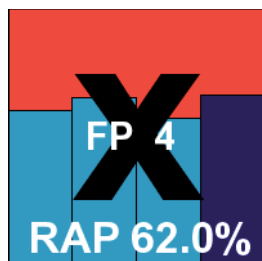
Detection rates were very good, continuing an upward trend observed in recent tests, and the WildList and clean sets presented no problems at all. *AhnLab* earns a VB100 award, making six passes and four fails in the last two years, with two tests not entered – five of the vendor’s last six entries have passed.

Antiy Ghostbusters 7.1.5.2760

Version 2011.02.23.20

ItW	87.02%	Polymorphic	19.82%
ItW (o/a)	NA	Trojans	23.91%
Worms & bots	72.88%	False positives	4

Antiy was an interesting newcomer to our line-up this month. We have been in contact with the company for some time now, and have long looked forward to the product’s debut in our comparatives. *Antiy Labs* hails from China, with branch offices in Japan and the US, and has been operating for over a decade. It makes its scanning engine available as an SDK, which sees it used in various firewalls, UTMs and other security devices, according to the company’s website.



The product was sent in as a 50MB executable, which had some fairly recent updates included, but for optimum performance we installed and updated the product online on the deadline date. This was not as simple as it might have been, as the product is only available in Chinese; however, a thorough usage guide was kindly provided, and once Chinese support had been added to the test system it was fairly straightforward to figure out what to click and when. The set-up process took only a few minutes, including updating, with no need to reboot.

The main product GUI looks slick and professional (although of course much of the actual content was unintelligible to us), and navigating wasn’t too difficult thanks to a combination of the guide provided, basic

recognition of some characters, and a general sense of where things tend to be in anti-malware product interfaces. The initial stages of testing ran through very nicely, with all on-demand tests zipping through without difficulty, but the on-access component proved elusive. We could find no evidence of the on-access scanner in initial trials of our archive tests, but this was inconclusive since we found that the on-demand component did not detect the EICAR test file either. Various other attempts, including checking that files were detected by the on-demand scanner before copying them around the system and even executing them, produced no results, and a request for information from the submitters went unanswered. Whether or not the product even has an on-access component thus remains a mystery, but either way as it does not appear to be enabled by default it would not be possible to include it in our official tests.

This also meant there was no point in running our standard performance measures, but on-demand scanning speeds were pretty zippy, and the product powered through the infected sets in good time too.

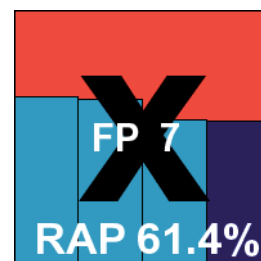
The logs showed some fairly disappointing scores, with coverage of polymorphic items particularly poor, but the RAP sets showed a steady, if not super-high detection rate. The WildList showed a fair few misses, with a handful of false alarms in the clean set too, and of course no obvious on-access capability was found, giving us several reasons to deny *Antiy* a VB100 award for the time being. However, the product impressed the team and looks like a good bet for some rapid improvements.

ArcaBit ArcaVir 11.2.3205.1

Update 2011.02.24.12:54:56

ItW	100.00%	Polymorphic	93.63%
ItW (o/a)	100.00%	Trojans	63.06%
Worms & bots	72.11%	False positives	7

ArcaBit has made a few appearances in our comparatives over the last few years, and has shown some steady improvements both in performance and stability.



The install package weighed in at 95MB and needed no additional updates; it ran through in good time with no surprises. The

product is a full suite including firewall, anti-spam, mail and web monitors, and some intrusion prevention components.

The interface has been adjusted and improved a little of late, and is now looking complete and polished. The layout is

On-demand tests	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	620	96.89%	0	100.00%	4820	88.57%		1
AhnLab V3 Internet Security	0	100.00%	329	98.35%	4	99.99%	2508	94.05%		
Antiy Ghostbusters	3170	87.02%	5409	72.88%	30093	19.82%	32100	23.91%	4	
ArcaBit ArcaVir	0	100.00%	5563	72.11%	534	93.63%	15585	63.06%	7	
AvailaSoft AS Anti-Virus	51	91.43%	10743	46.13%	1661	71.09%	26431	37.35%		
Avast Software avast! Free	0	100.00%	209	98.95%	1	100.00%	1352	96.80%		
Avertive VirusTect	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
AVG Internet Security	0	100.00%	277	98.61%	4	99.99%	2719	93.55%		
Avira AntiVir Personal	0	100.00%	110	99.45%	0	100.00%	630	98.51%		
Avira AntiVir Professional	0	100.00%	110	99.45%	0	100.00%	630	98.51%		
BitDefender Antivirus Pro	0	100.00%	93	99.53%	0	100.00%	1908	95.48%		
Bkis BKAV Professional	0	100.00%	82	99.59%	0	100.00%	218	99.48%	3	
Bullguard Antivirus	0	100.00%	73	99.63%	0	100.00%	1238	97.07%		
CA Internet Security Suite Plus	0	100.00%	606	96.96%	4	99.96%	8363	80.18%		1
CA Total Defense r12	0	100.00%	785	96.06%	4	99.96%	9170	78.26%		
Central Command Vexira	0	100.00%	597	97.01%	0	100.00%	4682	88.90%		
Check Point Zone Alarm	0	100.00%	165	99.17%	0	100.00%	3089	92.68%		1
Clearsight Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
CommTouch Command	0	100.00%	2569	87.12%	0	100.00%	9118	78.39%		3
Comodo I.S. Premium	0	100.00%	791	96.03%	648	90.63%	3278	92.23%		2
Coranti 2010	0	100.00%	33	99.83%	0	100.00%	420	99.00%		5
Defenx Security Suite	0	100.00%	642	96.78%	1	100.00%	4833	88.54%		
Digital Defender	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
eEye Blink	0	100.00%	2161	89.16%	4	99.98%	5596	86.73%		2
Emsisoft Anti-Malware	4	99.33%	224	98.88%	452	95.58%	2085	95.06%	2	1
eScan Internet Security	0	100.00%	59	99.70%	0	100.00%	1242	97.06%		
ESET NOD32	0	100.00%	372	98.13%	0	100.00%	4517	89.29%		3
Filseclab Twister	373	97.62%	6324	68.29%	14041	63.35%	13979	66.86%	19	
Fortinet FortiClient	0	100.00%	382	98.08%	0	100.00%	2923	93.07%	1	
Frisk F-PROT	0	100.00%	1841	90.77%	0	100.00%	10486	75.14%		
F-Secure Client Security	0	100.00%	77	99.61%	0	100.00%	1499	96.45%		1
F-Secure Internet Security	0	100.00%	74	99.63%	0	100.00%	1435	96.60%		1
G DATA AntiVirus 2011	0	100.00%	23	99.88%	0	100.00%	201	99.52%		
Hauri ViRobot Desktop	4	99.33%	6989	64.96%	0	100.00%	14747	65.04%		
Ikarus T3 virus.utilities	1	99.83%	113	99.43%	452	95.58%	1150	97.27%	3	1

Please refer to text for full product names.

On-demand tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
iolo System Shield	0	100.00%	2700	86.46%	0	100.00%	10804	74.39%		
K7 Total Security	0	100.00%	814	95.92%	0	100.00%	6529	84.52%		
Kaspersky Anti-Virus 6	0	100.00%	151	99.24%	0	100.00%	3779	91.04%		
Kaspersky Internet Security	0	100.00%	494	97.52%	0	100.00%	3912	90.73%		
Kaspersky PURE	0	100.00%	114	99.43%	0	100.00%	2771	93.43%		
Keniu Antivirus	0	100.00%	109	99.45%	0	100.00%	2712	93.57%		1
Keyguard Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
Kingsoft I.S. 2011 Advanced	0	100.00%	12077	39.45%	407	96.04%	35140	16.70%		
Kingsoft I.S. 2011 Standard-A	0	100.00%	12827	35.68%	407	96.04%	38614	8.47%		
Kingsoft I.S. 2011 Standard-B	0	100.00%	12832	35.66%	407	96.04%	38616	8.46%		
Lavasoft Ad-Aware Total Security	0	100.00%	57	99.71%	0	100.00%	1013	97.60%		1
Logic Ocean Gprotect	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
McAfee VirusScan Enterprise	0	100.00%	1045	94.76%	0	100.00%	6312	85.04%		5
Microsoft Forefront Endpoint Protection	0	100.00%	175	99.12%	0	100.00%	3815	90.96%		8
Nifty Corp. Security 24	0	100.00%	109	99.45%	0	100.00%	2730	93.53%		1
Norman Security Suite	0	100.00%	2161	89.16%	4	99.98%	5568	86.80%		1
Optenet Security Suite	0	100.00%	1632	91.82%	0	100.00%	9813	76.74%		
PC Booster AV Booster	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
PC Renew I.S 2011	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
PC Tools I.S. 2011	0	100.00%	312	98.44%	0	100.00%	2595	93.85%		
PC Tools Spyware Doctor	0	100.00%	312	98.44%	0	100.00%	2595	93.85%		
Preventon Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%		
Qihoo 360 Antivirus	0	100.00%	70	99.65%	0	100.00%	1159	97.25%		
Quick Heal Total Security 2011	0	100.00%	1451	92.72%	0	100.00%	7325	82.64%		
Returnil System Safe 2011	0	100.00%	1703	91.46%	0	100.00%	8910	78.88%		3
Sofscan Professional	0	100.00%	731	96.33%	0	100.00%	4682	88.90%		
Sophos Endpoint Security and Control	0	100.00%	2455	87.69%	0	100.00%	3503	91.70%		
SPAMfighter VIRUSfighter	0	100.00%	816	95.91%	0	100.00%	5750	86.37%		
GFI/Sunbelt VIPRE	0	100.00%	66	99.67%	19	99.79%	849	97.99%		
Symantec Endpoint Protection	0	100.00%	349	98.25%	0	100.00%	2900	93.13%		
Trustport Antivirus 2011	0	100.00%	29	99.85%	0	100.00%	355	99.16%		
UnThreat Antivirus Professional	0	100.00%	65	99.67%	19	99.79%	849	97.99%		1
VirusBuster Professional	0	100.00%	731	96.33%	0	100.00%	4682	88.90%		
Webroot Internet Security Complete	0	100.00%	306	98.47%	0	100.00%	2934	93.05%		

Please refer to text for full product names.

fairly usable and it responded well even under pressure; no stability problems of any kind were observed during the full test run, which completed in good time.

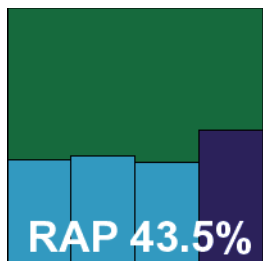
Scanning speeds were pretty good, and on-access lags were not bad either, while use of RAM and impact on our activities set were about average and CPU use was fairly low.

Scores were just about reasonable, with a fairly notable step down mid-way through the RAP sets. The WildList was handled without problems, but both the clean set and the speed sets threw up a handful of false alarms, including items from *Microsoft*, a component of *MySQL* and the popular *Joomla* wiki system. This was enough to deny *ArcaBit* a VB100 award this month, leaving it with just one pass in the last two years, from a total of five attempts.

AvailaSoft AS Anti-Virus 1.0.0.1

ItW	91.43%	Polymorphic	71.09%
ItW (o/a)	91.43%	Trojans	37.35%
Worms & bots	46.13%	False positives	0

When newcomer *AvailaSoft* first came to our attention we noted some interesting test results quoted on the company’s website – two testing labs, previously unknown to us, were quoted as rating the product very highly indeed. So far our attempts to contact these labs to find out more about their methodology – and encourage them to join testing community endeavours such as AMTSO – have gone unanswered. *AvailaSoft* itself is based in Duluth, GA, USA, with offices in several other regions, and was founded in 1996.



The install package weighed in at a very reasonable 61MB, and after the minimum number of set-up stages it zipped through its activities in double-quick time, with a reboot at the end. Getting the interface up proved less speedy however, as on boot-up the test machine seemed to take rather a long time to get its act together (we hope to add some boot speed checks to our test suite in the very near future to get more accurate measures of this kind of thing). The GUI eventually opened, however, and proved reasonably pleasant to operate, if a little drab and grey. Options were a little odd in places, with the list of possible actions to take on detection being ‘auto-treat’, ‘clean’ or ‘delete if disinfection fails’, which seemed to overlap each other and provide no actual choice. The interface was generally responsive, but prone to odd spells of slowing down, where buttons would take some time to elicit a response.

Scanning was similarly sluggish but generally well-behaved, although handling large quantities of infected items proved a heavy burden and many scans had to be aborted after slowing to a point of unbearable drag. On occasion, scans simply stopped with no sign of any results or logs. By breaking up the sets into smaller chunks we managed to get through most of the tests in the end, although it took several times the allotted 24-hour time period to do so.

Scanning speeds were very slow, and on-access lag times enormous, with one particular job – which usually takes less than a minute on a bare system – dragged out to several hours. This seemed to improve somewhat on warm runs. Impact on our activities suite was fairly heavy, and while RAM use was around average, CPU use actually showed a large reduction over the same job running on a bare system – this suggests that much of the extra time being added to the various jobs carried out actually left the processor idle.

Looking over the results we saw some confusing variation, with no apparent correlation between the scores recorded and those of other products using the same engine, or even with the same product in different detection modes. So we went back and repeated the tests, finding them once again slow and prone to sudden and unexplained death. Each time a scan failed to complete and report results, it was necessary to repair the affected sample set and re-run the job in smaller chunks.

Eventually we managed to get at least one set of scan logs for each area of the test sets, by running on up to six of our test systems for several further days, but even combining all the various runs together showed far lower scores than anticipated. With no further time available, we finalized the results as the combined best of all jobs. The results for the WildList set, after more than 20 runs through in both modes, seemed to be reliably accurate at least, showing good coverage of the polymorphic items but a fair number of other samples not detected. As a result, no VB100 award can go to *AvailaSoft* just yet, despite an enormous amount of work on our part.

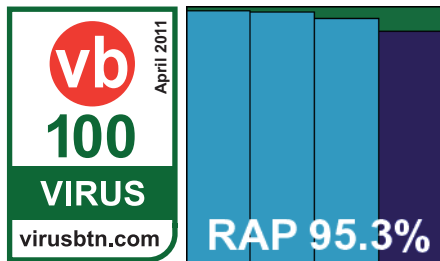
Avast Software avast! Free Antivirus 6

Version 6.0.1000; engine and virus definitions version 110223-1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.80%
Worms & bots	98.95%	False positives	0

Avast made some serious cosmetic and technical improvements with its version 5, released not long ago, and was heartily praised in these pages (see *VB*, January 2010,

p.17). Version 6 popped out rather unexpectedly, and we were intrigued to see what further strides had been made.



The 62MB install package, provided with all updates included, looked fairly similar to previous submissions, involving only a few steps, one of which is an offer to install the *Google Chrome* browser. A brief scan is also included as part of the set-up, but the whole thing is still complete in under half a minute. No reboot is required, although the application sandboxing system – which seems to be the main addition in this new version – does require a restart to become fully functional.

The interface remains much as before, the colours looking perhaps a little less bold and impressive, but the layout is generally sensible and easy to operate. The new sandbox caused a few problems in our speed tests, as prompts regarding innocent packages with potentially suspect capabilities interrupted measures. Eventually, the settings were tweaked to automatically apply the sandbox rather than prompting all the time. However, we had a few further issues using this setting, with the machine becoming unresponsive a few times and needing to be reimaged to a clean operating system to enable us to continue with tests – all this before even engaging in any malware tests. When these issues were not blocking progress, things zipped along with their customary speed, and even with the issues we still got all the necessary jobs done in under 24 hours.

As usual, scanning speeds were fast, and lag times very low, with low use of memory and a small effect on the time taken to complete our set of activities, although CPU use was closer to the average for this month's test.

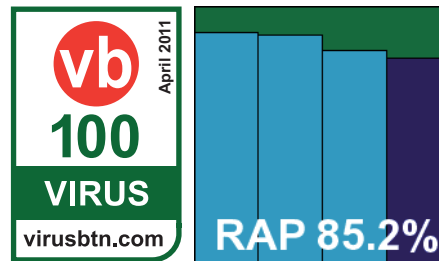
With the final results processed we saw some stomping good scores, highly impressive in all sets. The WildList and clean sets were handled without a glitch, earning *Avast* another VB100 award for its free product; the company boasts an impeccable 12 out of 12 record in the last two years of our comparatives.

Avertive VirusTect 1.1.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Avertive has appeared in a couple of tests recently, being part of a set of products derived from the same toolkit, a front end and SDK



to the *VirusBuster* engine developed by *Prevention*, whose own version first took part in late 2009 (see *VB*, December 2009, p.16). The number of these entries continues to grow, with *Avertive* already one of the more familiar names on the list.

The product comes as a 67MB installer and runs through a very standard set of steps, with no reboot needed to complete installation. An Internet connection is needed to apply a licence key, without which much of the configuration is inaccessible, but even with the time taken to complete this step, only a minute or so is needed in total to get things up and running.

The interface is pared-down and simple, but provides a decent range of controls covering most of the standard bases. The only issue that has troubled us in the past is a lack of control over the logging system, which defaults to overwriting logs once they have reached a certain size: 10MB for on-demand scans and 2MB for on-access activity. This presents a problem for us in gathering results of our large scans of course, but could also pose issues for real-world users: since the default setting is to log every file scanned, it would be easy to run a scan job which turned up an infection, but could not tell you at the end what was found or where (of course, with the default settings some action would have been taken to combat the threat, but it's usually best to be aware of what's been done to your system even in the name of good security). Fortunately, after some trial and error, we managed to increase the log sizes by making some simple registry tweaks.

The product proved as solid and stable as on previous occasions, with a nice simple process to get all the tests complete. Slow scanning of some polymorphic samples – which were heavily represented in some of our sets – dragged out the testing process somewhat, but with careful organization we just about got it all done in not much over a day.

Scanning speeds were fairly average and on-access lag times a little lighter than many, with low use of CPU cycles and RAM use. Impact on our activities suite was not excessive either.

On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	612	96.93%	0	100.00%	5304	87.43%
AhnLab V3 Internet Security	0	100.00%	448	97.75%	4	99.99%	2977	92.94%
Antiy Ghostbusters	NA	NA	NA	NA	NA	NA	NA	NA
ArcaBit ArcaVir	0	100.00%	5566	72.09%	534	93.63%	15680	62.83%
AvailaSoft AS Anti-Virus	51	91.43%	12089	39.39%	8861	78.12%	34872	17.34%
Avast Software avast! Free	0	100.00%	42	99.79%	1	100.00%	1056	97.50%
Avertive VirusTect	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
AVG Internet Security	0	100.00%	297	98.51%	4	99.99%	2984	92.93%
Avira AntiVir Personal	0	100.00%	129	99.35%	0	100.00%	927	97.80%
Avira AntiVir Professional	0	100.00%	129	99.35%	0	100.00%	928	97.80%
BitDefender Antivirus Pro	0	100.00%	70	99.65%	0	100.00%	1760	95.83%
Bkis BKAV Professional	0	100.00%	82	99.59%	0	100.00%	218	99.48%
Bullguard Antivirus	0	100.00%	73	99.63%	0	100.00%	1259	97.02%
CA Internet Security Suite Plus	0	100.00%	606	96.96%	4	99.96%	8363	80.18%
CA Total Defense r12	0	100.00%	785	96.06%	4	99.96%	9170	78.26%
Central Command Vexira	0	100.00%	813	95.92%	0	100.00%	5590	86.75%
Check Point Zone Alarm	0	100.00%	1444	92.76%	0	100.00%	10394	75.36%
Clearsight Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
CommTouch Command	0	100.00%	2714	86.39%	0	100.00%	11317	73.17%
Comodo I.S. Premium	0	100.00%	811	95.93%	648	90.63%	3590	91.49%
Coranti 2010	0	100.00%	41	99.79%	0	100.00%	827	98.04%
Defenx Security Suite	0	100.00%	635	96.82%	0	100.00%	5471	87.03%
Digital Defender	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
eEye Blink	0	100.00%	2394	88.00%	38	99.66%	6424	84.77%
Emsisoft Anti-Malware	2	99.66%	143	99.28%	452	95.58%	1164	97.24%
eScan Internet Security	0	100.00%	90	99.55%	0	100.00%	1842	95.63%
ESET NOD32	0	100.00%	583	97.08%	0	100.00%	4643	88.99%
Filseclab Twister	1933	92.81%	6798	65.91%	20304	48.84%	14067	66.65%
Fortinet FortiClient	0	100.00%	382	98.08%	0	100.00%	2923	93.07%
Frisk F-PROT	0	100.00%	1871	90.62%	0	100.00%	11176	73.51%
F-Secure Client Security	0	100.00%	65	99.67%	0	100.00%	1636	96.12%
F-Secure Internet Security	0	100.00%	76	99.62%	0	100.00%	1656	96.07%
G DATA AntiVirus 2011	0	100.00%	41	99.79%	0	100.00%	700	98.34%
Hauri ViRobot Desktop	4	99.33%	6990	64.95%	0	100.00%	14757	65.02%
Ikarus T3 virus.utilities	1	99.83%	113	99.43%	452	95.58%	1150	97.27%

Please refer to text for full product names.

On-access tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
iolo System Shield	1	99.83%	2700	86.46%	0	100.00%	10804	74.39%
K7 Total Security	0	100.00%	846	95.76%	0	100.00%	8168	80.64%
Kaspersky Anti-Virus 6	0	100.00%	158	99.21%	0	100.00%	3998	90.52%
Kaspersky Internet Security	0	100.00%	593	97.03%	0	100.00%	4142	90.18%
Kaspersky PURE	0	100.00%	168	99.16%	0	100.00%	3472	91.77%
Keniu Antivirus	1	99.83%	141	99.29%	0	100.00%	3809	90.97%
Keyguard Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
Kingsoft I.S. 2011 Advanced	0	100.00%	12082	39.42%	407	96.04%	35234	16.48%
Kingsoft I.S. 2011 Standard-A	0	100.00%	12828	35.68%	407	96.04%	38658	8.36%
Kingsoft I.S. 2011 Standard-B	0	100.00%	12833	35.65%	407	96.04%	38660	8.36%
Lavasoft Ad-Aware Total Security	0	100.00%	41	99.79%	0	100.00%	700	98.34%
Logic Ocean Gprotect	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
McAfee VirusScan Enterprise	0	100.00%	1047	94.75%	0	100.00%	6540	84.50%
Microsoft Forefront Endpoint Protection	0	100.00%	294	98.53%	0	100.00%	4449	89.45%
Nifty Corp. Security 24	0	100.00%	142	99.29%	0	100.00%	3506	91.69%
Norman Security Suite	0	100.00%	2394	88.00%	38	99.66%	6421	84.78%
Optenet Security Suite	0	100.00%	182	99.09%	1	99.99%	4657	88.96%
PC Booster AV Booster	0	100.00%	813	95.92%	0	100.00%	5618	86.68%
PC Renew I.S 2011	0	100.00%	813	95.92%	0	100.00%	5618	86.68%
PC Tools I.S. 2011	0	100.00%	312	98.44%	0	100.00%	2653	93.71%
PC Tools Spyware Doctor	0	100.00%	312	98.44%	0	100.00%	2653	93.71%
Preventon Antivirus	0	100.00%	815	95.91%	0	100.00%	5700	86.49%
Qihoo 360 Antivirus	0	100.00%	104	99.48%	0	100.00%	1936	95.41%
Quick Heal Total Security 2011	0	100.00%	2016	89.89%	0	100.00%	10482	75.15%
Returnil System Safe 2011	0	100.00%	1847	90.74%	0	100.00%	11100	73.69%
Sofscan Professional	0	100.00%	813	95.92%	0	100.00%	5590	86.75%
Sophos Endpoint Security and Control	0	100.00%	253	98.73%	0	100.00%	2761	93.46%
SPAMfighter VIRUSfighter	0	100.00%	816	95.91%	0	100.00%	5750	86.37%
GFI/Sunbelt VIPRE	0	100.00%	575	97.12%	38	99.50%	3662	91.32%
Symantec Endpoint Protection	0	100.00%	318	98.41%	0	100.00%	2692	93.62%
Trustport Antivirus 2011	0	100.00%	34	99.83%	0	100.00%	735	98.26%
UnThreat Antivirus Professional	0	100.00%	575	97.12%	38	99.50%	3662	91.32%
VirusBuster Professional	0	100.00%	813	95.92%	0	100.00%	5590	86.75%
Webroot Internet Security Complete	0	100.00%	299	98.50%	0	100.00%	3381	91.99%

Please refer to text for full product names.

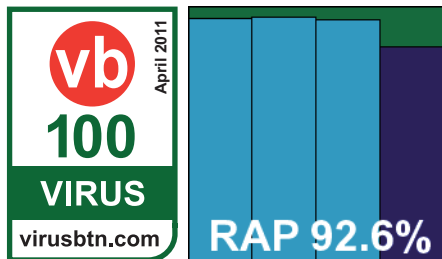
Detection rates were pretty decent, with an interesting two-step pattern in the RAP scores, and after a few unlucky months, where settings of the on-access component denied *Avertive* certification, this time all went well in the WildList, in both modes. With no problems in the clean sets either, the company can finally claim its first VB100 award after two previous failed attempts.

AVG Internet Security Business Edition 2011

Version 10.0.1204; virus database version 1435/3463

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	93.55%
Worms & bots	98.61%	False positives	0

AVG continues to consolidate its position as a well-known and widely trusted security brand, expanding and diversifying its capabilities



with regular acquisitions, and its premium products have established a solid record in our tests.

The current version came as a 149MB installer package, including updates, and the install process is reasonably rapid and straightforward – the only incidents of note being the offer of a browser toolbar and the choice of joining a feedback scheme. With no reboot required, the process is complete within a couple of minutes.

The interface has a sober and sensible feel to it, and somehow seems a little less cluttered than previous entries. On top of the standard anti-malware protection are extras including a rootkit scanner and *AVG's LinkScanner* safer browsing system. Configuration for all is exemplary in its clarity and comprehensiveness. Stability was rock-solid, with a nice simple scheduler helping to ensure time was well used, and all tests were completed well within the allotted 24 hours.

This was helped by some good use of result caching to speed up repeat scans of previously checked items, and the product powered through the speed tests in excellent time, showing very light lag times on access too. With RAM use not too high and CPU drain fairly noticeable, the set of standard tasks ran through almost as quickly as on the baseline systems.

Scores were excellent across the board, with impressive reliability throughout the reactive part of the RAP sets and

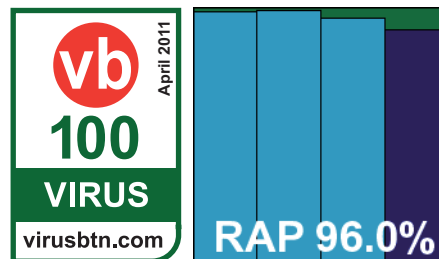
only a slight decrease in the proactive week. The WildList and clean sets presented no problems, and *AVG* easily earns another VB100 award – making 11 passes in the last two years, with just one test not entered.

Avira AntiVir Personal 10.0.0.611

Virus definition file 7.11.03.177

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.51%
Worms & bots	99.45%	False positives	0

Avira continues to thrive with its combination of efficiency and superb detection rates, its free product snapping at the heels of a couple



of others already looked at this month. The product has a soothing longevity of design, with changes introduced slowly to give an impression of evolution rather than sudden and drastic renewal.

The current iteration of the free-for-home-use personal edition was supplied as a 48MB installer, with an additional 38MB of updates, which were simple to apply using a standard built-in process. The set-up is straightforward and rapid, with (obviously) no licence code or file to apply, although there is an offer to register online. With no reboot required the process is complete in less than a minute.

The interface is clean and simple, with little by way of additional modules, but comprehensive configuration controls are easily accessed via an 'expert mode' button. Stability was generally as solid as ever, although a couple of scan jobs in our speed tests seemed to linger long after they had completed and been told to shut – simply ending the task with a right-click was all it took to get things moving again though. Tests were completed in excellent time, with just a few hours at the end of an afternoon and some jobs running overnight meaning several hours were cut from the expected day of testing.

Scanning speeds were very fast, as usual, and on-access measures showed a light footprint too, with low use of RAM and CPU and a light impact on our set of tasks.

Detection rates were pretty hard to beat, as is also usual for *Avira*, and even the proactive RAP set was more than 90% covered. The WildList was demolished and no issues emerged in the clean sets, only a couple of items alerted

on as adware. *Avira* thus earns another VB100 award quite comfortably. This free version of the product has only entered four tests in the last couple of years, but has aced all of them.

Avira AntiVir Professional 10.0.0.976

Virus definition file 7.11.03.177

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.51%
Worms & bots	99.45%	False positives	0

Avira's Pro edition is fairly similar to the free version on the surface, and although the installer package is a few MB larger, the

same update bundle was used. The install process felt fairly similar, although the application of a licence key file took the place of the registration step. Again, no reboot was needed and everything was over with in under a minute.

The interface looks and feels much the same. Configuration was excellent, and stability again generally solid, although we saw the same occasional minor snags when closing the 'Luke Filewalker' scanner module. We were happy to see another product out of the way in considerably less than 24 hours, freeing up more time for other, less zippy solutions.

Scanning speeds were again super fast, with very low impact on file accesses, and performance measures closely mirrored the free version.

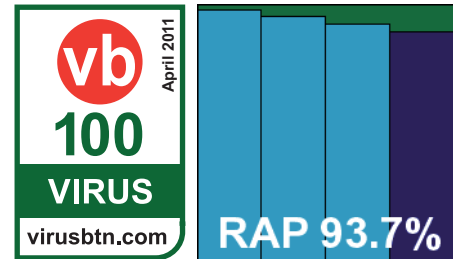
Scores were identical to the free edition, as might be expected given that both used the same detection data, and the lab team once again nodded their approval as set after set was demolished with remarkably high scores throughout – setting a high bar for others to aim for. A VB100 award is earned with style, giving *Avira's Pro* product line 10 passes out of 12 entries in the last two years, and a 100% record in the last six tests.

BitDefender Antivirus Pro 2011

Version 14.0.28.351 of branch 14.24; engine version 7.3681

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	95.48%
Worms & bots	99.53%	False positives	0

BitDefender is another major firm whose reputation continues to grow with the company itself. As usual it is well represented in OEM and rebranded products, with some half a dozen of this month's list including the company's engine in some form or other.

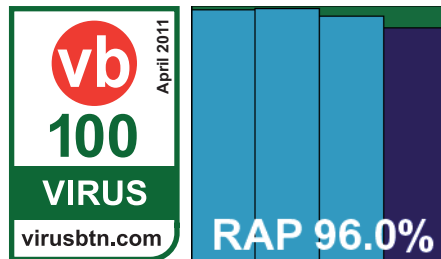


The current mainline product came in as a fairly large 265MB package, with all updates included. The set-up process was considerably longer and more involved than most. A 'quick' scan early on took close to five minutes, and a large number of steps followed, including options to remove other solutions already present on the system, to disable the *Windows Defender* system, and to share updates with other *BitDefender* users (presumably some kind of *Torrent*-style data-pooling system). After what seemed to be the last of many steps, listing the included features as anti-virus and identity protection, a ten-second pause was followed by another option: whether or not to contribute anonymous data to a feedback system. There was then another ten seconds of silence, then the offer of a demo video – fortunately we didn't have *Flash Player* installed on the test systems, so we could finally get testing under way.

As we have come to expect with *BitDefender* products, the interface has multiple personalities, with different degrees of complexity depending on the skills and knowledge of the operator. We opted for the most advanced mode, of course, which we found to provide an excellent level of controls in a nice usable style. The simpler versions also seemed clear and well laid out, and the styling is attractive. Stability was generally decent, although during one large scan of infected items there was a scanner crash, with no log data to be found, so nothing to show for several hours' worth of machine time. Nevertheless, decent progress was made elsewhere and the full test suite was completed in good order.

Scanning speeds were OK, with caching of results apparently no longer in effect on demand, where it is perhaps of less use than on access. Here, lag times were very light indeed, and did speed up enormously in the warm runs. CPU use was a little higher than many this month, but memory consumption was low, as was slowdown of our set of tasks.

Detection rates were splendid, as usual, with excellent scores in the main sets and a very slow decline across the weeks of the RAP sets – the proactive week a whisker short

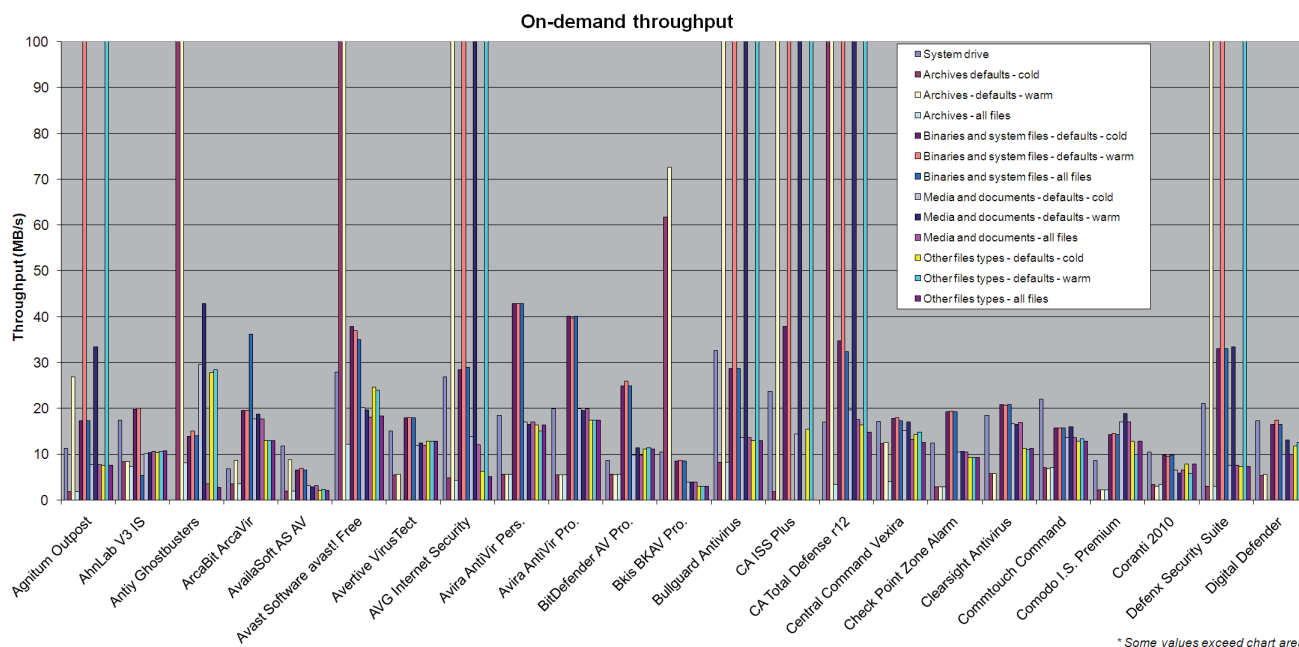


On-demand throughput (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost	11.26	1.83	26.92	1.83	17.35	259.27	17.35	7.76	33.40	7.76	7.57	135.25	7.57
AhnLab V3 Internet Security	17.42	8.45	8.33	7.30	19.78	20.02	5.38	10.10	10.41	10.59	10.40	10.61	10.71
Antiy Ghostbusters	27.70	290.69	290.69	8.17	13.95	15.11	13.99	29.69	42.94	3.48	27.74	28.47	2.75
ArcaBit ArcaVir	6.77	3.59	8.63	3.59	19.55	19.55	36.22	17.68	18.79	17.68	13.04	13.04	13.04
AvailaSoft AS Anti-Virus	11.81	1.91	8.78	1.91	6.51	6.99	6.51	3.11	2.86	3.11	2.04	2.38	2.04
Avast Software avast! Free	27.90	181.68	223.61	12.16	37.89	37.04	34.94	20.21	19.71	18.08	24.59	24.04	18.34
Avertive VirusTect	15.10	5.57	5.67	NA	17.98	17.98	17.98	11.90	12.46	11.90	12.88	12.88	12.88
AVG Internet Security	26.92	4.90	2906.94	4.32	28.47	1642.04	28.98	13.90	267.17	12.02	6.33	216.40	5.06
Avira AntiVir Personal	18.42	5.61	5.59	5.61	42.84	42.84	42.84	17.05	16.47	17.05	16.39	15.03	16.39
Avira AntiVir Professional	19.95	5.47	5.53	5.47	40.05	39.73	40.05	19.87	19.55	19.87	17.45	17.45	17.45
BitDefender Antivirus Pro	8.69	5.61	5.55	5.61	24.88	25.93	24.88	9.81	11.40	9.81	11.15	11.39	11.15
Bkis BKAV Professional	10.43	61.85	72.67	NA	8.51	8.61	8.51	3.87	3.97	3.87	3.04	3.07	3.04
Bullguard Antivirus	32.63	8.23	2906.94	8.23	28.64	4926.11	28.64	13.58	801.50	13.58	13.04	541.00	13.04
CA Internet Security Suite Plus	23.77	1.87	2906.94	NA	37.89	1642.04	NA	14.40	400.75	NA	15.46	270.50	NA
CA Total Defense r12	17.04	145.35	1453.47	3.38	34.69	1642.04	32.41	19.71	300.56	17.55	16.39	216.40	14.82
Central Command Vexira	17.11	12.32	12.64	4.06	17.85	17.91	17.35	15.22	17.05	13.28	14.24	14.82	12.58
Check Point Zone Alarm	12.42	2.92	2.87	2.92	19.32	19.39	19.32	10.45	10.59	10.45	9.25	9.33	9.25
Clearsight Antivirus	18.51	5.78	5.72	NA	20.87	20.79	20.87	16.58	16.58	16.93	11.27	11.04	11.27
CommTouch Command	22.00	7.07	6.78	7.07	15.74	15.74	15.74	13.66	16.03	13.66	12.88	13.36	12.88
Comodo I.S. Premium	8.61	2.23	2.27	2.23	14.32	14.53	14.32	17.05	18.93	17.05	12.88	9.93	12.88
Coranti 2010	10.43	3.42	3.04	3.42	9.77	9.57	9.77	6.52	5.95	6.52	7.90	5.76	7.90
Defenx Security Suite	21.04	3.00	2906.94	3.00	33.06	1642.04	33.06	7.61	33.40	7.61	7.36	135.25	7.36
Digital Defender	17.26	5.43	5.58	NA	16.48	17.41	16.48	10.02	13.14	10.02	11.76	12.58	11.76
eEye Blink	3.00	1.00	0.99	NA	3.20	3.27	3.20	3.30	3.29	3.30	2.35	2.36	2.35
Emsisoft Anti-Malware	10.19	5.59	5.70	NA	7.59	7.61	7.59	4.95	5.00	4.95	4.19	4.24	4.19
eScan Internet Security	15.16	4.90	90.84	4.90	3.16	20.27	3.16	0.49	3.20	0.49	1.12	19.32	1.12
ESET NOD32	22.13	4.82	4.84	4.82	37.32	38.19	37.32	10.83	11.40	10.83	11.76	11.89	11.76
Filseclab Twister	11.56	1.62	1.62	1.52	23.24	23.57	19.86	7.03	7.05	6.20	5.30	5.33	5.23
Fortinet FortiClient	13.46	7.96	8.76	7.96	9.85	9.93	9.85	10.83	9.47	10.83	14.62	14.82	14.62
Frisk F-PROT	17.82	10.20	10.20	10.20	14.79	14.88	14.79	10.41	12.14	10.41	15.91	16.91	15.91
F-Secure Client Security	15.04	10.13	2906.94	9.08	20.44	4926.11	20.19	18.93	1202.25	17.94	54.10	1082.01	10.93
F-Secure Internet Security	27.50	10.49	2906.94	2.19	21.61	4926.11	19.09	19.39	1202.25	12.14	54.10	1082.01	10.50
G DATA AntiVirus 2011	16.31	3.94	2906.94	3.94	20.61	492.61	20.61	9.47	96.18	9.47	10.02	36.07	10.02
Hauri ViRobot Desktop	7.76	4.08	3.91	0.33	11.87	13.50	11.87	2.42	2.42	2.42	2.13	2.13	2.13
Ikarus T3 virus.utilities	18.33	30.28	30.28	NA	16.76	16.76	16.76	16.03	16.70	16.03	13.87	14.24	13.87

Please refer to text for full product names.

On-demand throughput contd. (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
iolo System Shield	17.58	8.43	8.43	8.43	15.99	15.99	15.99	13.00	14.84	13.00	15.46	16.15	15.46
K7 Total Security	17.99	8.31	8.21	8.31	11.48	11.54	11.48	11.84	15.12	11.84	12.73	14.62	12.73
Kaspersky Anti-Virus 6	40.10	6.67	2906.94	6.67	34.45	821.02	34.45	17.30	160.30	17.30	15.03	180.33	15.03
Kaspersky Internet Security	13.90	4.64	2906.94	4.64	22.29	703.73	22.29	4.85	218.59	4.85	14.82	180.33	14.82
Kaspersky PURE	17.19	6.47	2906.94	6.47	30.41	821.02	30.41	15.82	80.15	15.82	17.45	67.63	17.45
Keniu Antivirus	12.38	2.74	2.74	2.74	16.05	19.02	16.05	11.18	10.19	11.18	10.02	8.87	10.02
Keyguard Antivirus	14.86	5.63	5.64	NA	20.70	20.87	20.70	15.72	16.58	15.72	10.71	11.15	10.71
Kingsoft I.S. 2011 Advanced	11.29	2.48	2.48	2.48	29.50	31.58	29.50	8.71	9.14	8.71	12.44	17.17	12.44
Kingsoft I.S. 2011 Standard-A	13.85	2.53	2.51	2.53	31.78	31.18	31.78	9.07	8.94	9.07	14.24	12.88	14.24
Kingsoft I.S. 2011 Standard-B	9.25	2.64	2.63	2.64	24.39	24.15	24.39	7.11	7.42	7.11	16.15	16.39	16.15
Lavasoft Ad-Aware TS	26.19	4.02	2906.94	4.02	15.69	492.61	15.69	9.62	104.54	9.62	6.44	541.00	6.44
Logic Ocean GProtect	17.58	4.09	5.58	NA	17.98	17.85	17.98	14.06	13.82	14.06	11.76	12.73	11.76
McAfee VirusScan Enterprise	13.80	26.19	322.99	26.19	41.05	307.88	41.05	22.68	120.23	22.68	23.02	135.25	23.02
Microsoft Forefront	9.75	3.96	4.02	3.96	14.49	14.40	14.49	15.51	16.14	15.51	12.44	12.73	12.44
Nifty Corp. Security 24	26.01	3.90	100.24	3.90	20.36	328.41	20.36	8.07	55.92	8.07	5.79	41.62	5.79
Norman Security Suite	2.91	1.28	1.27	1.28	4.53	5.10	4.53	5.45	5.53	5.45	3.40	3.50	3.40
Optenet Security Suite	14.00	2.96	9.38	2.96	15.54	31.18	15.54	7.22	11.34	7.22	7.67	13.04	7.67
PC Booster AV Booster	14.26	5.67	5.72	NA	17.10	17.10	17.10	11.50	12.21	11.50	11.89	11.89	11.89
PC Renew I.S 2011	15.04	5.30	5.26	NA	18.04	18.04	18.04	11.18	11.62	11.18	12.30	12.30	12.30
PC Tools I.S. 2011	18.42	2.79	581.39	1.26	17.66	259.27	17.66	6.93	68.70	6.93	4.87	43.28	4.87
PC Tools Spyware Doctor	28.52	2.71	968.98	1.23	14.84	273.67	14.84	6.85	55.92	6.85	5.79	49.18	3.08
Preventon Antivirus	18.60	5.12	5.24	5.12	16.42	16.53	16.42	10.69	11.29	10.69	11.89	12.02	11.89
Qihoo 360 Antivirus	11.49	1.91	2.67	1.91	16.48	19.17	16.48	8.53	9.36	8.53	7.46	8.07	7.46
Quick Heal Total Security 2011	18.60	2.45	2.44	2.46	41.75	41.75	42.10	10.45	9.01	9.81	10.82	9.41	9.93
Returnil System Safe 2011	14.53	3.92	3.87	3.92	11.40	11.38	11.40	3.01	3.05	3.01	7.31	7.46	7.31
Sofscan Professional	4.87	11.14	11.40	3.72	14.70	14.88	14.97	12.66	14.31	9.81	10.50	11.04	10.50
Sophos Endpoint Security	22.38	100.24	103.82	1.48	17.98	18.52	16.70	18.35	21.86	19.87	13.53	14.24	12.44
SPAMfighter VIRUSfighter	16.74	5.43	5.47	NA	17.72	17.78	17.72	13.74	13.74	13.74	12.58	10.40	12.58
GFI/Sunbelt VIPRE	13.01	3.12	3.11	3.12	21.99	24.03	21.99	1.87	1.87	1.87	2.03	2.03	2.03
Symantec Endpoint Protection	17.50	2.50	2.42	2.43	26.06	26.20	26.06	12.27	12.66	12.52	8.07	8.14	8.01
Trustport Antivirus 2011	6.28	1.79	1.81	1.79	13.00	13.92	13.00	6.79	7.05	6.79	5.76	6.01	5.76
UnThreat Antivirus Professional	13.28	3.14	3.12	3.14	15.35	15.35	15.35	1.06	1.07	1.06	3.99	3.96	3.99
VirusBuster Professional	11.96	4.02	3.81	4.02	16.05	15.54	16.05	11.84	11.29	11.84	12.73	11.39	12.73
Webroot IS Complete	10.72	1.39	4.14	0.84	16.76	289.77	16.76	25.05	160.30	25.05	12.16	67.63	12.16

Please refer to text for full product names.



Please refer to text for full product names.

of keeping all scores above 90%. The WildList caused no difficulties, and without a single alert in any of the clean sets *BitDefender* proves well worthy of a VB100 award. The company has a respectable record of seven passes and two fails in the last two years, with three comparatives not entered; four of the last six tests have been passed, from five entries.

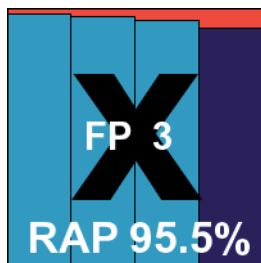
Bkis BKAV Professional Internet Security 3245

Definition version 3245; engine version 3.5.6; pattern codes 3.337.949

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.48%
Worms & bots	99.59%	False positives	3

Bkis first appeared on the *VB* radar around a year ago, and has rapidly gone from a fairly rocky start to achieving several VB100 awards and some superb scores in recent months.

The company's current '*Pro*' product came as a 212MB install package, with no need for further updates. The installation process was remarkably

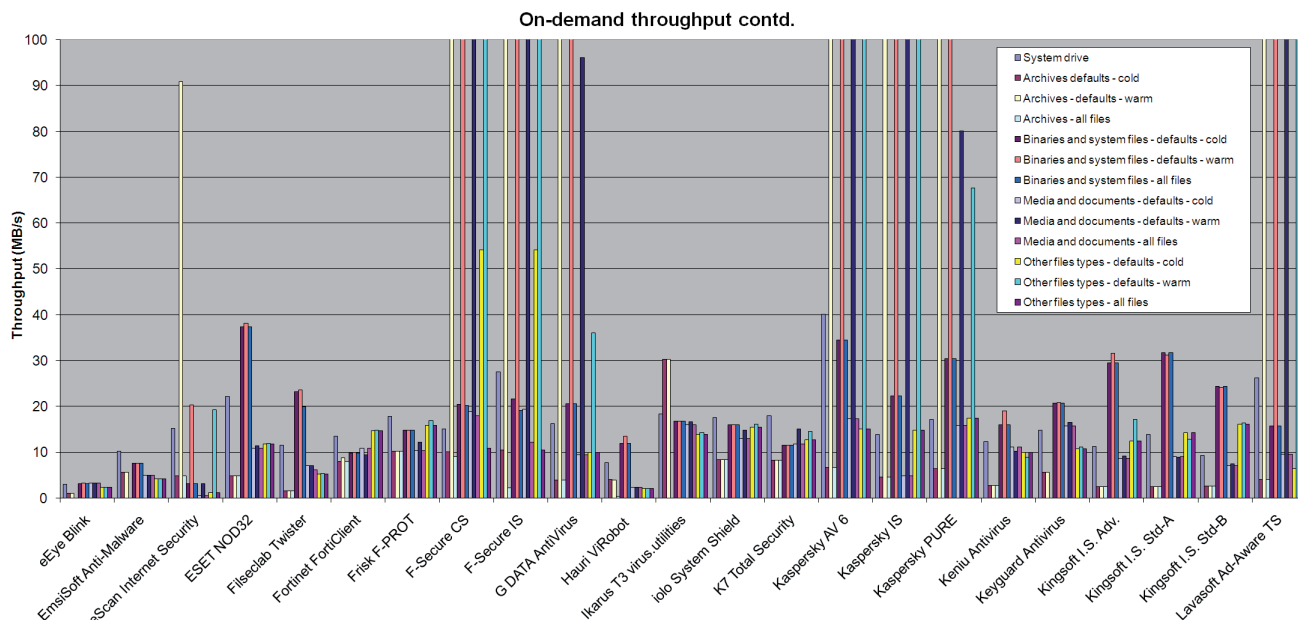


rapid, with only one step covering the install location and creation of desktop shortcuts. A reboot was needed after the fast copy process, but nevertheless the whole thing was completed in excellent time.

The interface is a hot and fruity orange colour, and provides fairly simple access to a reasonable level of options covering the basic requirements but not much more. As in recent tests, stability was excellent, with no problems even under the heaviest strain, and despite rather sluggish scanning times all tests completed within 24 hours as hoped.

On-access lag times were fairly heavy, and scanning speeds not too zippy except in the archive set where things were not being probed too deeply. While RAM usage was fairly low, and impact on our suite of activities similarly good, CPU use when busy was pretty high.

Detection rates were once again excellent, with stunning scores across the sets. Guessing from the rapid improvements since earlier entries however, it seems likely that heuristic strength has been tweaked upwards to improve scores, and at last this seems to have gone a step too far, with a handful of false alarms generated in our clean sets, including components of a common freeware file compression tool and an obscure part of *Microsoft Office*. *Bkis* thus misses out on a VB100 award this month, despite an impressive performance; the *Pro* edition had passed all three of its previous entries in the last year.



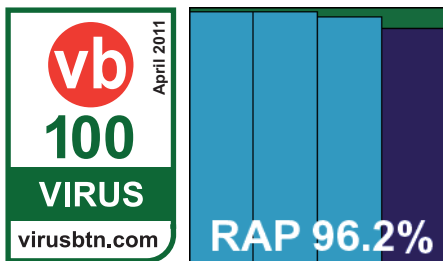
Please refer to text for full product names.

* Some values exceed chart area

Bullguard Antivirus 10.0.172

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.07%
Worms & bots	99.63%	False positives	0

Bullguard is an occasional to semi-regular participant in our testing, with its iconoclastic approach to interface design and general reliability making the product a welcome sight on any roster of submissions.



The latest edition came in as a 137MB install package, with no further updates needed, and ran through in very rapid time, with just a couple of clicks required. The whole thing was done within a minute, with no reboot needed.

The GUI design is somewhat on the wacky side, somehow blending cool and functional with warm and friendly, but after a little exploration it proved perfectly usable. Large buttons lead to an unexpected selection of main areas, with asymmetry another odd addition to the mix. Controls are

fairly plentiful however, once dug out, and stability was excellent. Logging was in a rather gnarly XML format – nice for displaying to the user, but awkward to process with our standard scripts. However, some smart result caching meant that many tests powered through in excellent time and the full test suite was completed in under a day.

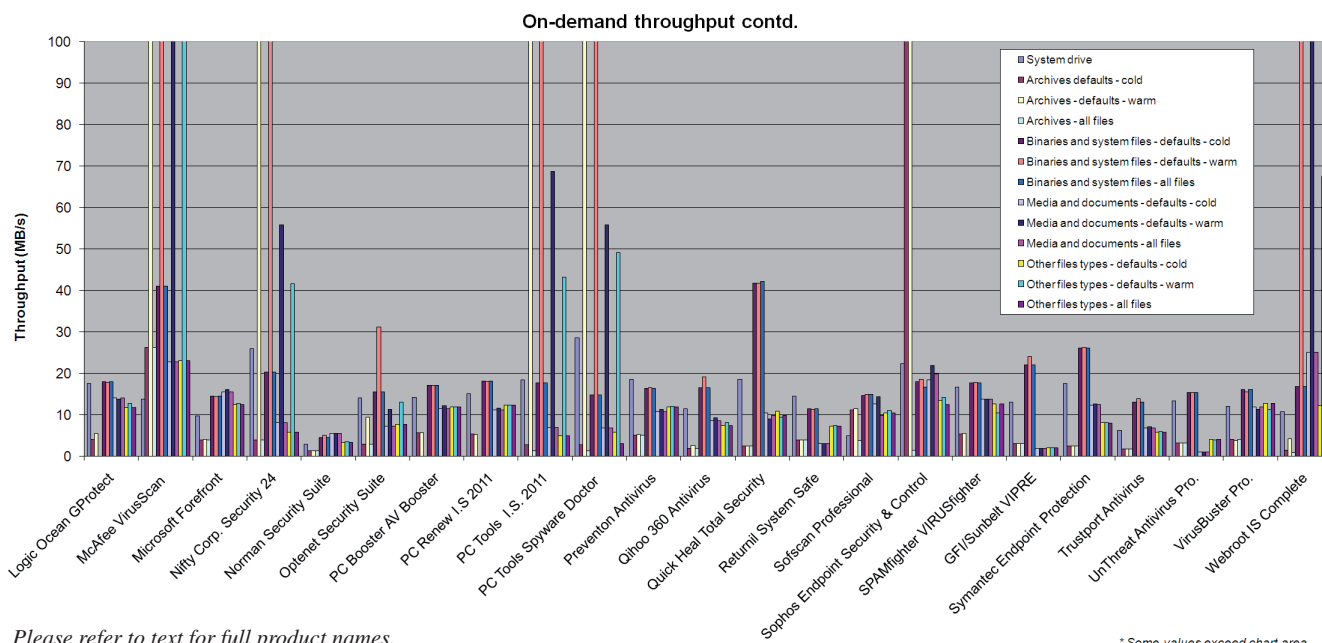
Scanning speeds were quite good, and on-access lags a little heavy at first but much quicker once the product had familiarized itself with things. RAM use was higher than most, but CPU use was very low, and impact on our activities was quite low too.

Detection rates were superb, with only the slightest decrease through the reactive weeks of the RAP sets, and the proactive week achieving the enviable heights of more than 90%. The WildList and clean sets caused no problems, and a VB100 award is duly earned; Bullguard now has four passes from four entries in the last two years, having skipped the other eight tests, with two of those passes coming in the last six tests.

CA Internet Security Suite Plus 7.0.0.115

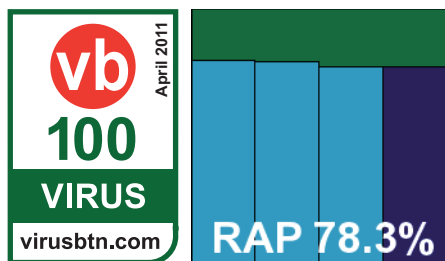
AM SDK version 1.4.1.1512; signature file version 4209.0.0.0

ItW	100.00%	Polymorphic	99.96%
ItW (o/a)	100.00%	Trojans	80.18%
Worms & bots	96.96%	False positives	0



Please refer to text for full product names.

CA's project to outsource the bulk of the work on its anti-malware solutions seems to be more or less complete, with the release



of the fully reworked corporate product. The consumer version, *ISS+*, has become a familiar sight in recent tests, and has presented few major headaches to the test team.

As usual, installation was performed online at the request of the submitters. The main installer weighed in at 154MB, and online updating took a few minutes. The rest of the set-up process was fairly brisk and straightforward, and could be dealt with within a few minutes with little effort.

The interface is snazzy and stylish, if a little baffling at times; there are several components, including firewalling, intrusion prevention and parental controls, but the configuration is scattered and often less than clear. Stability seems fine though, with no crashes or hangs at usual levels of pressure. When running the seriously strenuous tests for our malware detection measures though, some cracks began to show. Like several others of late, the developers seem to have decided that it would be a good idea to store all

detection results in memory, only writing out to file at the end of a scan. Presumably, in everyday usage there is some marginal performance gain from this approach, although it seems unlikely to be much given the size of most real-world results logs. In a testing environment this almost invariably causes problems. On this occasion scans began at a lightning pace (as we have come to expect from the excellent engine underlying the CA product range), but steadily grew slower and slower as RAM was eaten up with gusto. A first attempt at scanning the main test sets only (without even the RAP sets) ran for 18 hours and was consuming over 500MB of RAM before it froze out, leaving us with no option but to reboot the machine and abandon all the data not saved to disk. Scans were run in smaller chunks, each one carefully measured to hit the happy zone where speed hadn't slowed down too much and crashes were unlikely.

As a result of the extra work and time involved in running over 20 jobs in place of one, testing took rather more than the 24 hours we had allocated each product; although not too much more thanks to good speeds in the on-access run over the infected set.

Thanks to smart caching of results over the clean sets, scanning speeds went from good in the cold measures to excellent in the warm, while file access lag times were not bad either. In the performances measures we saw a fairly low addition to our activities' run time, while CPU and RAM use were both fairly high.

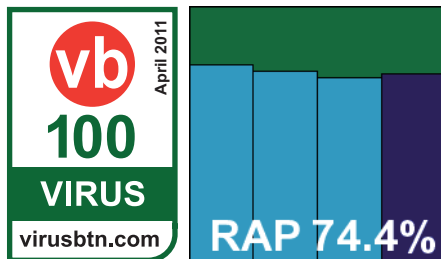
Detection rates were fairly respectable in general, with impressive reliability in the trojans and RAP sets – the team behind the detection part of the product seem to be maintaining things quite nicely. A single item of adware was identified in the clean set, and there were no problems in the WildList, earning CA a VB100 award for its consumer product. The solution has been having a rather tough time of late, with only two passes from six attempts in the last two years; this is the first pass in the last six tests, three of which were not entered – hopefully this will mark the start of a new chapter for CA.

CA Total Defense r12 Endpoint Protection Client

Product version 12.0.528; signature version 4209

ItW	100.00%	Polymorphic	99.96%
ItW (o/a)	100.00%	Trojans	78.26%
Worms & bots	96.06%	False positives	0

CA's business solution has had a major revamp, which we were first exposed to in the last *Windows* comparative in late 2010 (see



VB, December 2010, p.27). This was not the most pleasant experience, and we hoped a degree of familiarity would help things along this month.

With the installer package recycled from the previous encounter, there was fortunately no need to repeat the lengthy process of downloading the 4GB DVD iso image we were asked to use. The time saved in avoiding this chore was quickly used up though, as the install requested on the deadline day revealed that the product cannot be installed on *Windows XP* from the package provided. Instead, it must be set up on a supported platform (*Windows 7* or a recent server edition) and deployed from there. In great haste (as we needed to run an online update before the deadline day expired), a precious machine was taken away from its usual duties and set up with *Windows 7*. Installing the management system is a rather complex process with a number of dependencies, a guide tool helping by listing those not yet met. These included the ISS system, *Flash Player* for the interface, and some changes to the firewall, as well as the local password which didn't come up to the product's safety standards. With the system installed we then faced further hurdles with the licensing

scheme, which appears to need 2 a.m. to pass before it accepts new licences, and then running updates, which proved rather baffling and was not helped by the progress window being hidden in some kind of secured zone, having been reported as 'not fully compatible with *Windows*'. We finally managed to get the latest definitions in place just as the deadline came to an end.

Next day, safely isolated from further updates, we tried deploying to the machine which would be used for the test proper, having navigated the pretty, but not entirely intuitive management interface in what we hoped was the right way. A discovery job found our test machines readily enough, but try as we might, remote installation seemed unwilling to run. Urgently requesting help from the submitters we were put in touch with a support operative, who promised some details of changes to the WMI system which might help, but when no further advice was forthcoming we resorted to further experimentation. As usual in such circumstances, *Google* was our friend, leading us to the murky world of CA user forums. Here we learned that a simple install bundle, including all required updates etc., can easily be created on the management system and copied over to clients manually (perhaps it would have been easier had the original submission been provided in this format).

With this figured out, the install actually proved rather simple, with the standard half-dozen steps of any normal installer and a reboot at the end. All this was complete in under a minute – albeit more than two days after first starting the process. The client interface is clean and crisp, a huge improvement over the previous edition, with a good range of options laid out in a simple and accessible manner. Despite the *Flash* underpinnings, it seemed stable and responsive at all times, and with the zippy scanning engine under the hood it made short work of most of our tests.

Again, scanning speeds were quite good and file access lag times light, but the performance measures showed quite a lot of RAM usage, a fairly heavy impact on our activities suite and a massive amount of CPU use. These figures looked so out of place when compiling the final graphs that we re-ran the tests to confirm them, but got almost identical results on a second run through.

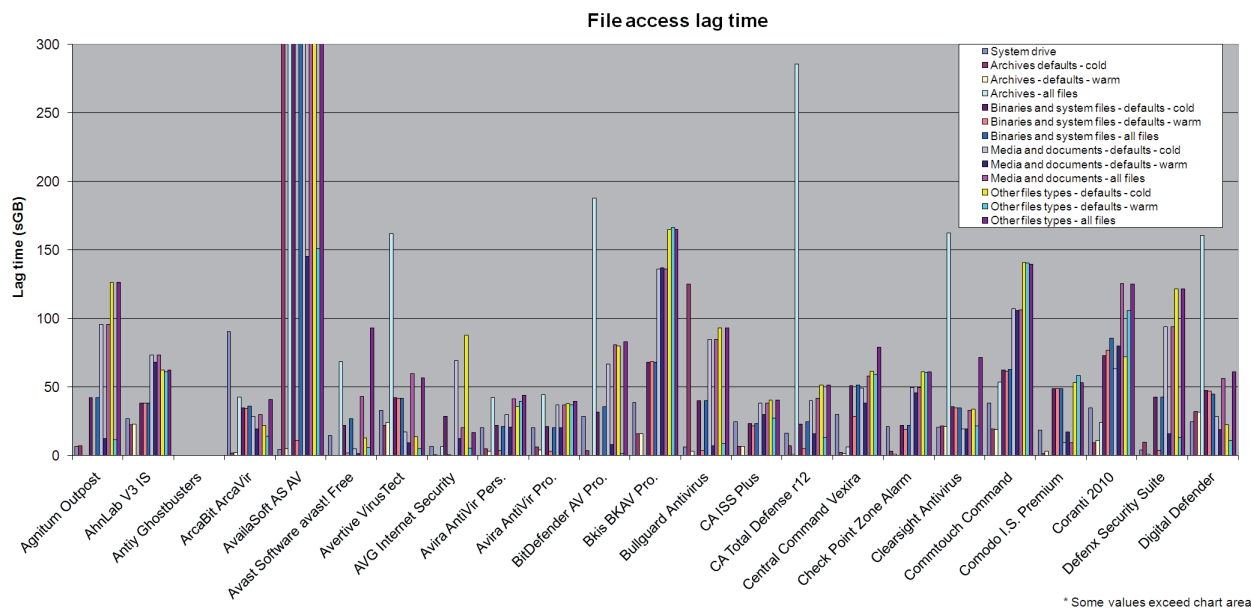
In the infected sets things were also a little problematic. Although the on-access run went by in a flash, on-demand scans were once again hampered by the storage of all data in memory, the overworked test system slowly grinding to a halt as its resources were eaten up. One attempt at running the standard scan of the full sets froze up with more than 1GB of memory taken up. Resorting once more to running multiple smaller jobs, and ripping results out of the raw SQL database files created at the end of each scan, we finally got the required data, which

File access lag time (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost	6.44	6.85	0.01	NA	42.01	0.01	42.01	95.85	12.34	95.85	126.18	11.42	126.18
AhnLab V3 IS	26.87	22.55	22.76	NA	38.34	38.31	38.34	73.25	67.78	73.25	62.09	60.86	62.09
Antiy Ghostbusters	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
ArcaBit ArcaVir	90.39	1.67	2.01	42.57	34.73	34.40	36.13	28.62	19.30	29.92	22.05	13.96	40.88
AvailaSoft AS Anti-Virus	4.37	519.73	4.65	519.73	792.72	10.79	792.72	5091.26	145.16	5091.26	5812.35	150.91	5812.35
Avast Software avast! Free	14.67	0.04	0.01	68.66	21.72	1.90	26.58	4.67	1.37	43.06	12.74	5.56	92.90
Avertive VirusTect	32.81	22.05	24.18	161.95	41.93	41.83	41.85	17.13	9.13	59.59	13.67	4.65	56.38
AVG Internet Security	6.37	0.36	0.01	6.52	28.38	0.49	-0.46	69.16	12.26	20.21	87.61	5.29	16.59
Avira AntiVir Personal	20.04	4.91	3.14	42.09	22.02	3.72	20.87	29.92	20.64	41.25	35.64	39.44	44.09
Avira AntiVir Professional	20.36	6.37	3.88	44.30	20.84	2.92	20.30	36.85	20.38	36.75	37.66	36.90	39.63
BitDefender Antivirus Pro	28.33	3.61	0.01	188.07	31.42	0.01	35.68	66.54	8.02	80.65	79.65	1.15	82.89
Bkis BKAV Professional	38.53	15.64	15.83	NA	67.84	68.30	67.84	135.87	136.68	135.87	164.83	166.38	164.83
Bullguard Antivirus	6.26	125.04	2.92	NA	39.74	3.44	39.74	84.70	6.97	84.70	93.10	8.71	93.10
CA ISS Plus	24.76	6.76	6.51	NA	23.37	21.47	23.37	38.06	29.94	38.06	40.52	27.06	40.52
CA Total Defense r12	16.26	7.25	0.83	285.70	22.80	4.98	24.55	39.81	15.87	41.60	51.18	12.99	51.29
Central Command Vexira	29.76	2.07	1.52	6.35	51.01	28.64	51.39	49.16	38.00	58.01	61.60	59.28	78.89
Check Point Zone Alarm	21.17	3.11	0.79	NA	22.10	18.87	22.10	49.66	45.49	49.66	60.94	60.36	60.94
Clearsight Antivirus	20.76	21.59	21.17	162.25	35.32	34.45	34.45	19.30	19.23	33.02	33.86	21.70	71.68
Commtouch Command	38.17	19.57	18.88	53.35	62.32	61.43	62.90	106.85	105.62	105.99	140.81	140.34	139.44
Comodo I.S. Premium	18.57	1.14	3.02	NA	48.73	48.60	48.73	9.26	17.05	9.26	53.06	58.50	53.06
Coranti 2010	34.79	9.45	10.77	23.96	72.83	76.95	85.40	63.28	79.81	125.43	71.94	105.53	125.19
Defenx Security Suite	4.08	9.56	0.84	NA	42.53	3.42	42.53	93.68	15.60	93.68	121.49	13.35	121.49
Digital Defender	24.40	32.21	31.64	160.71	47.41	47.11	44.67	28.47	18.79	56.17	22.41	10.81	60.91
eEye Blink	50.95	18.80	17.45	745.72	95.33	83.41	101.03	276.88	273.68	275.57	364.57	361.37	364.70
Emsisoft Anti-Malware	2.98	1.41	0.65	NA	14.47	3.34	14.47	5.89	5.33	5.89	6.05	8.04	6.05
eScan Internet Security	5.41	0.09	0.01	42.33	0.87	0.01	25.31	20.88	10.06	45.49	11.54	3.06	71.32
ESET NOD32	5.14	0.13	0.08	NA	15.06	2.55	15.06	64.73	24.52	64.73	56.68	23.25	56.68
Filseclab Twister	24.38	5.28	2.98	NA	20.57	17.24	NA	94.92	86.35	NA	18.14	4.81	NA
Fortinet FortiClient	28.69	99.19	0.01	NA	81.98	0.02	81.98	38.81	1.45	38.81	58.53	3.60	58.53
Frisk F-PROT	17.90	5.36	5.11	NA	48.75	46.84	48.75	25.86	13.84	25.86	26.79	23.45	26.79
F-Secure Client Security	16.89	5.18	7.61	NA	50.92	2.61	NA	69.19	6.73	NA	26.37	5.90	NA
F-Secure Internet Security	12.07	7.96	6.94	NA	50.52	2.75	NA	69.24	6.71	NA	25.80	7.04	NA
G DATA AntiVirus 2011	13.76	48.21	9.36	411.30	58.86	4.89	73.65	102.09	25.77	219.72	133.13	17.48	186.37
Hauri ViRobot Desktop	68.20	4.34	20.87	12.67	77.30	81.38	82.78	181.23	190.86	249.95	47.57	40.04	444.47
Ikarus T3 virus.utilities	22.91	25.98	25.81	22.62	43.04	42.56	42.40	22.48	21.55	20.66	39.47	38.24	37.53

Please refer to text for full product names.

File access lag time contd. (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
iolo System Shield	38.80	51.53	51.73	38.80	63.64	63.49	63.64	107.18	106.77	107.18	140.87	139.85	140.87
K7 Total Security	12.28	24.04	8.69	12.28	72.58	4.28	72.58	46.75	19.20	46.75	42.56	8.63	42.56
Kaspersky Anti-Virus 6	13.11	4.15	2.38	95.06	2.46	3.43	10.06	1.57	8.52	54.30	1.37	6.76	73.19
Kaspersky Internet Security	1.89	5.34	3.94	25.49	32.70	13.53	47.99	60.81	26.13	97.29	91.67	35.37	102.60
Kaspersky PURE	5.37	12.92	12.27	329.80	35.04	4.37	37.86	72.92	22.62	67.18	94.89	11.38	76.69
Keniu Antivirus	31.73	4.11	6.86	5.88	33.73	33.90	34.73	56.24	55.14	57.48	76.48	75.78	75.63
Keyguard Antivirus	32.19	23.38	23.37	161.74	45.17	45.30	45.15	19.66	12.61	51.02	22.02	15.62	58.25
Kingsoft I.S. 2011 Adv.	5.52	1.09	0.27	NA	15.60	3.00	15.60	76.48	2.20	76.48	51.38	13.20	51.38
Kingsoft I.S. 2011 Std-A	4.81	1.97	0.39	NA	14.28	3.60	14.28	76.40	3.57	76.40	48.84	12.38	48.84
Kingsoft I.S. 2011 Std-B	12.23	2.19	0.46	NA	24.27	3.68	24.27	106.15	8.27	106.15	37.24	5.27	37.24
Lavasoft Ad-Aware TS	11.51	34.84	1.21	34.84	40.70	0.01	40.70	72.41	0.01	72.41	142.50	29.14	142.50
Logic Ocean GProtect	25.88	26.42	25.78	163.32	44.77	44.76	44.66	10.97	3.27	56.50	16.09	7.04	59.80
McAfee VirusScan	5.58	2.66	0.33	439.91	53.68	3.23	53.98	99.23	6.24	90.25	129.01	9.09	129.81
Microsoft Forefront	16.89	1.63	0.01	NA	56.67	0.01	56.67	25.69	0.93	25.69	50.93	1.25	50.93
Nifty Corp. Security 24	1.93	14.83	0.26	NA	35.31	1.23	35.31	80.93	0.98	80.93	134.49	27.61	134.49
Norman Security Suite	46.23	3.05	2.95	NA	87.74	79.48	87.74	242.61	241.33	242.61	376.96	374.82	376.96
Optenet Security Suite	16.53	26.27	8.82	NA	47.53	5.18	47.53	89.19	23.89	89.19	100.62	9.59	100.62
PC Booster AV Booster	34.57	21.32	21.44	161.25	44.52	44.88	44.30	1.06	3.00	53.05	7.97	8.49	61.88
PC Renew I.S 2011	32.90	24.19	23.04	161.53	40.17	42.10	41.75	3.57	14.33	56.06	0.94	7.76	55.83
PC Tools I.S. 2011	9.55	1.91	1.71	NA	4.15	2.87	NA	74.30	69.15	NA	118.62	119.81	NA
PC Tools Spyware Doctor	28.43	1.78	1.70	NA	17.88	14.99	NA	96.27	85.51	NA	113.62	108.05	NA
Preventon Antivirus	24.14	32.98	33.35	169.70	46.68	46.57	47.48	30.87	18.71	75.94	21.56	11.81	63.34
Qihoo 360 Antivirus	60.17	3.96	7.54	4.34	10.96	7.13	4.53	17.99	20.57	31.73	29.52	11.38	14.27
Quick Heal TS 2011	11.33	33.54	33.92	33.87	17.92	16.70	15.92	72.21	70.68	67.61	68.30	67.85	65.20
Returnil System Safe 2011	21.03	33.11	31.94	NA	53.09	54.35	53.09	137.75	149.56	137.75	55.63	55.79	55.63
Sofscan Professional	35.76	12.27	12.67	637.64	67.33	67.35	49.81	30.65	39.81	49.21	51.48	53.68	63.97
Sophos Endpoint Security	26.32	12.27	12.67	637.64	67.33	67.35	49.81	30.65	39.81	49.21	51.48	53.68	63.97
SPAMfighter VIRUSfighter	27.95	24.52	24.95	107.70	44.92	44.97	44.66	11.19	3.37	56.66	15.12	7.07	59.75
GFI/Sunbelt VIPRE	16.51	4.59	4.58	NA	30.81	11.68	30.81	437.85	9.83	437.85	357.61	16.18	357.61
Symantec EP	15.55	1.68	1.51	NA	42.56	41.57	42.56	40.55	34.70	40.55	73.84	62.14	73.84
Trustport Antivirus 2011	25.19	15.27	1.89	796.28	95.40	9.67	108.79	122.74	37.58	160.52	194.21	14.66	237.03
UnThreat Antivirus Pro	8.54	10.76	10.75	NA	33.45	10.28	33.45	450.01	25.37	450.01	351.62	18.60	351.62
VirusBuster Professional	28.30	2.90	0.01	NA	48.09	28.37	48.09	47.81	41.46	47.81	59.38	56.60	59.38
Webroot IS Complete	51.51	0.03	0.01	NA	4.91	2.89	4.91	23.03	21.09	23.03	16.06	16.12	16.06

Please refer to text for full product names.



Please refer to text for full product names.

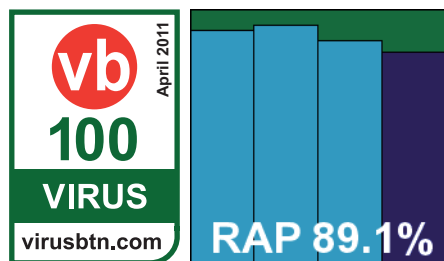
showed some perfectly respectable scores, with admirable consistency across the RAP sets. The WildList and clean sets were well handled, and a VB100 award could finally be granted, after several days of hard work. Over the longer term, CA's business solutions have a rather better record than its consumer ones, with seven passes and three fails in the last two years, two tests having been skipped; the last six tests show two passes, two fails and two no-entries.

Central Command Vexira Antivirus Professional 7.1.38

Virus scan engine 5.2.0; virus database 13.6.217

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.90%
Worms & bots	97.01%	False positives	0

Vexira has become a regular participant in our tests over the last few years, since starting up a highly successful partnership with the ubiquitous *VirusBuster*.

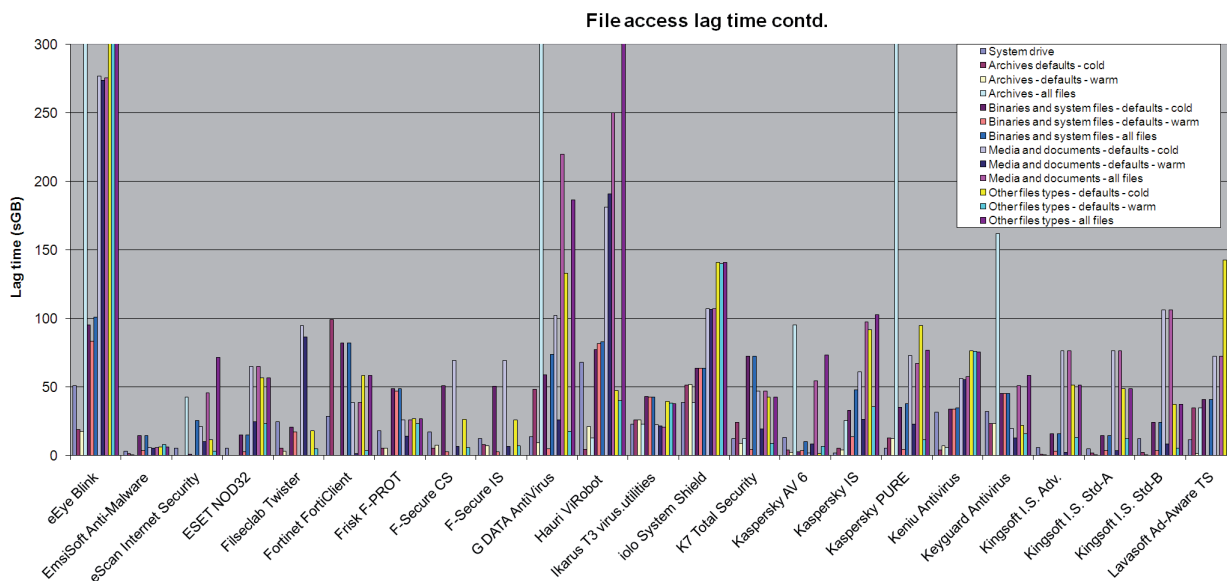


The installer submitted measured 65MB, with an additional 69MB archive of updates to add in. The set-up process included all the usual steps, split over rather more stages than most, with the option to join a feedback system rather deviously hidden on the same screen as the EULA and checked by default. Running through it all took less than a minute though, with the final screen somewhat confusingly reaching completion and leaving a progress bar at around 70% of the way across. No reboot was needed to complete the process, but we restarted anyway after the manual application of updates, just to be safe.

The interface is very familiar after dozens of appearances on the test bench in recent years, enlivened somewhat by Vexira's gaudy red colour scheme. The layout is a little unusual but generally usable once one has got to know its quirks. However, a scheduler system proved beyond our limited powers, failing to run as we had apparently failed to properly set the user/password settings – ideally this would be checked by the product before accepting the job. Despite this minor setback, things mostly went smoothly and there were no issues with stability.

Scanning speeds were not super fast but on-access lags seemed OK, with impressively low measures in all of our performance drain tests.

With everything looking set to be completed comfortably inside the allocated time slot – the on-access run over the main sets taking somewhat longer than average but not too much – the on-demand scan threw a heavy and ugly



Please refer to text for full product names.

* Some values exceed chart area

spanner in the works. Having been a popular product with the test team for several years, the developers have flung themselves firmly into our bad books by leaping headfirst onto the bandwagon of storing detection data in memory rather than writing it to a proper log file incrementally; this meant yet more agonizing waiting, watching RAM consumption steadily rise, with no certainty that results would be safe until all was complete. The full job did, in fact, run without incident, but took just over 56 hours – considerably more than the five or six we would have expected of this product in its previous iterations.

Having survived this trial, results were decent, with good scores in general and a stronger than usual showing in the RAP sets. The WildList and clean sets caused no problems, and a VB100 award is granted despite our grumblings. Since reappearing on our radar just over a year ago, *Central Command* has achieved an excellent record of seven passes in the last seven tests.

Check Point Zone Alarm Security Suite 9.3.037.000

Anti-virus engine version: 8.0.2.48; anti-virus signature DAT file version: 1045962880

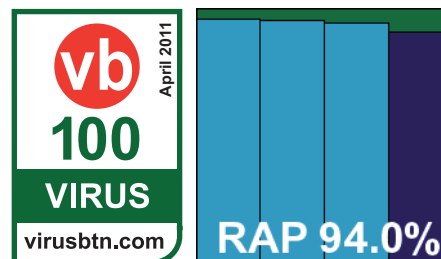
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	92.68%
Worms & bots	99.17%	False positives	0

Check Point's *Zone Alarm* is a bit of a classic name in security, the free firewall offering having been a common sight for many

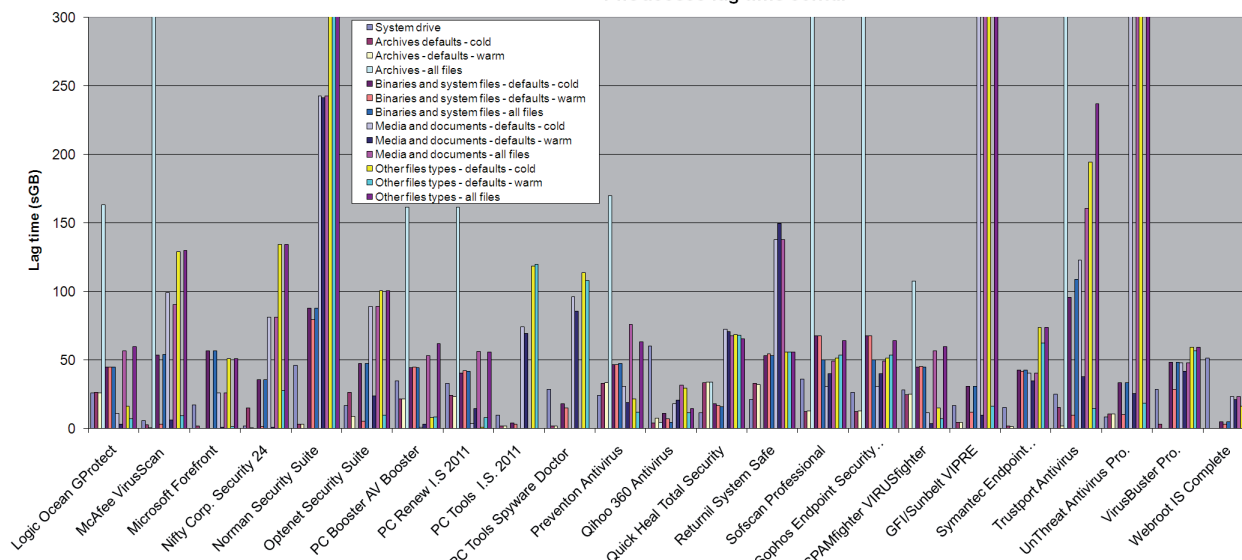
years. The premium suite version – with anti-malware based on the solid *Kaspersky* engine – has been around a good while too, and has been a regular, if infrequent, participant in our comparatives for several years.

The current version came as a 148MB installer, with 81MB of updates provided separately. The set-up process includes the option to install a browser toolbar, subscription to an email newsletter, and the option to disable protection after install, for those users installing in conjunction with another anti-malware product. A reboot is needed to complete the process.

The interface is plain and unfussy, with small icons and lots of text. The suite includes the firewall, of course, as well as 'Program control', mail and identity protection, and parental control modules, as well as the anti-malware component. Operation is a little fiddly and unintuitive in places, but generally usable, with a good level of options. Stability was good with no issues in any of the tests, and everything was done within less than a day.



File access lag time contd.



* Some values exceed chart area

Please refer to text for full product names.

Scanning speeds were fairly slow, but lag times were quite light, and while RAM use was around average and additional time taken to perform our set of tasks fairly insignificant, CPU use when busy was sky high – a result confirmed by a repeat run of the full set of measures.

Detection rates were excellent, with rock-solid scores in the RAP sets; on-access scores in the main sets seemed oddly lower than on demand, but the WildList was handled fine in both modes, and there were no problems in the clean sets either, earning *Check Point* another VB100 award. The company’s infrequent submission pattern, generally only targeting our annual XP test, means only two passes and one fail in the last 12 tests, with the rest not entered.

Clearsight Antivirus 2.1.48

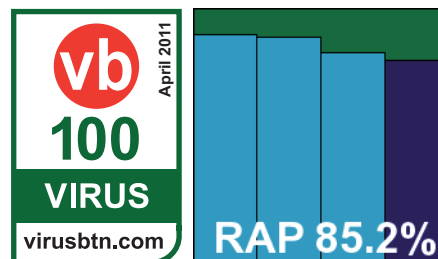
Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Another in the family of solutions based on the *Prevention* SDK and *VirusBuster* engine, *Clearsight* returns for only its second attempt at VB100 certification, having been denied it last time thanks to a minor technicality in what was clearly a solid product.

The latest version, as expected, was supplied fully updated in a 67MB installer. Setting up followed a simple pattern

of welcome screen, EULA, install location, go, with no reboot needed. An Internet connection was required to activate the product and access full controls, but all was over in under a minute.



The interface is highly familiar by now, this version being in a cool blue-and-white colour scheme. Its clear and simple operation made it easy to use and test – the only extra task being a registry tweak to enable full logging. Stability was not an issue even under heavy strain, and the tests took just about the full 24 hours allotted.

Scanning speeds closely mirrored those of others from this range, being a little slower than average over most types of files, but not too much. On-access lag times were around average and performance measures showed low use of resources and minimal impact on activities.

Detection results were also no big surprise, with solid scores averaging around the 90% mark, with a slight decline towards the more recent parts of the RAP sets. The WildList and clean sets were handled nicely, and *Clearsight* earns its first VB100 certification on its second attempt.

Commtouch Command Anti-malware 5.1.10

Engine version: 5.2.12; DAT file ID: 201102232246

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	78.39%
Worms & bots	87.12%	False positives	0

The *Command* product name has a long history in VB100 testing, dating all the way back to 1998. The company name may have

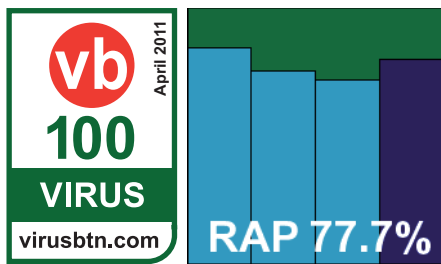
changed with the acquisition of *Authentium* by *Commtouch*, but not much seems to have changed in the product itself.

The installer is an ultra-compact 12MB, with only 28MB extra by way of updates. The installation process is pretty simple – although it includes an option to detect ‘potentially unwanted’ items – and needs no reboot to complete. The product interface is similarly abrupt and to the point, with a stark simplicity and minimal configuration, but it manages to get the job done effectively. The solution has a ‘cloud’ component, which had to be disabled for the purposes of the main test suite.

A few problems were encountered during the running of the tests, with several blue screens observed when under heavy pressure. This, along with a tendency to lose or overwrite logs, held us back a little; indeed, even when logging seemed to have run happily, the process of opening the logs and exporting in the main interface regularly took so long that we gave up on it. All log data is stored in *Access* database format – clearly not the most efficient choice as even the most basic log with only a handful of detections recorded could take several minutes to convert into a displayable format. For the most part, we took the raw database files and ripped the data out ourselves. With these issues slowing us down, testing took perhaps 36 hours – not too troublesome.

Scanning speeds were on the slow side, with file access lag times fairly high, and although RAM usage was perhaps just a fraction above average, CPU use was fairly high too. Impact on our set of standard jobs was around average for the month though.

Detection rates, when full results were finally gathered and analysed, proved respectable, with an interesting upturn in the last week of the RAP sets. A couple of items in the clean sets were alerted on as packed with *Themida*, while



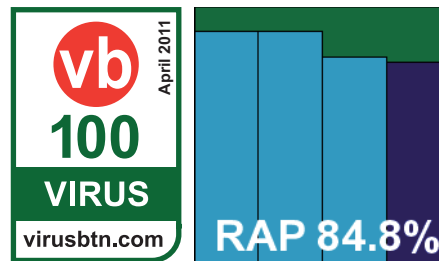
another was labelled adware, but there were no problems and the WildList was handled smoothly too. A VB100 is duly earned, improving *Command*'s record to three passes and three fails in the last 12 tests, with six tests not entered.

Comodo Internet Security Premium 5.3.176757.1236

Virus signature database version: 7793

ItW	100.00%	Polymorphic	90.63%
ItW (o/a)	100.00%	Trojans	92.23%
Worms & bots	96.03%	False positives	0

Comodo is a relative newcomer to our comparatives, although the company and the product have been around for some time.



The company's top-of-the-line suite solution came as a 34MB installer, but required full online updating on the deadline day. The set-up process was rather lengthy, partly because it included an extra component called ‘Geek Buddy’ – a support and troubleshooting system covering all aspects of the computer, with live chat and remote control by support staff. Once the initial install and required reboot were out of the way, this component had its own separate update process, which seemed to require a full re-download and re-install, just moments after the initial one. Then another update process began... Eventually everything seemed fully set up and up to date though, and a snapshot of the system was taken for later testing.

The product interface is quite attractive with its near-black background and hot red highlights. As well as the anti-malware and firewall components the suite includes a well-regarded HIPS system, ‘Defense+’, and much else besides. Controls lean towards the text-heavy rather than the blobby icons favoured by many, which makes them less easy to get lost amongst, and an excellent level of configuration is provided throughout. Stability seemed good in general, with some slowdowns in early runs attributed to the cloud component. This was disabled for on-demand scans but as far as we could tell it could not be switched off for the on-access module. Simply disconnecting from the lab network solved this little snag, and the rest of the test suite powered through in good time.

Performance measures	Idle system RAM usage increase	Busy system RAM usage increase	Busy system CPU usage increase	Standard file activities time increase
Agnitum Outpost	10.54%	11.08%	38.69%	8.25%
AhnLab V3 IS	6.15%	6.26%	32.90%	10.64%
ArcaBit ArcaVir	11.47%	9.50%	20.53%	7.83%
AvailaSoft AS Anti-Virus*	10.46%	10.11%	-38.31%	37.37%
Avast Software avast! Free	1.61%	1.07%	22.28%	7.92%
Avertive VirusTect	5.10%	5.15%	10.95%	12.06%
AVG Internet Security	8.59%	9.19%	43.98%	11.34%
Avira AntiVir Personal	4.13%	4.12%	21.72%	11.86%
Avira AntiVir Pro	10.24%	6.32%	25.05%	18.36%
BitDefender AV Pro	5.41%	6.18%	36.27%	4.97%
Bkis BKAV Pro	4.33%	4.56%	76.33%	9.84%
Bullguard Antivirus	12.15%	11.79%	17.80%	14.70%
CA ISS Plus	12.75%	12.81%	70.50%	20.60%
CA Total Defense r12	16.64%	16.52%	245.36%	55.07%
Central Command Vexira	3.78%	4.54%	19.85%	6.64%
Check Point Zone Alarm	8.90%	8.90%	132.79%	3.10%
Clearsight Antivirus	6.35%	7.05%	23.60%	11.17%
CommTouch Command	10.24%	9.60%	61.12%	12.26%
Comodo I.S. Premium	8.76%	5.55%	16.74%	11.33%
Coranti 2010	11.96%	12.23%	53.44%	9.34%
Defenx Security Suite	7.47%	7.74%	32.70%	13.95%
Digital Defender	7.36%	6.80%	16.56%	4.82%
eEye Blink	8.09%	8.43%	71.48%	6.06%
Emsisoft Anti-Malware	3.46%	2.29%	19.52%	28.84%
eScan Internet Security	2.36%	2.38%	25.97%	11.87%
ESET NOD32	5.15%	4.99%	20.16%	17.49%
Filseclab Twister	9.63%	9.75%	9.25%	14.06%
Fortinet FortiClient	9.48%	12.44%	42.68%	3.94%
Frisk F-PROT	11.24%	11.32%	26.91%	12.00%
F-Secure CS	5.53%	6.57%	14.60%	5.33%
F-Secure IS	7.37%	8.57%	9.90%	13.79%
G DATA AntiVirus	6.68%	7.96%	29.60%	13.35%
Hauri ViRobot	3.46%	3.56%	23.02%	14.65%
Ikarus T3 virus.utilities	6.95%	7.05%	37.08%	1.85%

*Negative value recorded for busy CPU.

Please refer to text for full product names.

Scanning speeds were on the low side of average, with light lag times on access, very low use of system resources and no great impact on the run time of our activities set.

Detection rates were excellent, and declined only very slightly across the RAP sets. The WildList was handled nicely, and with only two, entirely permissible ‘suspicious’ alerts in the clean sets, *Comodo* earns its first VB100 award, on its third attempt. We look forward to welcoming the vendor to the test bench again.

Coranti 2010

Version 1.003.00001

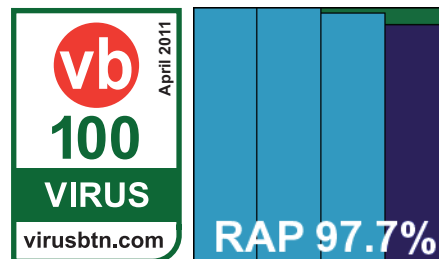
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.00%
Worms & bots	99.83%	False positives	0

Coranti has had something of a rollercoaster ride in its first year of VB100 testing, with some excellent results tempered by

the occasional false positive problem (as is always a danger with the multi-engine approach). The name of the product has seen a few changes as well, with the original ‘Multicore’ moniker dropped in favour of a simple ‘2010’ – somewhat odd given that earlier products had been labelled ‘2011’.

The latest version marks something of a departure, as the *Norman* engine that appeared in earlier tests has been phased out in favour of what is referred to as the ‘Lavasoft Ad-Aware scanning engine’ – this is presumably a combination of *Lavasoft*’s in-house anti-spyware expertise and the *GFI* (formerly *Sunbelt*) *VIPRE* engine also included in *Lavasoft*’s mainline *Ad-Aware* solutions. In addition to the *Frisk* and *BitDefender* engines retained from earlier incarnations, this should make for a formidable product, although the lab team did have some concerns based on stability issues encountered with *Ad-Aware*, and other solutions based on the same engine, in recent tests.

The installer was a lightweight 47MB, but online updates were also required on the deadline date. The install process was fast and simple, taking less than 30 seconds to complete and not demanding a reboot at the end. However, on opening the GUI the bulk of the controls were greyed out and it was clear that no scanning or protection was available. It may be that it simply needed some time to



Performance measures contd.	Idle system RAM usage increase	Busy system RAM usage increase	Busy system CPU usage increase	Standard file activities time increase
iolo System Shield	7.90%	7.85%	65.48%	13.97%
K7 Total Security	5.55%	5.47%	6.78%	13.75%
Kaspersky AV 6	7.34%	5.51%	48.86%	57.47%
Kaspersky IS	7.02%	6.10%	26.11%	47.15%
Kaspersky PURE	7.16%	6.91%	33.43%	31.43%
Keniu Antivirus	3.93%	4.05%	31.53%	11.85%
Keyguard Antivirus	6.28%	6.86%	11.69%	8.10%
Kingsoft I.S. Adv.	9.83%	8.82%	15.38%	9.68%
Kingsoft I.S. Std-A	7.06%	6.11%	16.97%	13.49%
Kingsoft I.S. Std-B	10.42%	8.68%	10.58%	8.78%
Lavasoft Ad-Aware TS	10.03%	9.42%	36.06%	22.99%
Logic Ocean GProtect	6.05%	5.26%	23.76%	11.41%
McAfee VirusScan	9.02%	5.13%	16.47%	12.97%
Microsoft Forefront	5.29%	6.08%	15.12%	4.35%
Nifty Security 24	6.25%	5.89%	37.59%	16.92%
Norman Security Suite	8.01%	8.72%	74.45%	14.07%
Optenet Security Suite	6.03%	5.55%	11.95%	41.59%
PC Booster AV Booster	6.98%	5.84%	15.59%	10.01%
PC Renew I.S. 2011	6.80%	4.47%	10.46%	13.39%
PC Tools I.S. 2011	16.85%	14.48%	69.94%	40.50%
PC Tools SD	22.31%	12.26%	48.55%	38.18%
Preventon Antivirus	5.59%	5.26%	16.10%	4.39%
Qihoo 360 Antivirus	30.59%	29.91%	20.98%	18.38%
Quick Heal Total Security	12.90%	12.24%	15.50%	27.00%
Returnil System Safe	7.00%	5.39%	79.89%	5.65%
Sofscan	11.80%	11.49%	225.86%	9.60%
Sophos Endpoint Security	7.28%	5.51%	14.24%	8.47%
SPAMfighter VIRUSfighter	6.58%	5.64%	21.12%	12.21%
GFI/Sunbelt VIPRE	3.72%	4.98%	31.75%	2.32%
Symantec EP	11.05%	10.40%	39.36%	8.84%
Trustport Antivirus 2011	6.12%	7.98%	19.90%	16.56%
UnThreat Antivirus Pro	6.34%	7.28%	32.88%	4.42%
VirusBuster Professional	6.75%	8.56%	17.53%	7.63%
Webroot IS Complete	4.28%	7.29%	4.53%	11.07%

Please refer to text for full product names.

settle down, but in our haste a reboot was initiated, which soon solved things. With the interface fully functional, the online update ran in reasonable time (given that over 260MB of detection data was being fetched).

The interface is something of a joy, being designed for maximum clarity and simplicity, but at the same time providing an impeccably detailed set of configuration controls to satisfy the most demanding power user. Examining deeply into archives on access was the only area we could claim to be lacking. The scheduler received particular praise from the lab team for its nifty design. Despite our earlier fears, the product proved rock-solid as far as stability goes, and although the multi-pronged approach inevitably affected speed over our large test sets, it still got everything done and dusted in excellent time.

Scanning speeds over clean samples were a little on the slow side, as were lag times on access. Although RAM was a little higher than many and CPU use also fairly high, our set of standard tasks ran through in good time.

As predicted, detection rates were stratospheric, with barely a thing missed anywhere, and even the proactive week of the RAP sets was covered extremely well. The clean sets threw up a few detections, but as these were only for Themida-packed items and possible adware there were no problems here. With the WildList also powered through effortlessly, *Coranti* easily earns another VB100 award after a truly excellent performance. This makes three passes out of five entries in the vendor's first year of competition, with only one (*Linux*) comparative not taken part in.

Defenx Security Suite 2011

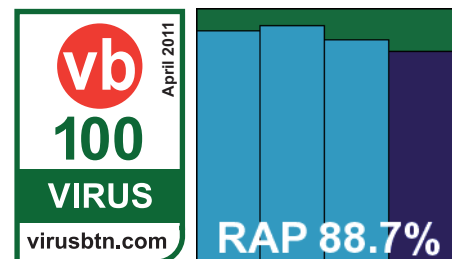
Version: 2011 (3390.519.1247)

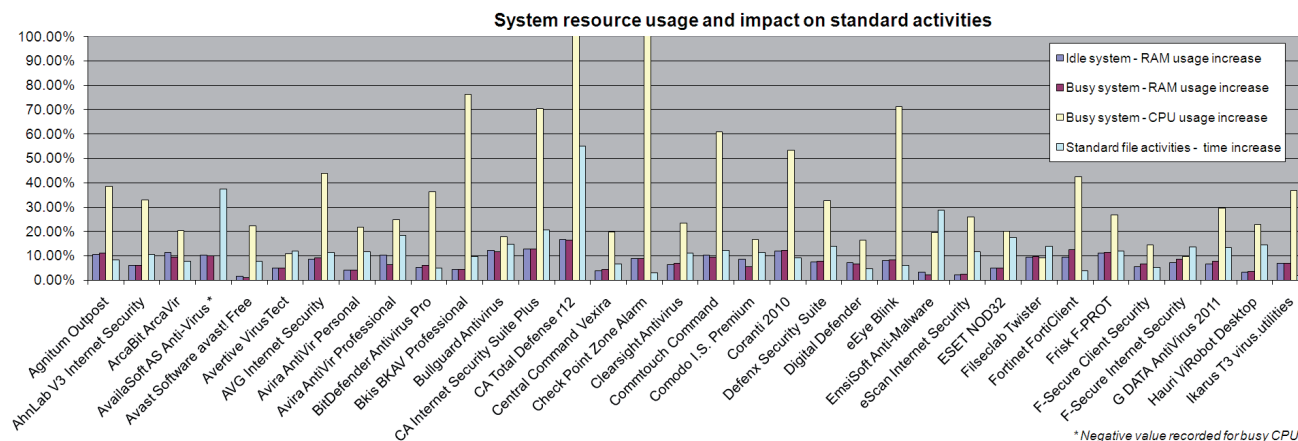
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.54%
Worms & bots	96.78%	False positives	0

Defenx has become something of a fixture in our comparatives over the past year or so, and has always been a welcome sight

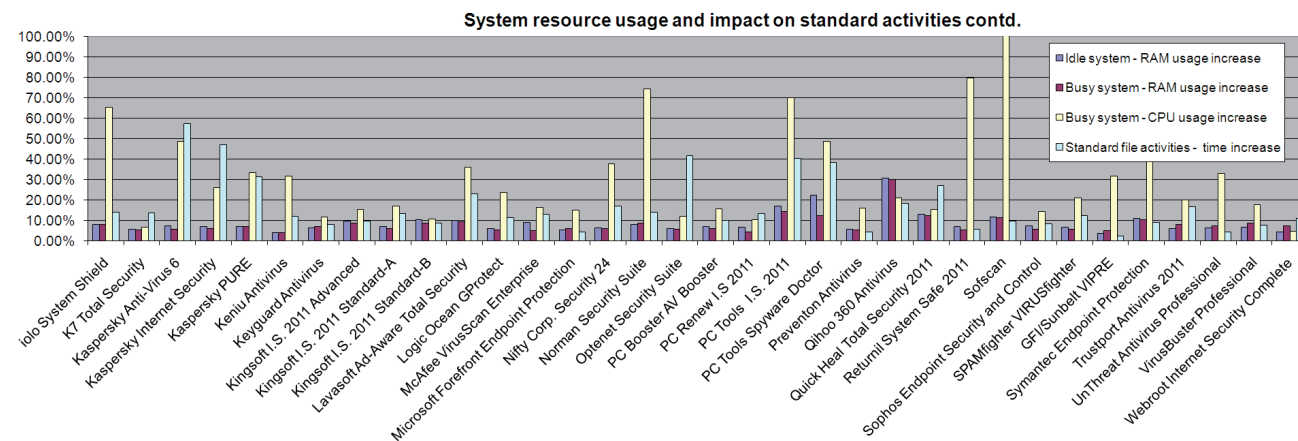
thanks to a record of good behaviour and reliability.

The version entered this month came as a 94MB installer, including updates, and took only a couple of clicks to install. The process continued for a couple of minutes





*Negative value recorded for busy CPU



Please refer to text for full product names.

after that, mainly taken up with firewall-related steps and checks, and a reboot was needed at the end. The interface reflects the company’s Swiss origins with its red-and-white colour scheme, and looks efficient and businesslike without seeming unfriendly or intimidating. Configuration is not over-generous for the anti-malware component (the full suite also including anti-spam and several other modules), but provides enough controls for most purposes and is easy to navigate and operate. Stability was excellent, with no problems at any point, and the use of caching of results even in infected items meant that the tests were sped through in excellent time.

Aided by the caching, scanning speeds were lightning fast, lag times feather-light, and performance measures stayed well within acceptable bounds.

Scores were solid, as we have come to expect from the *VirusBuster* engine underlying things, with decent levels across all sets. The WildList and clean sets were handled

perfectly, and a VB100 is awarded to *Defenx* for its efforts. The vendor’s history in our comparatives is impeccable, with seven entries and seven passes, the recent *Linux* test the only one not entered since the product’s first appearance in last year’s *XP* comparative.

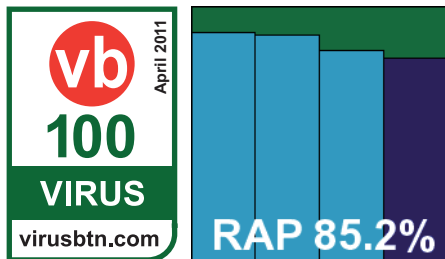
Digital Defender 2.1.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Another member of the *Preventon* club, *Digital Defender* has been around longer than most with more than a year’s worth of comparatives under its belt. The install process for the familiar 67MB package held no surprises, with a few stages and online activation all dealt with in a minute or so, no reboot required. The interface has a pleasant minty

green hue, its layout once again giving us little to worry about, with the same simple design and reasonable set of options. No stability issues were noted, and testing went according to plan, completing within 24 hours.



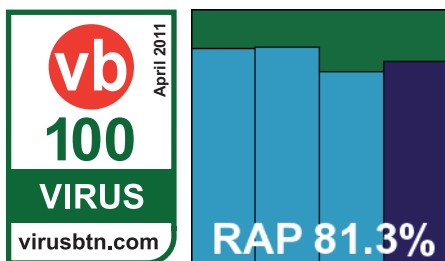
Scanning speeds were slowish and lag times not too zippy, but resource consumption was low and our set of jobs was not too heavily impacted. Detection rates closely matched those of the rest of the product family, with little to complain about, and the core certification sets were handled without fuss. *Digital Defender* thus earns a VB100 award, its first since this time last year thanks to a string of bad luck; we fully expect the product to continue to do well.

eEye Digital Security Blink Professional 4.7.1

Rule version 1603; anti-virus version 1.1.1257

ItW	100.00%	Polymorphic	99.98%
ItW (o/a)	100.00%	Trojans	86.73%
Worms & bots	89.16%	False positives	0

Having initially only participated in VB100 tests once a year, in the annual XP test, *eEye's Blink* has recently become a



more regular participant, and the product has become quite familiar to the test team. Its most notable feature is the vulnerability monitoring system which is the company's speciality, and which sits alongside anti-malware protection provided by *Norman*.

The product arrived as a fairly sizeable 157MB install package with an additional 94MB of updates. The installation process is not complex but takes a minute or two, starting off with the installation of some supporting packages and ending with no need to reboot. After installation the firewall seems to be switched off by default, but the anti-malware component – included alongside the

vulnerability management and intrusion prevention system – is up and running from the off. The interface is of fairly standard design, with status and configuration sections for each module, and controls are limited but provide the basic requirements. We encountered no problems with stability, and managed to use the scheduler system without any trouble, running the bulk of the testing over a weekend to make the best use of time.

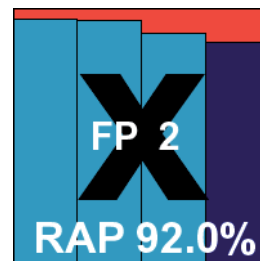
This proved to be a good thing since the product has a somewhat languorous approach to scanning, dawdling dreamily along and showing no sign of urgency. Scanning speeds were very slow, and file access lag times very high, with heavy use of CPU cycles when busy, but RAM was not too heavily drained and our set of jobs did not take much longer than normal to complete.

Detection rates were respectable but not jaw-dropping, with decent coverage in all the sets, the proactive week of the RAP sets showing a slight upturn over the previous week. A couple of suspicious detections in the clean sets were allowable, and the WildList was covered in its entirety, earning *eEye* a VB100 award. The product's recent test history has not been great, with a string of problems including missed polymorphic samples and false positives in the last year; it now has three passes and five fails in the last two years, having skipped four tests. The last six tests show a slightly better picture, with two passed, two failed, two not entered.

EmsiSoft Anti-Malware 5.1.04

ItW	99.33%	Polymorphic	95.58%
ItW (o/a)	99.66%	Trojans	95.06%
Worms & bots	98.88%	False positives	2

EmsiSoft dropped its widely recognized 'A-Squared' name in favour of a more sober title some time ago, but the product remains familiar and includes references to the old name in several folders and files used by the installed product. Much of the detection is provided by the *Ikarus* engine.



This month's submission measured a little over 100MB, including all updates, and ran through the standard steps followed by a lightning-fast installation. With this complete (no reboot was required), a configuration wizard ran through some set-up stages including licensing, updates, joining a feedback system, and an initial system scan. The interface is quite appealing, adorned with a rotating Trojan horse image, and has a few quirks of design but is

generally clearly laid out and not too difficult to operate. Configuration is reasonable, but provides no option to simply block access to infected items in the on-access module – something which often causes problems in large-scale testing.

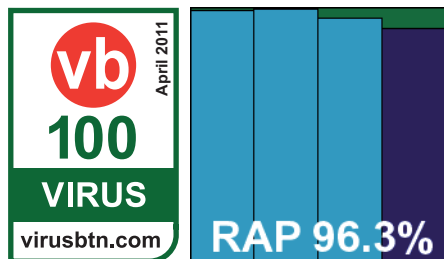
Scanning speeds were fairly slow, but on-access lag times were extremely low, with low use of system memory. CPU cycle use was a little higher than average though, and our suite of standard jobs took a little longer than usual to complete.

Once we got onto the infected sets the need to disinfect or quarantine all samples, or else respond to a pop-up for each and every one, soon caused the expected problems, with the product freezing up entirely and refusing to respond to anything. Even after a reboot it proved unusable, and we had to resort to reinstalling on a fresh machine image. Eventually, by chopping jobs up into smaller chunks, we managed to get a full set of results, which showed some splendid figures. Coverage of core certification sets, however, was not so splendid, with a handful of items missed in the WildList set, and some false alarms in the clean sets. These included one file flagged as the infamous Netsky worm and another as the nasty polymorphic Virut – both were, in fact, innocent PDF handling software. This was plenty to deny *EmsiSoft* a VB100 award this month, leaving it on a 50-50 record of two passes, two fails in the last six tests.

eScan Internet Security Suite 11.0.1139.924

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.06%
Worms & bots	99.70%	False positives	0

The *eScan* product range has a long and solid history in our comparatives, dating back to 2003 and covering a wide selection of



platforms. Not long after dropping an OEM engine from the product, it has put in some excellent performances of late.

The current version of the premium suite solution came as a 156MB installer, no further updates required, and installed in three or four clicks, with no reboot needed. After the main install came some standard initial set-up stages, and things were soon moving along.

The product interface is a rather funky affair, with a panel of glitzy cartoon icons along the bottom and a slightly more sober display of status information in the main window. Configuration is comprehensive and detailed with good attention paid to a logical, intuitive layout, and testing moved along nicely. Scanning speeds were rather sluggish at first, but after first sight of things some result caching came into play and the process sped up nicely. On access, lag times were impressively low, and memory use was fairly low too, with CPU drain and impact on our suite of standard jobs around average.

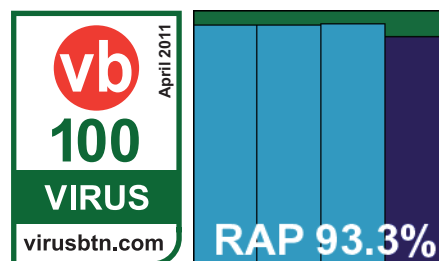
Detection rates were pretty decent, with highly impressive scores in all sets – a slight decline towards the newer end of the RAP sets still not taking things below 90%. The WildList and clean sets threw up no issues, and *eScan* comfortably earns another VB100 award – having not missed a single test in the last two years, it now has nine passes to only three fails: a very respectable record of achievement.

ESET NOD32 Antivirus 4

Version 4.2.71.2; virus signature database: 5901 (20110223)

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	89.29%
Worms & bots	98.13%	False positives	0

ESET has an even more illustrious history in our tests, still holding onto its record for the longest unbroken run of certification



passes – and indeed comparatives taken part in, the vendor not having missed a test since 2003.

The current product has been in stable form for some time. This month's submission, a nice small 44MB executable, was installed with the standard steps, enlivened as usual by the enforced choice of whether or not to detect 'potentially unwanted' software – the 'next' button is greyed out until a selection is made. It doesn't take long and no reboot is needed, just a short pause before the protection is in place.

The interface is simple and unfussy, but provides a wealth of fine-tuning controls. There is so much here that some of it seems to be a little superfluous and in places overlapping, and we have long had trouble figuring out the controls for

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	OD	2	√	√	X	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
AhnLab V3 Internet Security	OD	X	√	X/√	X/√	X	√	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Antiy Ghostbusters	OD	X	X	X	X	X	X	X	X	X	X	X
	OA	---	---	---	---	---	---	---	---	---	---	---
ArcaBit ArcaVir	OD	2	√	√	√	√	√	√	√	√	1	√
	OA	2	X/9	√	√	X/9	X/√	X/9	X/√	X/√	1	√
AvailaSoft AS Anti-Virus	OD	1	5	5	5	5	√	5	2	5	5	√
	OA	1	5	5	5	5	√	5	5	5	5	√
Avast Software avast! Free	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
Avertive VirusTect	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
AVG Internet Security	OD	√	√	√	√	√	√	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira AntiVir Personal	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avira AntiVir Professional	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Antivirus Pro	OD	√	√	7	7	√	√	√	7	√	√	√
	OA	X/√	X/√	X/√	X/√	2/√	X/√	X/√	X/√	1/√	1/√	√
Bkis BKAV Professional	OD	X	X	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bullguard Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	√	√	8	8	√	√	√	8	√	√	√
CA Internet Security Suite Plus	OD	X	√	√	√	√	√	√	√	√	√	X
	OA	X	X	X	X	1	X	X	X	1	X	√
CA Total Defense r12	OD	X	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	X/√	√
	OA	X	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	X/√	√
Central Command Vexira	OD	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Check Point Zone Alarm	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Clearsight Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√

Key:

√ - Detection of EICAR test file up to ten levels of nesting;

X - No detection of EICAR test file

X/√ - Default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

EXT* - Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Commtouch Command	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	X/4	X/4	X/4	X/4	X/4	√	X/4	X/2	X/4	X/4	√
Comodo I.S. Premium	OD	X	5	5	5	5	5	5	2	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Coranti 2010	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/1	X	X	X	X/√	X	X	X	1	X/1	X/√
Defenx Security Suite	OD	X	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Digital Defender	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
eEye Blink	OD	X	4/√	3/√	X/1	4/√	4/√	4/√	1/√	4/√	X	√
	OA	X	X/√	X/√	X	X/√	X/√	X/√	X/√	X/√	X	√
Emsisoft Anti-Malware	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	2	2	2	2	2	2	2	X	2	2	√
eScan Internet Security	OD	9	5	4	3	5	5	5	4	5	8	√
	OA	√	√	√	√	√	√	√	√	√	√	√
ESET NOD32	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Filseclab Twister	OD	5	3	3	3	4	1	4	X	5	X	√
	OA	X	X	X	X	X	X	1	X	2	X	X
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	√	1	√
	OA	X	√	√	√	√	√	√	√	√	1	√
Frisk F-PROT	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	2	2	X	X	X	2	2	√
F-Secure Client Security	OD	X/√	√	√	√	√	√	√	8	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure Internet Security	OD	X/√	√	√	√	√	√	√	8	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
G DATA AntiVirus 2011	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
Hauri ViRobot Desktop	OD	X	1	X	1	√	1	1	X	1	1	√
	OA	X	X	X	X	√	X	X	X	1	1	8/√
Ikarus T3 virus.utilities	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	2	2	2	2	2	2	2	3	2	2	√

Key:

√ - Detection of EICAR test file up to ten levels of nesting;

X - No detection of EICAR test file

X/√ - Default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

EXT* - Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
iolo System Shield	OD	5	5	5	5	5	√	5	5	5	5	√
	OA	5	5	5	5	5	√	5	5	5	5	√
K7 Total Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	1	1	X	X	X	1	1	√
Kaspersky Anti-Virus 6	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky Internet Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky PURE	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Keniu Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X/1	X/1	X	X	X	X	X	X	√
Keyguard Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
Kingsoft I.S. 2011 Advanced	OD	X	√	√	X	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kingsoft I.S. 2011 Standard-A	OD	X	√	√	X	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kingsoft I.S. 2011 Standard-B	OD	X	√	√	X	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Lavasoft Ad-Aware TS	OD	√	√	9	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
Logic Ocean GProtect	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
McAfee VirusScan Enterprise	OD	2	√	√	√	√	√	√	√	√	X	√
	OA	2	√	√	√	√	√	√	√	√	X	√
Microsoft Forefront	OD	√	√	√	√	2	2	2	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√
Nifty Corp. Security 24	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Norman Security Suite	OD	X	√	8	1	√	√	√	8	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Optenet Security Suite	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	X	X	√

Key:

√ - Detection of EICAR test file up to ten levels of nesting;

X - No detection of EICAR test file

X/√ - Default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

EXT* - Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
PC Booster AV Booster	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
PC Renew I.S 2011	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
PC Tools I.S. 2011	OD	√	√	√	√	√	√	√	√	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	X
PC Tools Spyware Doctor	OD	√	√	√	√	√	√	√	√	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	X
Preventon Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
Qihoo 360 Antivirus	OD	√	√	8	√	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Quick Heal Total Security	OD	X	2/5	X	X	2/5	X	2/5	1	2/5	X	X/√
	OA	X	X	X	X	1	X	X	X	1	X	√
Returnil System Safe 2011	OD	5	5	2	2	5	7	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Sofscan Professional	OD	√	√	√	√	X	X	√	√	√	X	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Sophos ESC	OD	X	X/5	X/5	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/5	X/5	X/√
SPAMfighter VIRUSfighter	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1		1	X/1	X/√
GFI/Sunbelt VIPRE	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Symantec Endpoint Protection	OD	3/√	3/√	3/√	3/√	3/√	3/√	3/√	1/5	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Trustport Antivirus 2011	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
UnThreat Antivirus Pro	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
VirusBuster Professional	OD	2	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Webroot IS Complete	OD	X	√	5	5	5	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√

Key:

- √ - Detection of EICAR test file up to ten levels of nesting;
- X - No detection of EICAR test file
- X/√ - Default settings/all files
- 1-9 - Detection of EICAR test file up to specified nesting level
- EXT* - Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names)

scanning inside archives on access. However, it is generally solid and intuitive. Occasionally the interface tends to get itself in a bit of a twist after a scan job, but it invariably sorts itself out within a few moments, and the only other issue noted was the occasional scan display screen not finishing properly, lingering at 99% when logs showed the scan had already completed without problems.

Scanning speeds were OK, and on-access lag times fairly low too, with low use of resources. Impact on our set of activities was a little higher than most, but not too much.

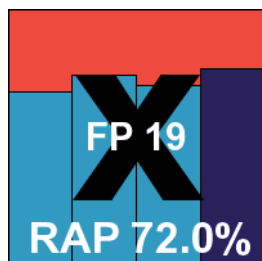
Detection rates were excellent as usual, with most of the sets demolished and there was superb regularity in the reactive part of the RAP sets. A couple of items were flagged as unsavoury in the clean sets, one of them being packed with Themida and another a toolbar, but no problems arose there or in the WildList – thus earning ESET yet another VB100 award to maintain the 100% record it has held for the best part of a decade.

Filseclab Twister AntiVirus V7 R3

Version 7.3.4.9985; definition version 13.35.42143

ItW	97.62%	Polymorphic	63.35%
ItW (o/a)	92.81%	Trojans	66.86%
Worms & bots	68.29%	False positives	19

Filseclab first took part in our comparatives just over two years ago, and has been gamely regular in its appearances ever since, despite as yet no luck in achieving certification. The vendor's solution is an interesting and unusual one, but provides all the usual features one would expect from an anti-malware product.



The main installer is 53MB, with a 54MB updater also freely available to download from the company's website. The set-up process is completed in three clicks and about ten seconds, although the updater program is a little less zippy – apparently doing nothing for a minute or so before a window appears showing progress. The interface is quirky but not unclear, with a wide selection of options crammed into a small area. We noted with interest that the support email address shown in the 'about' window is at hotmail.com.

Running through the tests is always a little fiddly as the product only records on-access detections when set to erase or clean automatically – otherwise, a pop-up appears noting the detection and asking for a decision as to what

to do about it, but no entry is made in the product log until the choice is made. Nevertheless, it seemed to cope with the heavy workload and got through the tests in good time.

Scanning speeds were not incredibly fast, but file access lags were very low and processor cycle use was low too, although memory consumption was fairly high. The set of standard jobs completed in average time.

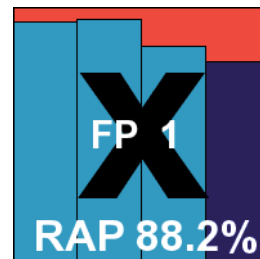
Detection rates were not too bad in general, but there were quite a few misses in the WildList set (many more polymorphic samples missed on access than on demand), and a fairly large smattering of false alarms in the clean sets. As a result, the product is denied certification once again, but it seems to be showing steady improvement in both solidity and coverage – and it seems likely that Filseclab will reach the VB100 standard in the not too distant future.

Fortinet FortiClient 4.1.3.143

Virus signatures version: 10.7; virus engine version: 4.2.257

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.07%
Worms & bots	98.08%	False positives	1

Fortinet's main business is in the appliance market, but its client solutions have long been regulars in VB100 tests, with some strong improvement in detection seen over the last few tests.



The installer is a tiny 9.8MB, supplemented considerably by 132MB of updates. The set-up process starts with a choice of free or premium versions, then after a couple more clicks and a pause of 20 seconds or so it's all ready to go without a reboot. Applying the updates is a simple and similarly speedy process.

The interface is efficient and businesslike, with an intuitive layout and an excellent level of configuration – as one would expect from a primarily corporate solution. Operating proved generally easy and stable, although at one point a considerable amount of work was wasted when the product appeared to delete all logs from the previous day, despite having explicitly been told not to. Even with this delay, testing did not overrun by more than a few hours. We also noted that the on-access scanner is fired when browsing folders containing infected items with the scanner module, which was rather confusing.

Speeds and lag times were fairly average, as were other performance measures, with CPU use perhaps slightly higher than most. Detection rates were highly impressive, showing a continuation of the gradual upward trend noted in recent tests. This appears for the most part to be due to the enabling of ever stronger heuristics, which used to be mainly switched off by default.

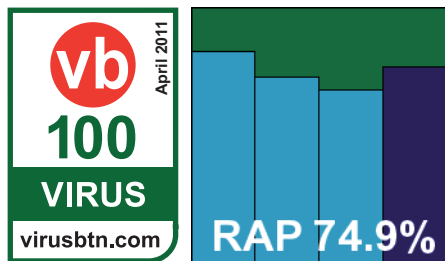
Of course, increasing heuristics always comes with its associated risks, and this month it looks like things have been taken a fraction too far: a single item in the clean sets, from Canadian software house *Corel*, was flagged as a Krap trojan. This false alarm denies *Fortinet* a VB100 award this month, despite a good showing and flawless coverage of the WildList set. The vendor's two-year record shows seven passes and now three fails, with only the *Linux* comparatives not entered; the last six tests show a slightly rosier picture, with only one fail and four passes from five entries.

Frisk F-PROT Antivirus for Windows 6.0.9.5

Scanning engine version number 4.6.2; virus signature file from 22/02/2011 14:06

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	75.14%
Worms & bots	90.77%	False positives	0

Frisk is a pretty long-serving company, its first VB100 appearance was in 1999 and it hasn't missed a comparative since 2007.



The product hasn't seen any major changes since then either, sticking to its tried and trusted formula.

The installer is a compact 30MB, with an extra 30MB zip file containing the latest updates. The set-up process requires three or four clicks and a ten-second wait, then a reboot is demanded to complete the installation. The interface is minimalist but provides a basic set of options, including among them the choice to detect only *Microsoft Office*-related malware – something of a throwback to the past. Operating is not difficult and stability is generally good, but as usual during large scans of weird and wonderful malware the scanner occasionally died. Its own friendly crash screen – from which several sets of debug info were saved – was presented each time it died mid-task.

Scanning speeds were fairly good, and lag times fairly low. RAM consumption was a little above average, but other performance measures showed a lighter touch.

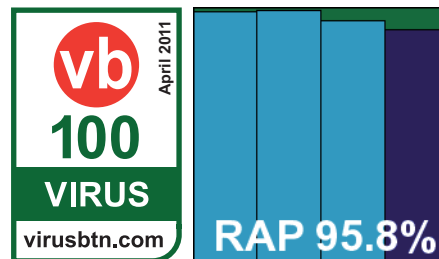
Detection results were gathered easily enough after repeating several jobs, and showed decent if not exactly mind-blowing scores across the sets. Once again there was a slight upturn in the proactive week of the RAP sets. The WildList and clean sets were properly managed, and *Frisk* comfortably earns VB100 certification once again. The company's record has been somewhat patchy over the last few years, with seven tests passed out of a potential 12.

F-Secure Client Security 9

9.01 build 122; anti-virus 9.20 build 16701

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.45%
Worms & bots	99.61%	False positives	0

F-Secure routinely submits a brace of products these days: one its standard desktop suite, and the other from the 'client' branch



– presumably a more business-focused effort – but there is usually little difference between the two. This client edition had a 58MB installer and a 125MB update bundle, which was shared by the two solutions.

The set-up process went through several stages including some questions about management systems and which components to install, and needed a reboot to complete. The interface is dominated by a large green tick to indicate all is well, and has a very simplified design which is somewhat awkward to navigate in places. There is little by way of fine-tuning controls. Stability seemed a little suspect, with some scans freezing and reboots required to restore functionality to the product. Running over infected sets was even more rocky, with age-old logging issues rearing their ugly heads once more. A run over the clean sets reported a number of detections, urgently labelled 'infection', but on trying to display the log we were instead shown one from a previous scan over the archive sample set. This sort of disinformation could be extremely troubling to a user.

Speeds were very fast once files had been checked out for the first time, and this effect had an even more notable impact on lag times. The batch of standard jobs

completed rapidly and resource consumption remained low throughout.

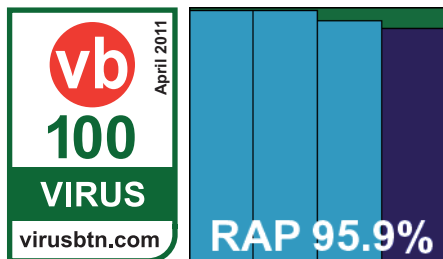
Logging problems continued in the main infected sets, where a large job was left to run overnight only to find that no details could be shown the following morning. The task was repeated using the command-line scanner included with the product, with options tuned to approximate the GUI scanner as closely as possible. The scores turned up in the end were uniformly excellent – more than sufficient to cheer us up after a rather dismal testing spell; RAP scores were particularly impressive. The clean sets were found to contain only a ‘riskware’ item, which is allowed, and the WildList set was covered without problems, thus earning *F-Secure* a VB100 award without difficulty. This product line has been entered in all desktop tests since late 2009, passing every time.

F-Secure Internet Security 2011

1051 build 106; anti-virus 9.30 build 400

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.60%
Worms & bots	99.63%	False positives	0

Despite slightly different version details and a change of product title, this looks like a pretty similar product to the last.



The 55MB installer and that same 125MB updater install slightly more simply – at least when choosing the automatic rather than step-by-step mode. After a minute or so copying files around and so on, it requests the opportunity to validate itself online, but no reboot is needed to finish things off.

The interface is much like the previous product: simple with a bare-bones set of options under the hood, but it proved reasonably easy to make our way through our tests, helped along by blink-and-you’ll-miss-it scanning speeds in the ‘warm’ scans. Once again we saw some wobbliness in the scanner set-up, with some scan jobs disappearing silently after being set up, and others failing to produce final reports – we saw the same confusion covering the clean set, where the scan progress indicated a detection had been found but the final report could not enlighten us further. Again the command-line tool was used for the more hefty jobs, and proved much more reliable.

With scan speeds and lag times similar to the client solution, memory use seemed a little higher, and a slightly heavier impact on our set of activities was observed.

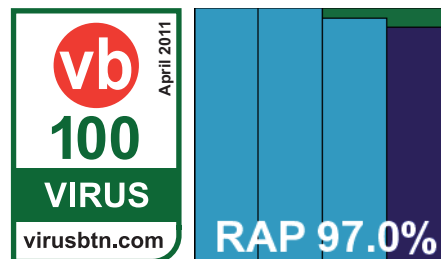
Detection rates were again superb, with over 90% everywhere. The core certification requirements were comfortably met, and *F-Secure* picks up a second award this month. The company’s main product line has an exemplary record of ten passes in the past two years, with only the annual *Linux* tests not entered.

G DATA AntiVirus 2011

Program version: 21.1.1.0 (9/22/2010)




























ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.52%
Worms & bots	99.88%	False positives	0

G DATA is always a welcome sight on our test bench thanks to an excellent record of stability and good behaviour, to say nothing of invariably impressive detection levels. The vendor’s dual-engine approach also manages to avoid the excessive sluggishness which is so often associated with this kind of product.



































The latest version came as a not too huge 189MB installer, including all the required data, and took only a few straightforward steps to get set up, although a reboot is required. The interface is simple but efficient, concealing a wealth of control beneath its pared-down exterior, and is a delight to operate. At one point we experienced something of an oddity during our performance tests, but this seemed to be something to do with the automation scripts (or possibly some behavioural monitor not liking what they were doing), and the product itself remained stable and solid. All jobs were out of the way within a single working day, well within the allotted 24 hours.

This was partly thanks to the excellent use of results caching to avoid repeating work, which made for some good speed measures. On-access lags looked higher than some in our graph thanks to very thorough checks with scanning depth and breadth turned up high. Resource use was pleasingly low, with our standard jobs running through in reasonable time.

Reactive And Proactive (RAP) scores		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		91.40%	93.24%	87.51%	90.72%	83.08%	88.81%
AhnLab V3 Internet Security		94.44%	94.15%	82.34%	90.31%	82.37%	88.32%
Antiy Ghostbusters		59.95%	65.11%	56.99%	60.68%	65.88%	61.98%
ArcaBit ArcaVir		66.29%	65.23%	57.16%	62.89%	56.73%	61.35%
AvailaSoft AS Anti-Virus		40.46%	42.15%	39.69%	40.77%	51.76%	43.52%
Avast Software avast! Free		98.29%	97.74%	95.03%	97.02%	90.02%	95.27%
Avertive VirusTect		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
AVG Internet Security		95.11%	95.95%	94.75%	95.27%	84.38%	92.55%
Avira AntiVir Personal		98.40%	98.82%	95.69%	97.64%	91.21%	96.03%
Avira AntiVir Professional		98.40%	98.82%	95.69%	97.64%	91.21%	96.03%
BitDefender Antivirus Pro		97.55%	95.45%	92.33%	95.11%	89.28%	93.65%
Bkis BKAV Professional		97.93%	96.56%	95.17%	96.55%	92.15%	95.45%
Bullguard Antivirus		98.48%	98.47%	96.06%	97.67%	91.61%	96.15%
CA Internet Security Suite Plus		79.60%	79.31%	77.01%	78.64%	77.06%	78.25%
CA Total Defense r12		77.33%	74.81%	71.90%	74.68%	73.68%	74.43%
Central Command Vexira		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Check Point Zone Alarm		95.71%	95.23%	94.31%	95.08%	90.79%	94.01%
Clearsight Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
Commtouch Command		84.14%	74.95%	71.80%	76.97%	79.72%	77.66%
Comodo I.S. Premium		90.21%	90.19%	80.33%	86.91%	78.33%	84.77%
Coranti 2010		99.70%	99.76%	97.97%	99.14%	93.30%	97.68%
Defenx Security Suite		91.22%	93.00%	87.53%	90.59%	82.95%	88.68%
Digital Defender		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
eEye Blink		84.70%	85.02%	75.86%	81.86%	79.57%	81.29%
Emsisoft Anti-Malware		95.72%	95.22%	90.18%	93.71%	86.77%	91.97%
eScan Internet Security		98.71%	99.06%	95.84%	97.87%	91.67%	96.32%
ESET NOD32		94.24%	94.31%	94.92%	94.49%	89.86%	93.33%
Filseclab Twister		67.63%	73.88%	70.22%	70.58%	76.41%	72.03%
Fortinet FortiClient		94.12%	95.34%	84.59%	91.35%	78.53%	88.15%
Frisk F-PROT		82.53%	72.59%	67.67%	74.26%	76.76%	74.89%
F-Secure Client Security		98.46%	98.78%	94.60%	97.28%	91.43%	95.82%
F-Secure Internet Security		98.53%	98.84%	94.69%	97.35%	91.50%	95.89%
G DATA AntiVirus 2011		99.94%	99.82%	95.88%	98.55%	92.17%	96.95%
Hauri ViRobot Desktop		65.26%	69.24%	62.33%	65.61%	74.07%	67.73%
Ikarus T3 virus.utilities		98.50%	99.48%	98.72%	98.90%	91.84%	97.13%

Please refer to text for full product names.

Reactive And Proactive (RAP) scores contd.		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
iolo System Shield		76.12%	72.43%	67.46%	72.01%	76.97%	73.25%
K7 Total Security		86.13%	78.12%	75.25%	79.83%	82.20%	80.42%
Kaspersky Anti-Virus 6		95.50%	95.20%	93.18%	94.63%	89.32%	93.30%
Kaspersky Internet Security		96.42%	95.67%	94.99%	95.69%	91.17%	94.56%
Kaspersky PURE		96.39%	95.64%	94.96%	95.66%	91.18%	94.54%
Keniu Antivirus		96.44%	95.69%	94.60%	95.58%	90.78%	94.38%
Keyguard Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
Kingsoft I.S. 2011 Advanced		24.24%	33.85%	25.46%	27.85%	34.63%	29.54%
Kingsoft I.S. 2011 Standard-A		15.86%	16.54%	13.87%	15.42%	25.52%	17.95%
Kingsoft I.S. 2011 Standard-B		15.86%	16.53%	13.86%	15.42%	25.51%	17.94%
Lavasoft Ad-Aware Total Security		99.95%	99.83%	95.96%	98.58%	92.22%	96.99%
Logic Ocean GProtect		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
McAfee VirusScan Enterprise		86.13%	86.31%	82.73%	85.05%	83.69%	84.71%
Microsoft Forefront Endpoint Protection		94.38%	95.07%	91.12%	93.52%	87.18%	91.94%
Nifty Corp. Security 24		96.39%	95.66%	93.87%	95.30%	90.50%	94.10%
Norman Security Suite		84.72%	85.04%	75.89%	81.88%	79.58%	81.30%
Optenet Security Suite		81.29%	85.30%	79.04%	81.87%	81.48%	81.78%
PC Booster AV Booster		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
PC Renew I.S 2011		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
PC Tools I.S. 2011		94.28%	96.82%	87.04%	92.72%	83.00%	90.29%
PC Tools Spyware Doctor		94.28%	96.82%	87.04%	92.72%	83.00%	90.29%
Preventon Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
Qihoo 360 Antivirus		98.86%	98.62%	92.02%	96.50%	90.42%	94.98%
Quick Heal Total Security 2011		92.12%	90.84%	88.37%	90.44%	89.67%	90.25%
Returnil System Safe 2011		85.19%	75.87%	72.61%	77.89%	80.02%	78.42%
Sofscan Professional		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Sophos Endpoint Security and Control		91.34%	93.16%	88.46%	90.99%	83.59%	89.14%
SPAMfighter VIRUSfighter		89.28%	88.46%	80.62%	86.12%	78.68%	84.26%
GFI/Sunbelt VIPRE		98.67%	99.35%	95.59%	97.87%	84.66%	94.57%
Symantec Endpoint Protection		92.92%	95.82%	84.06%	90.94%	81.50%	88.58%
Trustport Antivirus 2011		99.82%	99.86%	99.21%	99.63%	93.18%	98.02%
UnThreat Antivirus Professional		98.67%	99.36%	95.59%	97.87%	84.66%	94.57%
VirusBuster Professional		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Webroot Internet Security Complete		91.92%	93.53%	87.84%	91.10%	83.70%	89.25%

Please refer to text for full product names.

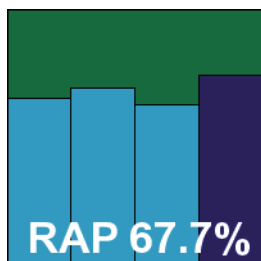
Detection rates were uniformly excellent, with only the tiniest number of samples not spotted and even the proactive week of the RAP sets covered superbly. The WildList was demolished in short order and the only alerts in the clean sets were for password-protected archives, thus *G DATA* earns another VB100 award with some ease. The vendor's recent record is pretty strong: eight passes and only a single fail in the last two years, with three tests not entered; four of the passes, as well as that one unlucky fail, have been in the last six tests.

Hauri ViRobot Desktop 5.5

Engine version 2011-02-22.00(6659169)

ItW	99.33%	Polymorphic	100.00%
ItW (o/a)	99.33%	Trojans	65.04%
Worms & bots	64.96%	False positives	0

Hauri has a somewhat sporadic history in our comparatives, entering several tests in a row and then vanishing for a few years. The company's current product is a combination of the *BitDefender* engine with some additional detection of its own.



The installer is a sizeable 300MB, but it gets to work fairly rapidly, even taking into account the scan of running processes performed before it gets going. No reboot is required to complete. The interface is clear and sensible, simple to navigate even for an unfamiliar user, and our lab team found it pleasant both to look at and to use. The product generally ran stably, but logging was a bit of an issue, the process of going from the end-of-scan dialog to a saved log taking anything from ten minutes to three hours, depending on the size of the log being exported. We also found the scheduler a little irritating, as despite having set it only to log all detections, it stopped at the first sample spotted and asked if it should continue with the scan. As this detection took place at 8PM on a Friday, and we had hoped to get a few hundred thousand more in the bag by Monday morning, it was a bit of a disappointment to find it sitting there waiting for our decision when we got back after the weekend. Repeating this job meant it took up more than double the expected 24-hour period, even excluding the time we were out of the office.

Scanning speeds were pretty sluggish even with the fairly light default settings, and turning on full scanning of archives resulted in a truly exhaustive and lengthy scan time. On-access measures showed some pretty heavy lag times too, although memory use was low and other performance measures around average.

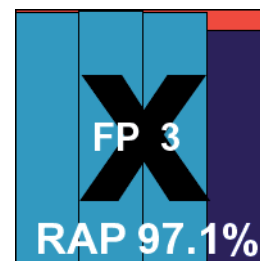
Detection rates were rather disappointing given the OEM engine included, and we had to repeat things later on to reassure ourselves we had not made some mistake. A second run showed the exact same set of scores however. These were not too dismal, but well short of what was expected, and although the clean set seemed to be handled without problems, a handful of items in the WildList went undetected, and a VB100 award remains just out of reach for *Hauri*. The product has been entered twice in the last year with a similar lack of success on each occasion.

Ikarus T3 virus.utilities 1.0.258

Virus database version 77801

ItW	99.83%	Polymorphic	95.58%
ItW (o/a)	99.83%	Trojans	97.27%
Worms & bots	99.43%	False positives	3

Ikarus earned its first VB100 award last summer, having first taken part in a comparative as long ago as 2001, but then disappearing for several years. The achievement was repeated on *Windows 7* in the autumn, and now *Ikarus* returns to try to make it a hat-trick.



The product is provided as a complete CD iso image, weighing in at 206MB, with an extra 69MB of updates to apply as well. The installation process includes adding the *Microsoft .NET* framework, if not already available. This is handily bundled into the install package but adds several minutes to an already fairly lengthy task.

The interface has traditionally been a little wobbly, particularly when first trying to open it, but it seemed a little more responsive on this occasion. It is pretty basic, with not many menus or buttons, but manages to provide a rudimentary set of controls to fill most needs. When running under heavy pressure it is particularly ungainly, flickering and juddering like a mad thing, and often needs a reboot after a big job to get back to normal operation. After one fairly reasonable job scanning our set of archive files, things took a turn for the worse, and even a reboot couldn't help. With the OA module munching up RAM, the interface refusing to open and several standard *Windows* functions failing to function, we had no choice but to wipe the system and start again with a fresh operating system image. This time it kept going despite the heavy load, getting to the end in reasonable time.

Scanning speeds were OK, and lag times fairly light, with RAM use below average and CPU use a little above

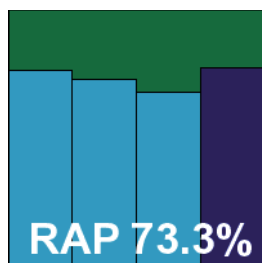
average, while the set of activities completed very quickly indeed.

Detection rates were excellent, with splendid scores across the board. However, a single item in the WildList set was missed – a closer look showed this was an exceptionally large file, which has upset some other products of late, implying that *Ikarus* imposes some limit on the size of files scanned by default. Further investigation confirmed that there was a cap, sensibly set to 8MB, which was considerably smaller than the file in question. However, removing this limit still did not result in detection, even when the file was scanned on its own. Finding this a little odd, we tried re-running the job with the limit left in place, but increased to a size that covered the file in question. This successfully enabled detection, hinting that the controls are less than fully functional. Of course our rules insist on default settings for our official scores, so the eventual detection cannot be counted. In addition, a handful of false alarms were generated in the clean sets, including a Virut alert on a piece of office software, thus *Ikarus* doesn't quite make the grade for certification and will have to wait for its third award.

iolu System Shield 4.2.1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	99.83%	Trojans	74.39%
Worms & bots	86.46%	False positives	0

Specializing in the optimization, clean-up and recovery spheres, *iolu* has been active in security for a while too, with occasional VB100 entries dating back to 2007. The company achieved its first VB100 award in the last *Windows 7* test (see *VB*, December 2010, p.27), with its current security offering based on the *F-Prot* engine.



The install process requires an Internet connection, with the initial installer no more than a downloader – only 450KB in size. This fetches the main installer, which is also fairly small at 3MB, and which proceeds to fetch the other components required. The process is not too long or taxing, but a reboot is needed at the end.

The interface is attractive and simply laid out, with minimal clutter, and provides a decent level of configuration in a pleasantly accessible style. The only things missing were a setting to simply block or record detections without any automatic action, and the lack of an option to save log

data to a file – leaving us wrangling an ugly and ungainly database format into shape to retrieve results. Occasionally scans seemed to stop at random, and the awkward log format made it difficult to see how far they had gone, or even if any results had been saved. We also saw some scans claiming to have completed but clearly not having covered the full area requested. In the end, however, we managed to pull together what looked to be a complete set of results.

Speed measures were a little slow on demand, with some fairly heavy lag times on access, and with RAM use about average and impact on our suite of tasks average too, CPU use was fairly high.

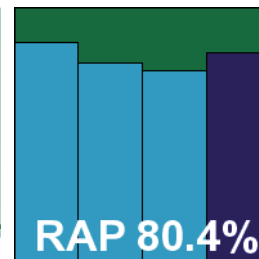
Our decryption of the logs we gathered showed some fairly respectable scores in most areas, with no problems in the clean sets or with the on-demand scan of the WildList set. On access, however, the same large file which has tripped up a couple of other products was not spotted – probably due, once again, to a cap imposed on the file size to scan, although we could find no visible information on this limit and no clear way to change it if desired. This missed detection was enough to deny *iolu* its second VB100 award, by a whisker. From three entries in the last two years the vendor now has two fails and one pass.

K7 Total Security 11.1.0025

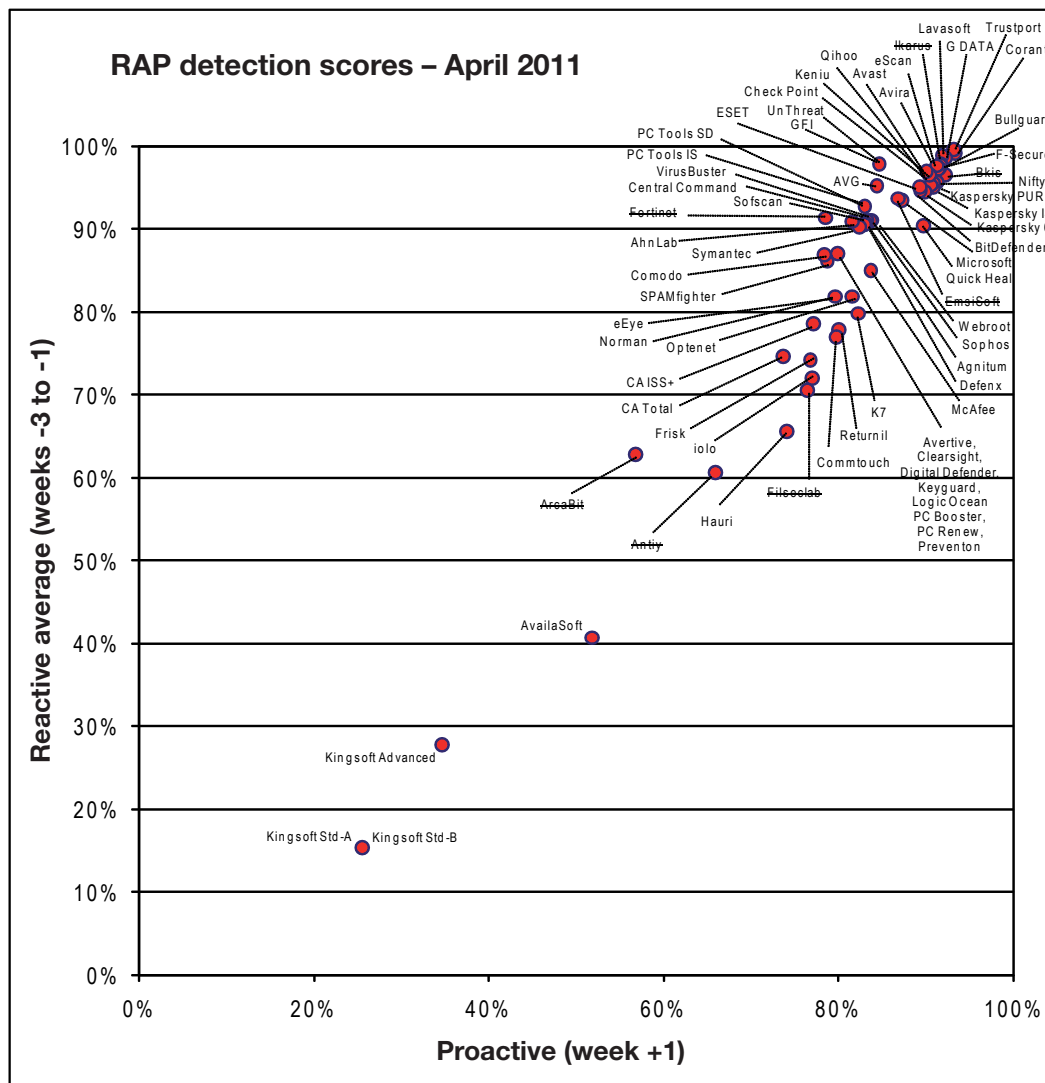
Malware definition version: 9.90.3942

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	84.52%
Worms & bots	95.92%	False positives	0

K7 Computing has become a regular in our tests over the last few years, building up a solid record of success and keeping the lab team happy with simple, reliable products.



The latest version was provided as a 71MB installer complete with all required definition data. The install process seems to consist only of a welcome screen and a EULA – in the blink of an eye everything is done and set up, with the product asking if it can be activated. No reboot is required and the process is all over in under ten seconds. This gives instant access to the interface, which is truly something to behold in an eye-watering collection of bright and gaudy reds, yellows, oranges and pinks. The layout, at least, is pleasant and



(Products with strikethrough generated false positives.)

Please refer to text for full product names.

simple, with good navigation, although it is somewhat wordy in places and we found it easy to click in the wrong place where a lot of options were clustered close together.

Running through the tests proved reasonably straightforward, although a couple of scan jobs seemed to have trouble traversing directory structures, occasionally only covering the first of several subfolders of the selected region.

We also hit a problem in the on-access test where a single item seemed to be tripping up the engine, causing a blue screen – several runs over the same batch of samples brought the same result, so the set was split into small chunks to get as much coverage as possible.

Scanning speeds were not very fast, but lag times were not very heavy, and system resource use was low, with a low impact on our set of activities. In the end detection results proved pretty solid too, with respectable scores in all sets, a gradual downturn through the RAP weeks and a slight rally in the proactive week – an unusual pattern that K7 has repeated in three comparatives in a row now.

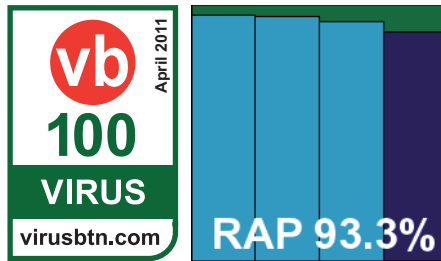
Both the WildList and the clean set were handled well, and another VB100 award is earned by K7 this month. The company now has a solid record of seven passes and one fail in the last 12 tests, with four not entered; in the last year, K7 has three passes from three entries.

Kaspersky Anti-Virus 6.0 for Windows Workstations

Version 6.0.4.1212 (a)

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	91.04%
Worms & bots	99.24%	False positives	0

This month sees a trio of entries from *Kaspersky Lab* – which, until it skipped last year's *Linux* test, was the only vendor with a 100%



record of participation in our comparatives since the VB100 award was introduced in 1998.

The product family has evolved considerably over the years. The rather modest title of this, the vendor's business-focused solution, conceals the multi-faceted nature of what is really a fairly complete suite, including anti-spam, device control and intrusion prevention alongside the anti-malware. The installer is not too huge though, at just under 150MB, and is accompanied as usual by a large archive containing all updates for the company's wide range of products. The set-up process is fairly lengthy, going through a number of stages including disabling the *Windows Firewall*, the option to set a password to protect the product settings, and analysis of applications allowed to connect to the network, alongside more standard items like licensing, updates and so on. It requests a reboot to finish things off.

The interface is cool and stylish, with perhaps a little too much emphasis on the funkiness – an odd approach to blending text links and buttons is occasionally confusing, but as a whole it is generally workable, improving greatly with a little familiarity. Fine-tuning is provided in exhaustive depth, with detailed reporting as well, and things were generally smooth and stable. At one point we observed the product crashing, having snagged on a single file in the RAP sets, but when the offending item was removed everything ran through without problems.

File access lags were low, and scanning speeds pretty good, improving immensely in the warm runs. Memory usage was also low, with CPU use a little higher than most, and in the activity test a fairly high impact was observed on the time taken to complete the task.

Detection rates, when finally analysed after the very slow process of exporting log files, proved to be excellent,

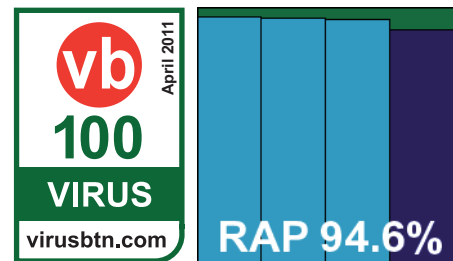
with only a very slight decline across the RAP sets. The WildList and clean sets were handled expertly, comfortably earning *Kaspersky* a VB100 award for its business solution. The product's recent record is pretty solid, with nine passes and two misses in the last two years, with just the one test not entered. The last six tests show five passes.

Kaspersky Internet Security 2011

Version: 11.0.2.5556 (a)

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	90.73%
Worms & bots	97.52%	False positives	0

Kaspersky's consumer suite solution will be a familiar sight to anyone who frequents retail software outlets, with its metallic green packaging.



It has been a semi-regular participant in our comparatives for a couple of years now, usually appearing alongside the business variant already discussed here.

The installer is somewhat smaller at 115MB, and the set-up process is considerably simpler, with only a few standard steps, a few seconds processing and no reboot to complete. The interface looks much like the business version, and the usage experience is pretty similar. We found it occasionally slow to respond, and once again found some of the buttons less than clear to use. However, the level of control available was excellent and stability was generally fine, with the known-bad file removed from the RAP sets in advance to ensure a steady run through. Once again, exporting logs was slow but sure.

Memory consumption was fairly low, and CPU use not too high either, while scanning speeds were pretty fast, again speeding up massively in the warm runs. Once again there was a fairly significant impact on the time taken to complete our suite of activities.

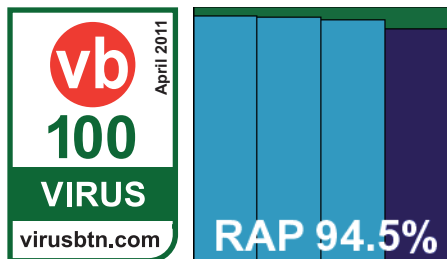
Detection rates were splendid, with excellent scores in all sets. Perfect coverage of the WildList and clean sets comfortably earns *Kaspersky* a second award this month. Our records for the consumer product line look pretty good, with seven passes, a single fail and one test skipped since first appearing in December 2009. Five of the last six entries have earned certification.

Kaspersky PURE

Version: 9.1.0.124 (a.b)

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.43%
Worms & bots	99.43%	False positives	0

PURE is a fairly new arrival from *Kaspersky*, an extension of the suite concept while promising an even broader range of protection. This is its first appearance on our test bench.



Much like the standard suite offering, the installer is around 120MB and, coupled with the same update package shared by its stable mates, it runs through very rapidly, the whole job being over with in less than half a minute with no restart needed. The GUI eschews the company’s traditional deep greens, opting instead for a pale, minty turquoise, and has a somewhat simpler and clearer layout – although it sticks to the practice of blending buttons and links in places. Again, an enormous amount of fine-tuning is provided under the hood, with the controls generally easy to find and use, and the overall experience felt nimbler and more responsive than the previous offering.

Scanning speeds closely mirrored those of the rest of the range, while on-access lags were a little heavier. RAM usage was on the low side and CPU use a little high, with impact on the set of activities quite high too.

Detection rates were very similar to the *I.S.* product, with superb scores in all sets. A clear run through the core certification sets earns *PURE* a VB100 award on its first attempt.

Keniu Antivirus 1.0

Program version: 1.0.5.1142; virus definition version: 2011.02.23.1008

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	99.83%	Trojans	93.57%
Worms & bots	99.45%	False positives	0

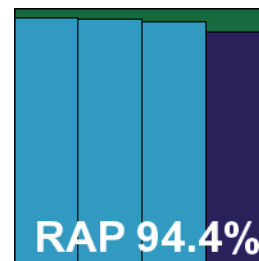
Keniu has been a regular participant in the last few tests, having first entered in the summer of last year. The company has recently formed an alliance with fellow

Chinese security firm *Kingsoft*, but so far there have been no signs of a merging of their solutions, with *Keniu* still based on the *Kaspersky* engine.

The install package is a fraction under 100MB, including all required updates, and the set-up process is fast and simple, with only a few steps, no need to reboot and everything done in less than a minute. The interface is bare and minimalist, with two basic tabs, a few large buttons and a basic set of configuration controls. With sensible defaults and smooth stable running the tests were out of the way in no time.

Scanning speeds were somewhat on the slow side, especially in the archives set, with archives probed very deeply by default. RAM and CPU usage were on the low side, and impact on our activities bundle was not too high.

Detection rates were excellent, as expected from the solid engine underpinning the product, with very high figures in all sets. The clean set threw up no problems, and the WildList was handled fine on demand, but in the on-access run a single item was marked as missed by our testing tool. Suspecting an error, we reinstalled and repeated the test, this time finding several dozen items missed, including the one not spotted the first time, and the product’s internal logs matched those of our testing tool. Running a third install showed another selection of misses – even more this time. In the end, no changes to the product settings or the way the test was run could prod the product into functioning properly. This rather baffling result denies *Keniu* a VB100 award this month; the vendor’s record shows three consecutive passes in its earlier three entries.

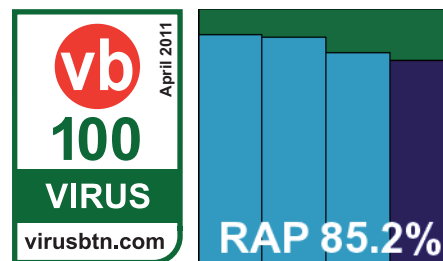


Keyguard Internet Security Antivirus 1.1.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Another from the family of products based on the *Preventon* set-up, *Keyguard* was a last-minute addition to this month’s



list, our first contact with the company coming on the submission deadline day itself.

The familiar 67MB installer was pushed through its set-up in good order, with the usual connection to the Internet required to activate and access controls. The *Keyguard* version of the interface has a pleasant spring green colour scheme, with the usual simple but lucid and usable layout and solid levels of stability.

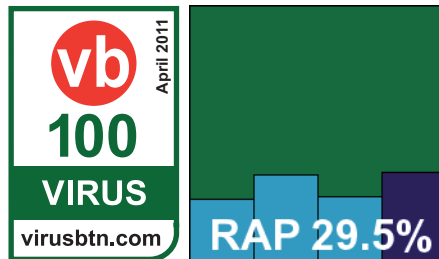
Speeds and overheads were all on the decent side, with low impact on file accesses and activities and low use of resources, while detection rates were decent and respectable. With no problems in the certification sets, *Keyguard* proves worthy of a VB100 award on its first attempt.

Kingsoft Internet Security 2011 Advanced

Program version: 2008.11.6.63; engine version: 2009.02.05.15; data stream: 2007.03.29.18; virus definitions: 2011.02.24.02

ItW	100.00%	Polymorphic	96.04%
ItW (o/a)	100.00%	Trojans	16.70%
Worms & bots	39.45%	False positives	0

Kingsoft is a major player in the Chinese market, and has been a regular in our comparatives since its first appearance in 2006. The



vendor came into this month's test looking for a change of fortune, after a string of tricky tests upset by problems with polymorphic viruses in our WildList sets.

The vendor's 'Advanced' version came as a compact 68MB installer, which runs through simply in a handful of standard steps with no reboot required. The product interface is bright and cheerful – not the most visually appealing, but clean and simply laid out, with a basic but functional set of configuration controls. Operation was stable and solid throughout, and the tests were completed in good time.

Scanning speeds were not outstanding, but on-access lag times were not bad, and while RAM use was a little higher than some, CPU use was below average, as was impact on our suite of standard activities. Detection rates were far from stellar, with low scores in all our sets. The trojans set was particularly poorly covered, and RAP scores fluctuated unpredictably but never achieved anything close to a decent level. Nevertheless, the core certification requirements were

met, with no problems in the WildList or clean sets, and a VB100 award is duly earned. The last two years show six passes and four fails, with only the two *Linux* comparatives not entered; three of those fails were in the last six tests.

Kingsoft Internet Security 2011 Standard-A

Program version: 2008.11.6.63; engine version: 2009.02.05.15; data stream: 2007.03.29.18; virus definitions: 2011.02.23.08

ItW	100.00%	Polymorphic	96.04%
ItW (o/a)	100.00%	Trojans	8.47%
Worms & bots	35.68%	False positives	0

Kingsoft has routinely entered its 'Standard' product alongside the 'Advanced' one, and this time offers two separate



variants on the theme ('Standard-A' and 'Standard-B'), although as usual they are hard to tell apart.

The install process is again fast and simple, and the interface clean, responsive and easy to navigate, with good stability allowing us to get through all the tests in good time.

Scanning speeds and lag times closely matched those of the 'Advanced' edition, while RAM use was a little higher and CPU use a little lower, with impact on our activity set a little higher too. As expected, detection rates were even worse, with some truly terrible scores in the RAP sets – the proactive week score bizarrely some way better than the others.

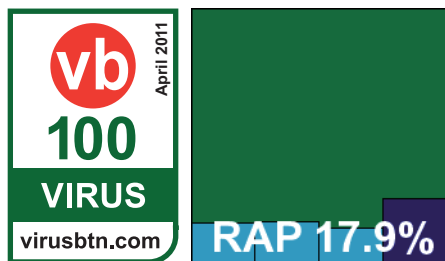
Despite this poor showing, the WildList set was covered fully and there were no issues in the clean sets, so a VB100 award is earned, just about. That makes for four passes and four fails in the last dozen tests, with four not entered; in the last year the product has had two passes and two fails, with two tests skipped.

Kingsoft Internet Security 2011 Standard-B

Program version: 2008.11.6.63; engine version: 2009.02.05.15; data stream: 2007.03.29.18; virus definitions: 2011.02.23.08

ItW	100.00%	Polymorphic	96.04%
ItW (o/a)	100.00%	Trojans	8.46%
Worms & bots	35.66%	False positives	0

There's not much more to say about the third entry from *Kingsoft*, with very little to distinguish it from the other two in terms of user experience, with the install process and interface identical to the other two. Even the fine detail of the version information is unchanged.



Scanning speeds were a little slower, and lag times a little higher in some cases, with more RAM consumed than either of the others, but fewer CPU cycles, while the impact on our activity suite was much the same.

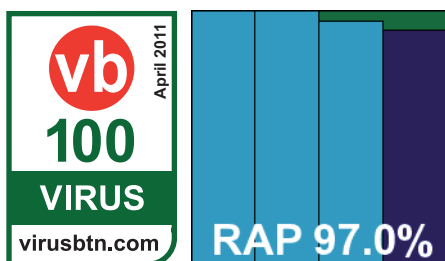
Detection rates were fairly abysmal, a fraction lower than the other 'Standard' edition, but the core certification requirements were met and a VB100 award is earned.

Lavasoft Ad-Aware Total Security

Anti-virus version 21.1.0.28

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.60%
Worms & bots	99.71%	False positives	0

Lavasoft first entered our comparatives in 2010, and has submitted both its standard product, based on the *GFI Sunbelt VIPRE*



engine, and this one, combining the might of *G DATA* with its own anti-spyware expertise, in several recent tests. The *Total* version has had some unlucky results recently, and has yet to achieve a VB100 award, despite some very strong performances. This month the standard product is absent pending fixes to some issues coping with the heavy stresses of our tests, but we were pleased to see the *Total* offering return for another stab.

The installer is something of a beast at over 450MB, but that includes all required update data for all the engines. The set-up process runs through a number of stages, including the options to include parental controls and a data shredder system, and setting up some scheduled scanning

and backup tasks, before the main installation. This runs for a minute or so, followed by a reboot.

The interface is very similar to *G DATA*'s, with a few extras and a little rebranding, and as such proved a delight to operate, with its excellent level of controls and solid, reliable running even under heavy pressure. All tests were out of the way well within the allotted 24 hours.

Scanning speeds were not super fast to start with but benefited hugely from the smart caching of previous results, and on-access lag times were not too heavy either. Use of RAM and CPU cycles, and impact on our set of activities, were perhaps slightly above average, but not too heavy.

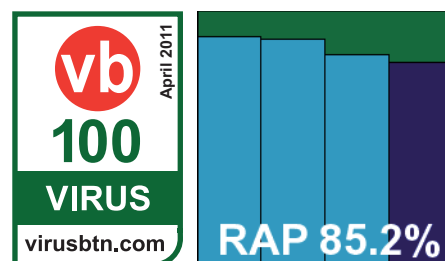
Most users would consider the reasonable system impact more than made up for by the superb detection levels achieved by the product, which destroyed our test sets with barely a crumb left behind. The RAP set closely approached complete coverage in the earlier two weeks, dropping off only very slightly. The WildList presented no difficulties, and finally the clean set was handled without incident either. *Lavasoft's Total* product earns its first VB100 award after its third showing.

Logic Ocean GProtect 1.1.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Yet another entry from the *Preventon* family, based on the *VirusBuster* engine, *GProtect* was another last-minute arrival, turning up right at the end of the submission deadline day.



This version of the solution had the same 67MB installer, running through the same handful of steps to get set up rapidly with no need to restart, although an Internet connection is needed to activate. The interface is a rather sickly blend of greens, oranges, purples and pastel blues, but with some turning down of the screen it is just about bearable, and provides the usual solid, if basic set of controls. Stability remained excellent, with no problems getting through the full test suite within the expected time.

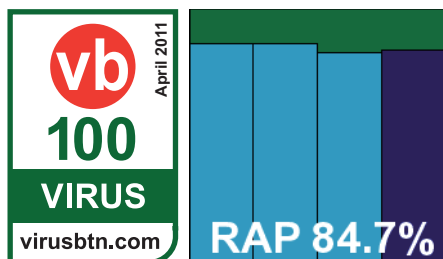
Scanning times were OK and lag times not too heavy, while RAM use and impact on our set of tasks were fairly low and CPU use not too high either. Detection rates were respectable, with no problems in the core sets, and *Logic Ocean* duly earns a VB100 award on its first attempt.

McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8

Scan engine version: 5400.1158; DAT version: 6266.0000

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	85.04%
Worms & bots	94.76%	False positives	0

McAfee has recently been having a bit of a tough time handling some of the polymorphic strains replicated in large numbers



for our test sets. However, with a lot of work having been put into ironing out these issues, things looked good for a return to form.

The product came as a 37MB installer with the DAT package measuring 85MB, and the set-up process was simple and straightforward, with a reboot not demanded but subtly recommended. The GUI remains grey and sober but efficient and simple to use. A full and complete range of controls is provided, as one would expect from a major corporate solution.

Running through the tests proved no great chore, as stability was rock-solid throughout and everything behaved just as expected. Scanning times were pretty good to start with and sped up enormously in the warm scans. Overheads were not bad either, and there was low drain on CPU cycles and minimal impact on our set of activities. Detection rates were pretty good, with a step down in the second half of the RAP sets, but the WildList was handled fine and the clean sets threw up only a handful of adware alerts – presumably from the anti-spyware component which has been added to the product title since previous entries.

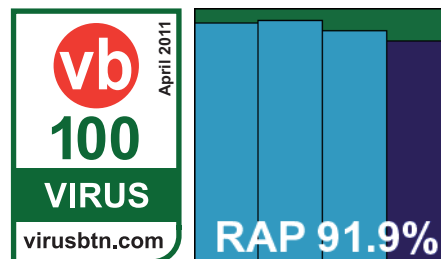
A VB100 award is duly earned, doubtless to great relief at *McAfee*, making two passes and two fails from four entries in the last six tests; the two-year picture is much brighter, with eight passes and two fails, with two tests not entered.

Microsoft Forefront Endpoint Protection 2010

Version: 2.0.657.0; anti-malware client version: 3.0.8107.0; engine version: 1.1.6502.0; anti-virus definition version: 1.97.2262.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	90.96%
Worms & bots	99.12%	False positives	0

Microsoft has generally alternated its *Forefront* and *Security Essentials* products in our server and desktop tests



respectively, but this pattern is shaken up a little this month with the corporate product appearing.

The installer is compact at 19MB, with 63MB of updates also provided. The set-up process is fairly simple, with a half-dozen steps to click through and no reboot required, and all is done with in under a minute. The product interface is similarly brief and to the point, only providing a minimal set of controls and in some places mincing words to a rather confusing degree. However, it is generally usable and it ran stably throughout the test suite. From past experience we knew to expect long scanning times over large sets of infected samples, but leaving this over a weekend proved a successful tactic and no testing time was wasted.

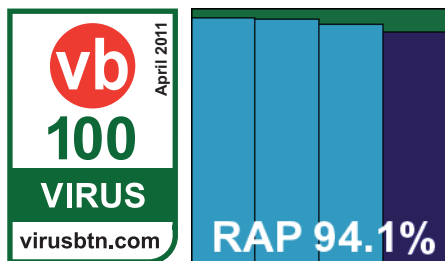
Over clean files scan times were not too bad, and on-access measures proved fairly light, with low use of resources and one of the fastest average times taken to complete our set of tasks. Detection rates were pretty solid, with a very gradual decline across the RAP sets, and the WildList set proved no problem at all. Our clean set threw up only a handful of adware alerts, hinting that we may want to clean out some of the less salubrious items from the popular download sites, and a VB100 is thus comfortably earned. *Forefront* has taken part in only five tests in the last two years, only two of the last six comparatives, but has an excellent record with every entry achieving certification.

Nifty Corporation Security 24

Version 3.0.1.50; client 5.63.2

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.53%
Worms & bots	99.45%	False positives	0

Nifty has become a regular participant in our comparatives, the Japanese brand providing its own quirky interface over the *Kaspersky* engine, and showing no signs of adding translated versions. As usual, therefore, we relied heavily on usage instructions included with the submission, aided somewhat by our limited ability to understand the markings on the interface.



The install process seemed to require that Japanese language support be added to the system, rather sensibly, but even then much of the display was garbled and not usable as a guide. It ran through half a dozen or so incomprehensible steps before rebooting the system. On boot up, we found the GUI as strange and interesting as ever, with quirks both in layout and operation; it frequently fades into semi-transparency when not focused on. Nevertheless, it seemed fairly stable, and proved OK to operate as long as no complex configuration was needed.

As in previous tests, on-demand scans over infected sets took an enormously long time. No real reason could be found for this; the main cause of such slowdowns elsewhere is the foolish attempt to store all log data in RAM until the end of the scan, but here the standard *Windows* event system is used as the only available logging, and memory use did not seem to increase too dramatically. Scans would simply start off very rapidly and gradually slow to a crawl. So, having prepared for this, we set the product up on several systems at once and ran various jobs over the weekend, with most of them finished by Monday. In total around five full machine days were used up getting through the tests – considerably more than the allotted 24 hours.

No such problems were encountered when scanning clean files though, with a light touch in the on-access lag measures and initially sluggish on-demand scans speeding up hugely for the warm runs. CPU use was perhaps a little higher than average, but RAM use and impact on our activities were fairly standard.

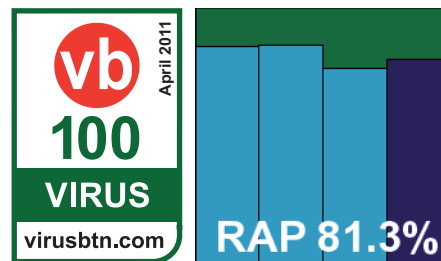
As expected from the *Kaspersky* engine, detection rates were excellent across the board, with little missed anywhere, and with no issues in the core certification sets *Nifty* earns another VB100 award. The product has taken part in all six desktop tests in the last two years, failing only once; the last six tests show three passes from three entries.

Norman Security Suite 8.00

Product Manager version 8.00; anti-virus version 8.00; scanner engine version 6.07.03; NVC version 8.1.0.88

ItW	100.00%	Polymorphic	99.98%
ItW (o/a)	100.00%	Trojans	86.80%
Worms & bots	89.16%	False positives	0

Norman has hit its stride again recently after a run of difficulties, and is now back on a winning streak with no problems encountered in the last few tests. The vendor returned this month doubtless hoping to continue its streak of success.



The *Suite* solution was provided as a 112MB installer, including all the required updates, and it ran through in only a handful of steps. The process was all over in good time, but needed a reboot to complete. The interface is a little bizarre at times, for a start being a little too large for the browser-based window it is displayed in, thus requiring a pair of scroll bars which only move a tiny way. The window size is locked so the issue cannot be fixed by the user. The layout is unusual and sometimes confusing, with a limited set of options and a quirky approach to just about everything – but with practice and patience it is just about usable. Less forgivable is its disregard for instructions, with samples routinely removed or disinfected despite all settings being firmly set to avoid such behaviour. Otherwise stability seemed good, with no hitches to prevent us completing the set of tests in good time.

What did impede things somewhat was the scanning speed, which was slow in the extreme, mainly thanks to the sandbox component looking at things in great depth. As we have suggested here before, this might benefit from some sort of memory of what it's already run to avoid such unnecessary duplication of work. On-access lag times were also fairly high, and use of CPU cycles was well up too, although RAM use was not much above average and our set of tasks was completed in reasonable time.

Detection rates were not bad, with respectable scores throughout the sets, and once again the WildList was handled well. The clean sets threw up only a single suspicious alert, on a rather bizarre piece of software which claimed to be an entertaining game but in fact seemed to simulate the experience of driving a bus. Being quite

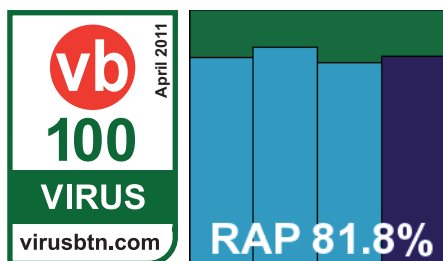
forgiven for this result, *Norman* earns a VB100 award once again, making a total of four passes and two fails in the past six tests, with the longer view showing six passes and four fails, with two tests not entered, in the last two years.

Optenet Security Suite V. 10.06.69

Build 3304; last update 21 February 2011

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	76.74%
Worms & bots	91.82%	False positives	0

Optenet first entered our tests at the end of last year with a successful run on *Windows 7*, and returns for more of the same. Based on the ever popular *Kaspersky* engine, its chances looked good from the off.



The product installer was 105MB including updates, and ran through a series of set-up steps including the providing of a password to protect the settings and a request for online activation before a reboot was requested to complete the process.

The interface is another browserly affair, which can be a little slow and occasionally flaky, but it is at least clearly laid out and provides a reasonable level of fine-tuning. From a tester's point of view the most annoying aspect is the tendency to log out and require a password every time it is revisited after more than a few moments.

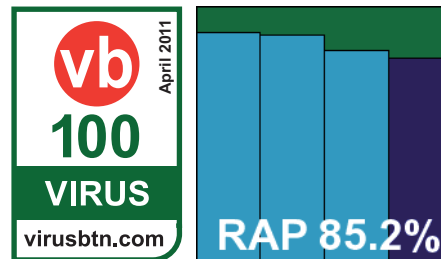
Scanning speeds were reasonable, but on-access lag times seemed a little high, and while resource use was fairly low our suite of standard jobs took a while to run through as well. Detection rates were pretty solid, with a lot of partial detections ruled out under our rules thanks to being labelled as 'suspicious' only. The clean set threw out none of these alerts though, and certainly no full detections, and with the WildList covered admirably *Optenet* earns another VB100 award, making it two from two attempts.

PC Booster AV Booster 1.1.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

This is the second time on the test bench for *PC Booster*, whose product is another in the *Preventon* line. The vendor's



previous entry, in last December's *Windows 7* test, was thrown off course by an unlucky technicality, with the on-access component not checking packed files on read or on write. This month, given the results of a plethora of similar products, all seemed to be on course for a smoother run.

The installer was once again 67MB and completed in a few simple steps, with no reboot but a brief spell online required to activate a licence for full functionality. The interface has a crisp, cool blue-and-white colour scheme, with the layout unchanged from the rest of the range; tests ran through according to a well-oiled schedule, completing in good order with no stability issues.

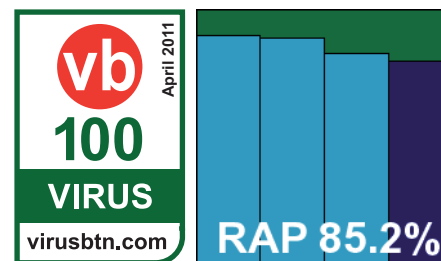
Speeds were average on demand, and reasonable on access, with no outrageous drain on system resources, and our set of jobs ran through in decent time. Detection rates were respectable, with decent coverage in all areas. With no issues in the main certification sets *PC Booster* qualifies for its first VB100 award.

PC Renew Internet Security 2011

Version 1.1.48; definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

Yet another from the same stable, *PC Renew* – appearing for the first time this month – makes rather cheeky use of the



standard phrase 'internet security', generally used to imply a multi-layered suite product but here providing little more than standard anti-malware protection, based on the common *VirusBuster* engine.

With no change in the set-up process or interface, the only other area worth commenting on is the colour scheme, which here stuck to a fairly standard blue and white, with a touch of warmth in the orange swirl of the logo. For some reason some of the speed tests seemed a fraction slower than other similar products, but only by a few seconds a time, and on-access measures reversed the trend by coming in a touch lighter. Resource use was also fairly similar to the rest of the range, being reasonably light in all areas and not impacting too heavily on our set of standard tasks.

Not surprisingly, detection rates were not bad either, with no serious complaints in any of the sets, and with the core sets covered without problems another newcomer joins the list of VB100 award winners.

PC Tools Internet Security 2011S

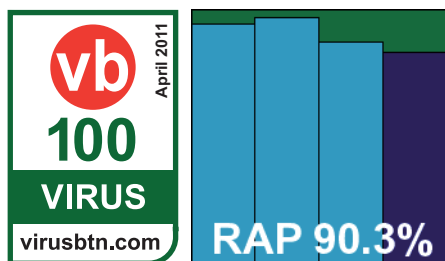
Version 2011 (8.0.0.624); database version 6.16970

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.85%
Worms & bots	98.44%	False positives	0

PC Tools' products have been fairly regular participants in our tests since 2007, although the *Internet Security* line has only

taken part since 2009, following the company's takeover by *Symantec*. After a slightly wobbly start the product has amassed a good run of passes of late. Although the underlying detection technology has changed considerably, the look and feel remains much as it did when we first tested it several years ago.

The install package was fairly large, at 209MB, and ran through a fairly standard set of stages. Towards the end, the machine froze completely, not responding to any stimulus, and a hard restart was required. After that all seemed fine though, and a subsequent reinstall did not reproduce the problem. The interface is clear and friendly, with large status indicators covering the firewall, anti-spam and various 'guard' layers, but configuration of the latter is fairly basic, generally limited to on or off. Tests proceeded rapidly, although at one point while scanning the main clean set the scanner – and indeed the whole system – froze once again and a push of the reset button was required, but even with this interruption and the re-run it necessitated,



the complete set of tests was finished within the allotted 24 hours.

Scanning speeds were fairly slow to start off with but sped up hugely on repeat runs. On-access overheads were light in some areas but heavy in others, notably our sets of media and documents and miscellaneous file types. Here, no sign of smart caching was evident – which is odd, given that it would be most useful in this mode. We could find no way of persuading the product to scan more than a defined list of extensions on access. Use of system resources was fairly high in all areas, and our suite of standard activities was quite heavily impacted, taking noticeably longer than usual to complete.

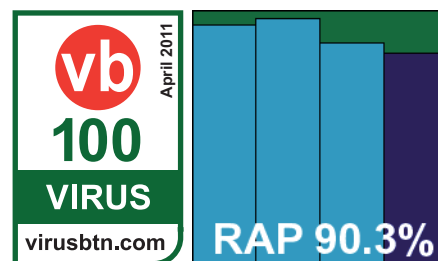
Detection results showed very good scores in most areas, with some excellent figures in the first half of the RAP sets, dropping off notably in the later two weeks. No problems cropped up either in the WildList set or (other than the one-off system freeze) in the clean sets, and *PC Tools* earns another VB100 award. The vendor's two-year history shows entries in all desktop tests, with five passes and a single fail from six entries; all three entries in the last six tests have resulted in passes.

PC Tools Spyware Doctor with AntiVirus 8.0.0.624

Database version 6.16970

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.85%
Worms & bots	98.44%	False positives	0

The second entry from *PC Tools* is the company's well-known *Spyware Doctor* brand, which has a long history in the



anti-spyware field. This also has a rather longer history in our tests than the *I.S.* version, dating back to 2007.

The product itself is fairly similar in look and feel, with the installer somewhat smaller at 185MB, and the set-up process running through the same set of stages – successfully this time – with no reboot requested at the end. The interface is also similar, although with fewer modules than the full suite edition, and provides fairly basic configuration controls.

Speeds and performance measures were pretty comparable, with slow cold speeds in the on-demand scans and much

faster in the warm runs. Fairly heavy lag times were observed in the same sets as for the *I.S.* product, but less so in the sets of archives and executables, and there was high use of memory and processor cycles and a fairly heavy slowdown when carrying out our set of tasks.

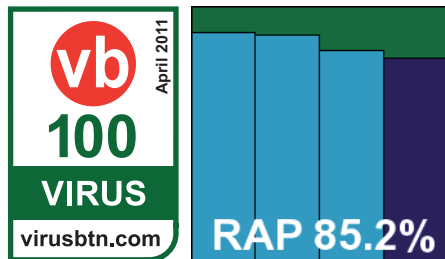
Detection rates were just about identical, with solid scores in the main sets and decent coverage of the RAP sets, declining from high levels in the earlier part to lower but still respectable levels in the latter half. The core sets proved no problem, and a second VB100 award goes to *PC Tools* this month. The *Spyware Doctor* line has an identical record to the suite, with six entries in the last dozen tests, the last five of them passes.

Preventon Antivirus 4.3.48

Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.49%
Worms & bots	95.91%	False positives	0

The daddy of them all, *Preventon's* own product has been entering our tests since late 2009, with a record of strong



performances occasionally upset by minor technicalities.

The install and user experience is much like the rest of the range, with the installer a fraction larger at 69MB but the process unchanged, completing quickly with no reboot but needing a connection to the web to apply a licence and to access full configuration. The GUI remained stable and usable throughout our tests, with its simple set of options allowing us to progress rapidly through them, completing within 24 hours as usual.

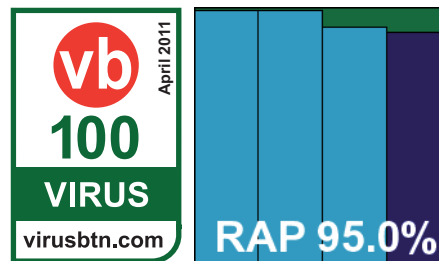
Speeds were (unsurprisingly) fairly similar to the rest of the group, perhaps a fraction slower but no more than can be attributed to rounding errors and so on. Performance measures showed the expected light use of resources and a nice low impact on our suite of tasks. Detection rates were fairly steady across the sets and there were no issues in the clean or WildList sets, thus *Preventon* earns another VB100 award. Having entered five of the last nine tests, *Preventon* now has three passes under its belt, with one pass and two unlucky fails in the last year.

Qihoo 360 Antivirus 1.1.0.1316

Signature date 2011-02-19

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.25%
Worms & bots	99.65%	False positives	0

Qihoo (apparently pronounced 'Chi-Fu') is another of the wealth of solutions active in the bustling Chinese



market space – this one based on the *BitDefender* engine. Having entered our tests on several occasions in the last couple of years, the product has a decent record of passes – but has also put us through some rather odd experiences.

The latest version came as a 110MB install package, including signatures from a few days before the submission deadline. Set-up was fast and easy, with no need to restart and the process was complete in half a minute or so. The interface is fairly attractive, with bright colours and clear icons, a decent level of configuration options and a decent approach to usability.

Stability seemed OK, and the oddities noted in previous tests were kept to a minimum. However, once again we noted that, although the on-access component claimed to have blocked access to items, this was not the experience of our opener tool, and often the pop-ups and log entries would take some time to appear after access was attempted (and apparently succeeded) – implying that the real-time component runs in something less than real time.

This approach probably helped with the on-access speed measures, which seemed very light, while on-demand scans were on the slow side. RAM consumption was high, although CPU use was about average, and impact on our set of everyday jobs was not heavy.

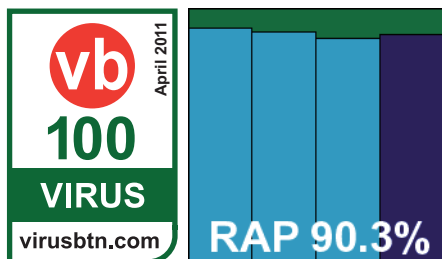
Detection rates, when finally pieced together, proved just as excellent as we expect from the underlying engine, with very high scores in all areas, and with no issues in the core sets a VB100 award is duly earned. Since its first entry in December 2009, *Qihoo* has achieved six passes and a single fail, with three tests not entered; the last six tests show three passes and a fail from four entries.

Quick Heal Total Security 2011

Version: 12.00 (5.0.0.2), SP1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	82.64%
Worms & bots	92.72%	False positives	0

Quick Heal is one of our more venerable regulars, with entries dating back to 2002 – and the vendor hasn't missed a test since way back in August 2006.



The current product revels in the now popular 'Total Security' title and offers a thorough set of suite components, including all the expected firewalling and anti-spam modules. As such, the installer package weighs in at a sizeable 205MB. The set-up process is fast and easy though, with only a couple of steps to click through and less than a minute run time, with no reboot needed.

The interface is glitzy and shiny without overdoing things, and has a slightly unusual, but not unusable design. Options – once they have been dug out – are fairly thorough, and stability was good, allowing us to zoom through most of the tests in good time. We had some problems with some of our performance measures, where some of the automation tools were apparently being blocked by the product, and at one point a scheduled job we had prepared to run overnight failed to activate. However, it's possible that we missed some important step out of the set-up procedure. Nevertheless, we got everything done in reasonable time.

Scanning speeds were OK in some areas but a little on the slow side in others, while on-access lag times were a little heavy. Memory use was a little on the high side, but CPU use was not too bad, and our set of tasks was completed in good time.

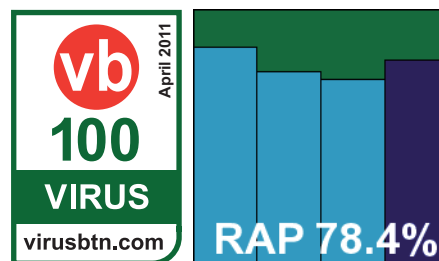
Detection rates proved pretty decent across the sets, and had 'suspicious' detections been included in the count they would have been considerably higher. The core certification sets were well handled, and a VB100 is well deserved by *Quick Heal*. The vendor's record shows ten passes and two fails in the last two years, with all of the last six tests passed.

Returnil System Safe 2011

Version 3.2.11937.5713-REL12A

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	78.88%
Worms & bots	91.46%	False positives	0

We first looked at *Returnil*'s offering last summer (see *VB*, August 2010, p.21), when it went by the name 'Virtual System' in



reference to the sandboxing/virtualization set-up that is at the core of its protective approach. It also includes the *Frisk* malware detection engine, which is the main aspect we looked at on this occasion.

The installer is compact at only 40MB, and takes only a few moments to complete, with a reboot requested after 30 seconds or so. The interface is bright and colourful, and fairly easy to use, although the configuration section seems mainly focused on the virtualization system and on providing feedback on incidents, with little by way of actual options for the scanning or protection. With sensible defaults and good stability though, testing progressed nicely and was completed in short order.

Scanning speeds were rather slow, and on-access lags a little heavy, with low use of memory and minimal impact on our suite of tasks, but very heavy use of CPU cycles.

Detection rates were pretty decent in most sets, with a slow decline in the RAP sets and once again that slight and unexpected upturn in the proactive week. The core sets were handled well, and *Returnil* earns another VB100 award. Having entered four of the last five tests, skipping only the recent *Linux* test, *Returnil* can now boast three passes and only a single fail.

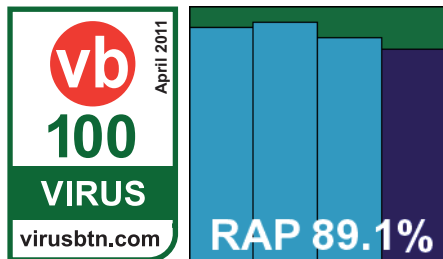
Sofscan Professional 7.2.27

Virus scan engine 5.2.0; virus database 13.6.217

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.90%
Worms & bots	96.33%	False positives	0

Another new name but not such a new face, *Sofscan* was another last-minute arrival with its product closely modelled

on some others taking part this month, and the test's most popular detection engine once again driving things.



The installer package measured 66MB, with an extra 62MB zip file containing the latest updates. The set-up process featured all the usual steps including, as we have observed with a few others this month, the option to join a community feedback system and provide data on detection incidents. This was disguised as the 'accept' box for a EULA and was pre-selected by default. It doesn't take long to get set up, and no reboot is needed to complete.

The interface is a familiar design, dating back many years now and showing its age slightly in a rather awkward and fiddly design in some areas, but providing a decent level of controls once its oddities have been worked out. Operation seemed a little wobbly at times, with some tests throwing up large numbers of error messages from *Windows*, warning of delayed write fails and other nasties. We also experienced problems with logging to memory rather than disk once again, with our large tests slowing to a crawl and taking days to get through. Worried by the repeated write warnings, we broke things up into several jobs and re-imaged the test system in between runs, and eventually got everything done, after about four full days of run time.

Scanning speeds came in rather slow, and lags were pretty heavy, with high use of system resources – processor drain was particularly high. Impact on our suite of activities was not too significant though. Detection rates were pretty good, tailing off somewhat in the RAP sets but showing good form in the core certification tests and earning *Sofscan* its first VB100 certification.

Sophos Endpoint Security and Control 9.5

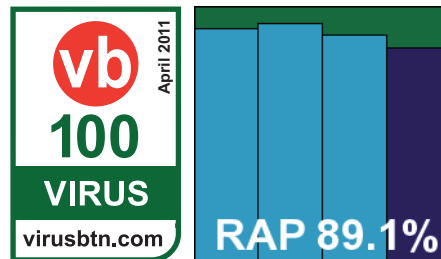
Sophos Anti-Virus 9.5.5; detection engine 3.16.1; detection data 4.62G

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	91.70%
Worms & bots	87.69%	False positives	0

Sophos is another of our most regular participants, with a history going all the way back to 1998 and only two tests not entered, both of which were over five years ago.

The vendor's main product is provided as a 75MB installer, with additional, incremental updates in a svelte 4MB

package. Set-up follows the usual path, with a few corporate extras such as the removal of 'third-party products' (i.e. competitor



solutions), and the option to install a firewall component, which is unchecked by default. No reboot is needed to finish the process, which is completed in under a minute.

The interface is stern and sober with little unnecessary flashiness, providing easy access to standard tasks and settings, with some extreme depth of fine-tuning also available if required. HIPS and 'live' online lookups are included, but not covered by our testing at the moment – the live component had to be disabled to avoid delays in our tests. Stability was solid, with no problems under heavy pressure, and testing ran through in decent time.

Speed times and on-access lags were good with default settings where only a preset list of extensions are covered. With a more in-depth set of settings only the archive set was heavily affected, the others still getting through in good time. Resource consumption was low and our suite of standard tasks ran through quickly with little time added.

Detection rates were solid, with good coverage across the sets and a slow decline into the most recent parts of the RAP sets. The core certification sets proved no problem, and *Sophos* comfortably earns another VB100 award. The company's recent records show only a single fail and 11 passes in the last two years, with all of the last six tests passed with flying colours.

SPAMfighter VIRUSfighter 7.100.15

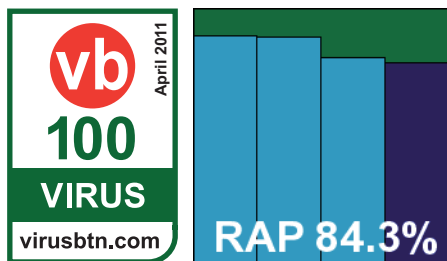
Definitions version 13.6.215

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	86.37%
Worms & bots	95.91%	False positives	0

The people behind *VIRUSfighter* specialize in fighting spam (as the company name makes admirably clear), but have been producing anti-malware products for some time too. When we first looked at their solutions they were using the *Norman* engine, but of late they have been based on *VirusBuster*, using the *Preventon* SDK but adding a fair amount of their own work to things.

The installer came in at 68MB including all updates, and the set-up process was zippy and to the point, with a request

for the user's email details the only notable aspect. Everything is done in under a minute, with no need to reboot. The interface is a



khaki green, the logo adorned with military chic, and the layout fairly clear and simple. Some options were a little baffling though – checkboxes marked 'turn on/off' beg the question of whether checked means on or off. Although the layout is different, much of the wording is similar to other products based on the same SDK, with perhaps a few extra settings over and above those provided by the others. We also found that registry entries used elsewhere to ensure logs were not thrown out after a certain time were missing, or at least not where we expected, so we had to run tests in smaller jobs to ensure all data was kept for long enough for us to harvest it.

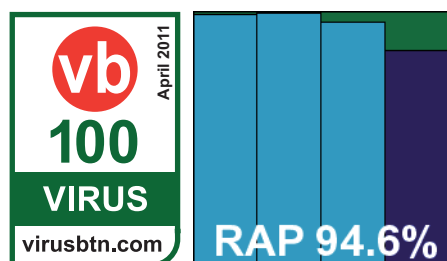
Speeds were much as expected: fairly average on demand but pleasantly light on access, with fairly low use of resources and little impact on standard tasks. Detection rates were also respectable, with a decline into the later parts of the RAP sets but no serious issues, and full coverage of the WildList and clean sets. A VB100 award thus goes to *SPAMfighter*, its second from five entries in the last seven tests.

GFI/Sunbelt VIPRE Antivirus 4.0.3904

Definitions version: 8516; VIPRE engine version: 3.9.2474.2

ItW	100.00%	Polymorphic	99.79%
ItW (o/a)	100.00%	Trojans	97.99%
Worms & bots	99.67%	False positives	0

The *VIPRE* product has been taking part in our tests for 18 months or so now, with some decent results and, in recent tests at least, signs of



overcoming some nasty issues with stability which made its earlier appearances something of a chore.

The installer is pretty small at only 16MB, but contains no detection data initially, requiring the extra 62MB of the standard installer bundle to get things fully set up. The initial job is thus very rapid, with just a couple of clicks required, and all is complete in about ten seconds, before a reboot is demanded. After the reboot a set of set-up stages must be run through, and a demo video is offered to guide one through using the product. This is probably not necessary for most users, with the GUI fairly simple and clearly laid out, and with little by way of fine controls to get lost in – most areas seem limited to little more than on or off. Thankfully stability was generally good, even in the on-access runs which have given us some problems in the past. However, it remains unclear what the product's approach to actions on detection is, with some runs seeming to go one way and others another.

Scanning times were very slow over some sets, such as our collection of media and document files, but surprisingly quick over executables, which one would expect to be looked at most closely. On-access lag times showed a similar pattern, with some good speed-up in the warm runs improving things considerably. Resource use was low in terms of memory but perhaps a fraction above average in CPU use, and impact on our suite of activities was barely noticeable.

Detection rates were excellent, continuing a steady upward trend noted over several months. The RAP scores were very high in the reactive weeks, with something of a drop in the proactive week as expected. The clean sets were covered without problems, and after double-checking a selection of files which were not initially denied access to but alerted on slightly behind real time, the WildList set proved to be well handled too. A VB100 award is thus well earned, making for four passes and a single fail in the vendor's five entries so far; the last year shows three passes and three no-entries.

Symantec Endpoint Protection 11.0.6200.754

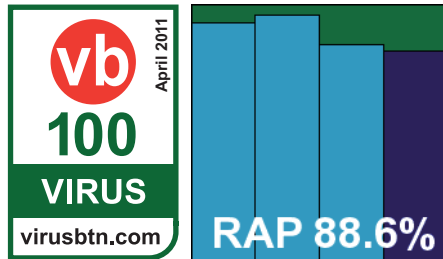
Definitions: 21 February 2011 r2

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.13%
Worms & bots	98.25%	False positives	0

Symantec is another long standing regular in VB100 testing, but has been somewhat unpredictable in its entries of late, with its last appearance as long ago as August 2010. Finally back on our list, we expected to see a solid performance.

The installer seemed to cover the entire corporate product range, with multiple platforms supported and management

tools etc. included, so weighed in at a chunky 1.3GB. For the standalone anti-malware solution the set-up process was fairly short and simple though, running through a standard set of stages for a business product, and offering to reboot at the end, but not demanding one immediately. The interface is fairly bright and colourful for a corporate offering, with large, clear status displays. A hugely detailed range of controls can be found under the hood, again with a clear layout and good usability.



Scanning speeds were good in most areas – slower than most over archive files thanks to scanning internally by default, while on-access lag times were perhaps a little on the heavy side but nowhere near some of the extremes seen this month. Resource usage was a little above average, but a good time was recorded over our suite of standard tasks.

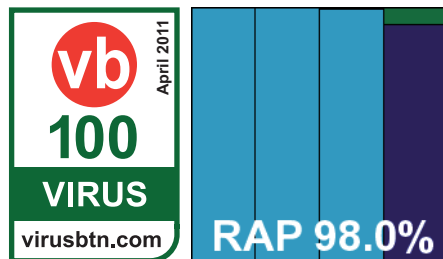
Detection rates were pretty good, with a fairly sharp drop through the RAP sets but solid coverage in most areas, and the core certification sets caused no unexpected issues, thus comfortably earning *Symantec* a VB100 award this month. After several tests skipped, the company’s test history now shows six passes and a single fail over the last two years, with two entries (both passed) in the last six tests.

Trustport Antivirus 2011

11.0.0.4606

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.16%
Worms & bots	99.85%	False positives	0

Trustport is one of the handful of multi-engine products that routinely vies for the highest set of scores in our tests, marking out the top right corner of our RAP quadrant as its own. We have been testing the vendor’s products since June 2006, during which time a range of engines have been used, but of



late the company seems to have settled on a fairly winning combination of *BitDefender* and *AVG*.

The twin cores make for a fairly large install package, although not too huge at 188MB including all required updates. The set-up process is fairly speedy, with no deviations from standard practice, and all is done in a minute or so with no need to restart.

The interface is a little unusual, with multiple mini-GUIs rather than a single unified console, but it proves reasonably simple to operate with a little exploring, and provides a solid set of controls, as one would expect from a solution aimed at the more demanding type of user. Under heavy pressure the interface can become a little unstable, occasionally doing strange things to general windowing behaviour too, and we observed log data being thrown away a few times despite having deliberately turned the limits to the (rather small) maximum possible. We had no major problems though, and testing took not too much more than the assigned 24 hours.

Scanning speeds were a little on the slow side, particularly over archives, thanks to very thorough default settings, and on-access lag times were fairly heavy too. Although resource usage looked pretty good, we saw quite some impact on our set of standard activities.

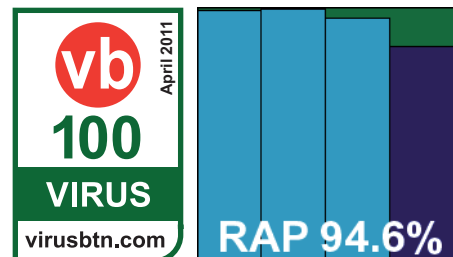
This heaviness was more than counterbalanced by the detection rates though, which barely dropped below 99% in most areas, with even the proactive week of the RAP sets showing a truly superb score. The *WildList* was brushed aside, and perhaps most importantly the clean set was handled admirably, easily earning *Trustport* another VB100 award. The company’s recent test record is excellent, with nine passes in the last dozen tests, the other three not entered; the last year shows four passes from four entries.

UnThreat Antivirus Professional 3.0.17

DB version: 8516

ItW	100.00%	Polymorphic	99.79%
ItW (o/a)	100.00%	Trojans	97.99%
Worms & bots	99.67%	False positives	0

Yet another new name, and another last-minute arrival on the test bench, *UnThreat* is based on the *VIPRE* engine,



which gave us a few worries as we prepared to try it out for the first time.

The installer was pretty compact at under 8MB, although 60MB or so of updates were needed in addition. The set-up process presented a very large window but didn't have much to fill it with, zipping through in no time at all and requesting a final reboot after only 10 seconds or so. The interface is fairly nice and attractive, in a dappled grey shade with large, clear buttons and icons. The layout is lucid and sensible. The family relationship was clear in some areas, with some sets of controls closely mirroring those in *VIPRE*, but in other areas we actually found more detailed configuration available, which was a pleasant surprise.

Speed measures ran through safely, with an appealing animated graphic to keep the user entertained during the scanning process. The expected slow times were observed over most file types, although executables were well handled. Lag times were pretty hefty too, again with good improvements in the warm runs, and with low RAM use and CPU drain not too high either, the impact on our activities was pretty slight.

Detection tests proved rather more of a challenge though. An initial run over the main sets was left overnight. When it still hadn't finished at the end of the following day, it was left for another night. In the end it took 42 hours to complete, and by the end the scanning process was using 1.2GB of RAM, the test machine just about holding its own and remaining responsive. Unfortunately, the scan seemed to have frozen at the moment of completion and failed to write any logs out to disk. Scans were re-run in a dozen or so smaller chunks, each taking from four to eight hours, and this approach produced much better results, with no repeats of the earlier logging failure. Moving on to the on-access tests, we saw similar problems to those experienced with other OEM versions of the same engine, with any kind of stress causing an immediate collapse. Detection seemed to stay up for a few hundred detections, then either switched itself off silently, or stopped detecting but continued to delay access to any file for a considerable period. The set was broken into smaller and smaller chunks, each one being run separately with the product given plenty of breaks in between to recover from the ordeal of having to look at a few dozen files. Testing continued for several more days, and in the end a complete set of results was obtained, closely matching those of the *VIPRE* product, with the same engine and updates but in massively less time.

This meant solid scores across the board, with a great showing in the RAP sets and no problems in the core certification sets, earning *UnThreat* its first VB100 award at

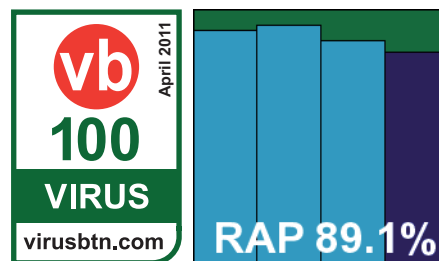
first attempt. A lot of work was involved, with perhaps 15 working machine-days devoted to getting it through the full suite of tests – we have to hope *GFI/Sunbelt* passes on the improvements it has made to its own product to its OEM partners sometime soon.

VirusBuster Professional 7.0.44

Virus scan engine 5.2.0; virus database 13.6.217

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.90%
Worms & bots	96.33%	False positives	0

VirusBuster is another old hand at the VB100, with entries running back over a decade and the vendor's last missed entry way back in



2007. As usual we've seen several entries spawned from this engine this month, with most achieving good results, which bodes well for *VirusBuster* itself. However, those most closely modelled on the original engine have had some nasty issues this month, with scan slowdowns and memory drainage, which left us somewhat apprehensive.

The 69MB installer tripped through rapidly, with nothing too taxing to think about and no reboot needed before applying the 62MB offline update bundle. The interface is very familiar, having barely changed in many years, but somehow still seems to bewilder and baffle with its awkward and non-standard layout and approach to controls, which are actually provided in decent depth once they are dug out.

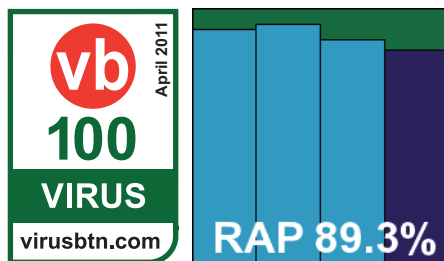
Running through the speed sets proved simple, with scanning speeds and lag times around average and resource use and impact on everyday tasks fairly low. Getting through the larger infected sample sets proved harrowing as feared though, with several crashes and several scans taking huge amounts of time to complete. After leaving it over several nights – taking it off during the days to get on with more urgent tasks – results were finally put together, showing the expected decent scores across the sets, with a slight decline in the latter half of the RAP sets. The core sets were well handled, and *VirusBuster* earns another VB100 award. The long view shows passes in all of the last six tests, three fails and nine passes in the last two years.

Webroot Internet Security Complete 7.0.6.38

Security definitions version 1892; virus engine version 3.16.1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.05%
Worms & bots	98.47%	False positives	0

Entering into its fifth year of VB100 entries, *Webroot* has a good record of passes thanks to the *Sophos* engine that provides the bulk of



the malware detection. However, the product has yet to earn much popularity with the test lab team thanks to its control-free interfaces and long run times getting through tests. As usual, we hoped for an improvement but, after an exhausting few weeks, feared more of the same.

The installer provided measured close to 300MB, but was a custom build for testing including a wide range of extras and several versions of the virus data. Some special steps were involved in the set-up too, but the main process ran through the basic simple steps, completing fairly rapidly and needing a reboot at the end.

Performance tests proved somewhat difficult as a number of our scripts and tools seemed to be being prevented from running. No warnings were displayed by the product however, and no log entries could be found referencing the actions carried out. Delving into the controls, we eventually found some settings to whitelist applications, and added everything used by our tests, but still they were not allowed to function properly. In the end, we had to completely disable the firewall portion of the product to get a simple job like fetching files with `wget` to work.

With this done, we saw some decent scanning speeds, especially in warm runs where unchanged files are ignored. Lag times were very low too, and resource use and impact on tasks were also kept to a minimum.

This did little good in our larger jobs, but some special controls disabling the default quarantining action promised to speed things through, and with these enabled we set off the main detection task with high hopes. Close to 60 hours later, it all seemed finished, and we moved on to the on-access tests. These were performed on-write as on-read protection appeared not to be present. Again, it

took several days to complete the process of copying the main sample sets from one place to another. Logs were at least comprehensive and complete though, and results were finally harvested, showing the expected solid scores, declining slightly in the newer parts of the RAP sets. A fine showing in the core sets earns *Webroot* a VB100 award, the vendor's fourth from four entries in the last two years, and perhaps its most exhausting (for us) so far.

CONCLUSIONS

Another giant test, with another record-breaking roster of products entered, and once again we considerably overshot our target completion date. However, the main cause of this was not the large number of products. Nor was it the perhaps rather ambitious plan to introduce some new, untried and rather time-consuming performance measures into the busiest test of the year – nor the absence of half the lab team through illness for the bulk of the testing period. The main issue was with a handful of unruly, unstable, slow and unreliable products – perhaps a dozen or so taking up the whole lab for a full two weeks. The other 55 or so were completed in less than three weeks and, had all products behaved as well as we hoped – or, indeed, as well as the majority did – we could easily have squeezed in another 30 or so in the time we had available.

The bulk of wasted time was the result of inadequate or unreliable logging facilities, and lack of user controls. Products which insist on quarantining, disinfecting and so on by default are fairly commonplace – it's a fairly sensible approach given the lack of interest most users display in their own security. However, even if most users are not interested in controls, and would be unlikely to set their products to log only, or deny access only, when submitting products for a large-scale comparative it seems fairly obvious that this would be a useful thing to have available. Presumably many of the companies producing security solutions these days, putting products together based on engines developed elsewhere, do not have access to malware samples to use for QA, but that is a pretty poor excuse for not getting the QA done. Stability of a piece of security software should not be undermined by having to work a little harder than usual, and passing that instability on to the entire machine is likely to be pretty unforgivable to most users.

Logging is another area of difficulty, and another one where testers perhaps have somewhat special needs. However, this is something else which is made very clear when submissions are called for testing, and one which is clearly going to be important in a large-scale test. Inaccurate or incomplete logs of what has been observed and carried out on a machine would be utterly

unacceptable in a business environment, and most consumers would be unhappy to find that their security solution had fiddled with their system but couldn't tell them anything about what it had done or why. The growing popularity of logging to memory, and only outputting to file at the end of a scan, seems targeted specifically at irritating testers. The benefits are presumably in faster scanning times and less use of disk, but presumably most normal users would see little of this benefit, as there would rarely be much written to logs anyway. The only people with large amounts of data to log are those who have too much data to be comfortably stored in memory without causing horrible side effects: the slowdowns and collapses and fails we have seen so many of this month.

Having dealt with the dark side, there are also good things to report this month. We saw a good ratio of passes this month, with only a few products not qualifying for certification, partly of course thanks to our extreme efforts in the face of difficulties, but mainly due to good detection rates and low rates of false alarms. Those not making it were generally denied by a whisker, with only a few showing fair numbers of false positives or significant samples not covered. In a couple of unlucky cases, selection of default settings led to items being missed which could otherwise easily have been detected. In general though, performances were good. As well as the simpler measure of certification passes, we saw some excellent scores in our RAP sets, with a general move towards the upper right corner of the quadrant. We saw several new names on this month's list, a few of whom had some problems, but several put in strong showings and there are a number of proud new members of the VB100 award winners' club.

We also saw some interesting results in our performance measures, which we'll continue to refine going forward, hopefully making them more accurate and reliable as we fine-tune the methodology over the next few tests. We also hope, now that the lab has a little breathing space, to get back to work on plans to expand coverage of a wide range of protective layers and technology types. The overheating, overworked lab hardware may need a little downtime first though – as might the similarly hot and tired lab team – to recover from what has been quite an ordeal.

Technical details

All products were tested on identical machines with *AMD Phenom II X2 550* processors, 4GB RAM, dual 80GB and 1TB hard drives running *Windows XP Professional SP3*.

For the full testing methodology see <http://www.virusbtn.com/vb100/about/methodology.xml>.



VB2011 BARCELONA 5-7 OCTOBER 2011

Join the VB team in Barcelona, Spain for the anti-malware event of the year.

- What:**
- Three full days of presentations by world-leading experts
 - Rogue AV
 - Botnets
 - Social network threats
 - Mobile malware
 - Mac threats
 - Spam filtering
 - Cybercrime
 - Last-minute technical presentations
 - Networking opportunities
 - Full programme at www.virusbtn.com

Where: The Hesperia Tower, Barcelona, Spain

When: 5-7 October 2011

Price: VB subscriber rate \$1795 – **register before 15 June** for a 10% discount

**BOOK ONLINE AT
WWW.VIRUSBTN.COM**

END NOTES & NEWS

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

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

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

The Counter eCrime Operations Summit 2011 takes place 26–28 April 2011 in Kuala Lumpur, Malaysia. This year's meeting will focus on the development of response paradigms and resources for counter-ecrime managers and forensic professionals. For details see http://www.apwg.org/events/2011_opSummit.html.

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

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

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

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

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

CONFidence 2011 takes place 24–25 May 2011 in Krakow, Poland. Details can be found at <http://confidence.org.pl>.

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

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

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

Black Hat USA takes place 30 July to 4 August 2011 in Las Vegas, NV, USA. DEFCON 19 follows the Black Hat event, taking place 4–7 August, also in Las Vegas. For more information see <http://www.blackhat.com/> and <http://www.defcon.org/>.

The 20th USENIX Security Symposium will be held 10–12 August 2011 in San Francisco, CA, USA. See <http://usenix.org/>.

VB2011 takes place 5–7 October 2011 in Barcelona, Spain. The conference programme will be announced shortly at <http://www.virusbtn.com/conference/vb2011/>.

RSA Europe 2011 will be held 11–13 October 2011 in London, UK. For details see <http://www.rsaconference.com/2011/europe/index.htm>.

ADVISORY BOARD

Pavel Baudis, *Alwil Software, Czech Republic*
Dr Sarah Gordon, *Independent research scientist, USA*
Dr John Graham-Cumming, *Causata, UK*
Shimon Gruper, *NovaSpark, Israel*
Dmitry Gryaznov, *McAfee, USA*
Joe Hartmann, *Microsoft, USA*
Dr Jan Hruska, *Sophos, UK*
Jeannette Jarvis, *Microsoft, USA*
Jakub Kaminski, *Microsoft, Australia*
Eugene Kaspersky, *Kaspersky Lab, Russia*
Jimmy Kuo, *Microsoft, USA*
Costin Raiu, *Kaspersky Lab, Russia*
Péter Ször, *McAfee, USA*
Roger Thompson, *AVG, USA*
Joseph Wells, *Independent research scientist, USA*

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

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

Corporate rates include a licence for intranet publication.

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

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: <http://www.virusbtn.com/>

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2011 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2010/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.