

virus

BULLETIN

Fighting malware and spam

CONTENTS

2 COMMENT

Are takedowns an exercise in futility?

3 NEWS

VB2010 programme announced

All star superstars

Dangerous places to be online

3 VIRUS PREVALENCE TABLE

FEATURES

4 Evasions in Intrusion Prevention/ Detection Systems

11 Botnets, politics and hacktivism – an interesting partnership

15 'Signatures are dead.' 'Really? And what about pattern matching?'

21 TUTORIAL

Exploit kit explosion – part one

23 COMPARATIVE REVIEW

VB100 – Windows XP SP3

68 END NOTES & NEWS

IN THIS ISSUE

A FUTILE BATTLE?

Mary Landesman evaluates recent botnet takedown efforts.

page 2

CYBER WARFARE

Terry Zink looks at the increasingly common phenomenon of hacktivism and details three recent cyber warfare attacks.

page 11

EXPLOIT KIT EXPLOSION

In the first of a two-part series introducing exploit kits Mark Davis outlines the basic details of the dime-a-dozen kits used in drive-by browser-based attacks.

page 21

RECORD VB100 ON XP

In VB's largest ever VB100 comparative review, a total of 60 products are put to the test on Windows XP. John Hawes has all the details.

page 23





'There is often little incentive for domain registrars or hosting providers to make it more difficult for criminals to obtain services.'

Mary Landesman, ScanSafe

ARE TAKEDOWNS AN EXERCISE IN FUTILITY?

The first quarter of 2010 witnessed multiple takedown efforts aimed at the Lethic, Waledac, Mariposa and Zeus botnets. Lethic, which specialized in spam for counterfeit goods, pharmaceuticals and degree-less diplomas, was shut down by *Neustar* in January. In February, *Microsoft* obtained a court order allowing *Verisign* and other registrars to withdraw the domains used by the Waledac botnet.

But these takedowns appear to have had little or no effect on spam levels, with statistics from *Arbor Networks*, *Trend Micro*, *Commtouch* and *MessageLabs* all indicating either steady or increasing spam levels month over month in the first quarter. For example, *MessageLabs* reported spam levels of 89.4% in February – a 5.5% increase on January totals – and 90.7% in March, a 1.4% increase on February totals.

The effects of the Mariposa and Zeus takedowns were equally disappointing. Within days of announcing the arrest of Mariposa's bot herders, *Panda Labs* (which assisted in the botnet's takedown) reported on new Mariposa activity from a different set of attackers.

Likewise, efforts aimed at de-peering the *Troyak-AS* ISP, which provides service to a segment of the Zeus command and control (C&C) servers, proved to be a virtual game of whack-a-mole. Less than 24 hours after being de-peered by its latest upstream provider,

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

Consulting Editors:

Nick Fitzgerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, USA*

Troyak-AS resumed service under a new upstream provider, and this pattern was repeated numerous times.

These less than dramatic results beg the (multi)-million-dollar question: are such takedown efforts an exercise in futility?

Certainly if one focuses only on short-term statistics, the answer would appear to be 'yes'. However, if one focuses on some of the precedents set during the first quarter, tangible long-term impact may become a reality.

In the case of Lethic, Waledac and Zeus the takedown efforts engaged the service providers, hosts and domain registrars. This not only sets an important legal precedent facilitating future takedown efforts, but also shifts the responsibility – and some of the costs – onto those who (unknowingly or otherwise) enable criminal activity.

Consider the situation with *Troyak-AS* and the Zeus C&C serviced by that provider. An analysis of *ScanSafe* traffic involving the domains and IP addresses listed in *ZeusTracker* reveals that the traffic serviced by *Troyak-AS* in the first quarter of 2010 made up 48.5% of all Zeus traffic. Thus, a successful shutdown of that segment could lead to significant disruption and financial losses for Zeus bot herders.

Perhaps most importantly, though, *Troyak-AS* also suffers a financial loss. It is presumed that costs were incurred each time *Troyak-AS* moved to a new upstream provider. Assuming the ISP serviced legitimate businesses as well as Zeus, it is also quite possible that it suffered a loss of customers due to its inability to maintain service. The combination of increased costs and customer loss could cause such a service provider to re-evaluate their business model.

Currently, there can be a considerable financial incentive for so-called bulletproof hosts to turn a blind eye to malicious activity occurring through their services. And there is often little incentive for domain registrars or hosting providers to make it more difficult for criminals to obtain services. But if efforts continue to engage these providers – and where necessary hold them accountable – at some point the cost of turning a blind eye may become unpalatable.

The punches delivered in the first quarter may not have resulted in a technical knockout, but at the very least we've winded the bot herders and set a precedent for the enablers. Long-term success depends on continued concerted takedown efforts that engage the providers and cause the enabling of criminal activities to become a cost centre rather than a profit centre. We should support – and not criticize – these types of takedown efforts because we are all reaching for the same goal: better security for all.

NEWS

VB2010 PROGRAMME ANNOUNCED

Following a bumper crop of submissions, the VB2010 conference committee is pleased to announce the programme for VB2010 in Vancouver.



Presentations cover subjects including: botnets, cyber terrorism, blackhat SEO, targeted attacks, Mac threats, anti-spam testing, anti-malware testing, in-the-cloud scanning and more. Later in the year a selection of 'last-minute' technical papers will be added to the programme to allow for up-to-the-minute material.

VB2010 takes place 29 September to 1 October 2010 in Vancouver, Canada. Delegates who register before 15 June will benefit from early bird discounts on the subscriber and non-subscriber rates. The programme can be viewed at <http://www.virusbtn.com/conference/vb2010/programme/>.

ALL STAR SUPERSTARS

Channelweb has revealed three lists of 'security superstars' in 2010: 'Security Superstars: Visionaries' (pioneers in security), 'Security Superstars: Researchers' (the best and brightest researchers in the industry) and 'Security Superstars' (simply 'superstars in the security space'). Those honoured include Mikko Hypponen, Graham Cluley, Eugene Kaspersky, Roger Thompson, David Perry, Paul Judge and the CEOs of *McAfee*, *Symantec* and *Trend Micro*. The full lists are at <http://www.crn.com/security/>.

DANGEROUS PLACES TO BE ONLINE

Symantec's PR team excelled in the art of producing pointless pieces of information last month when it revealed the top ten 'riskiest online cities' in the US and Canada. Topping the list as the US city most vulnerable to cybercrime was Seattle, followed by Boston, Washington, DC, San Francisco and Raleigh. In Canada the top five danger zones were Burlington, Port Coquitlam, Langley, Vancouver and Calgary. The lists were compiled using data on cyber attacks and potential malware infections, as well as information about users' online behaviour – such as accessing wifi hotspots and online shopping. The research was conducted in association with *Sperling's BestPlaces*, a site which provides regional information on cost of living, employment rates, crime rates, schools, climate and so on. Those troubled by finding out they live in a cybercrime hotspot could consider relocating to Detroit in the US or Longueuil in Canada – ranked the least dangerous cities in each country.

Prevalence Table – February 2010^[1]

Malware	Type	%
Autorun	Worm	11.81%
Adware-misc	Adware	10.35%
Conficker/Downadup	Worm	6.44%
VB	Worm	5.78%
OnlineGames	Trojan	5.47%
FakeAlert/Renos	Rogue AV	4.37%
Delf	Trojan	3.95%
Virtumonde/Vundo	Trojan	3.79%
Agent	Trojan	3.69%
HackTool	PU	3.03%
Istbar/Swizzor/C2lop	Trojan	2.83%
Injector	Trojan	2.60%
Encrypted/Obfuscated	Misc	2.57%
Virut	Virus	2.42%
Hupigon	Trojan	2.36%
Heuristic/generic	Misc	2.16%
Alureon	Trojan	2.02%
Small	Trojan	1.92%
Downloader-misc	Trojan	1.68%
Zbot	Trojan	1.52%
Bifrose/Pakes	Trojan	1.27%
PCClient	Trojan	1.25%
Iframe	Exploit	1.11%
Exploit-misc	Exploit	1.09%
Crack	PU	1.01%
Sality	Virus	0.97%
Heuristic/generic	Virus/worm	0.82%
Peerfrag/Palevo	Worm	0.78%
Zlob/Tibs	Trojan	0.67%
Looked/Viking	Virus	0.63%
RemoteAdmin	PU	0.52%
Autolt	Trojan	0.47%
Others ^[2]		8.64%
Total		100.00%

^[1]This month's prevalence figures are compiled from desktop-level detections.

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

FEATURE 1

EVASIONS IN INTRUSION PREVENTION/DETECTION SYSTEMS

*Abhishek Singh, Scott Lambert, Tanmay A. Ganacharya, Jeff Williams
Microsoft, USA*

Use of an Intrusion Prevention System (IPS) and/or Intrusion Detection System (IDS) can be very effective in preventing and/or detecting the exploitation of certain classes of vulnerability over the network. This is most commonly achieved by matching patterns against the raw bytes sent over the network. This approach can be improved upon by breaking the raw bytes into constituent parts (protocol fields) before applying appropriate checks on the parsed data. The goal is to maximize both the confidence of the detection (match) and the resilience of the IDS/IPS systems to evasion.

There are many different types of protocol decoder in IDS/IPS systems. Some devices have protocol decoders which parse both the client and server messages, and have the capability of forwarding the traffic from one protocol to another. Some protocol decoders are limited to parsing the server messages, while others do not provide any forwarding of traffic to other layers. However, regardless of the type of protocol decoding used, detection can be evaded.

The structure and usage of each protocol is different. A protocol can accept an external input in various forms, and this can be a weakness. For example, in the case of HTTP, the web server www.microsoft.com can also be referred to as www.%6D%69%63%72%6F%73%6F%66%74%2E%63%6F%6D. While a strong signature can be developed to block attempts to exploit a given vulnerability, if the IPS/IDS itself does not take steps to prevent evasion, the signature will easily be bypassed.

In this article we look at some of the more common methods of evading IDS/IPS detection. Each section provides an overview of the problem, one or more concrete examples, and their respective solutions. A good IDS/IPS device should be able to address most, if not all, of the issues discussed in this article.

DOES THE IDS/IPS PROVIDE SUPPORT FOR BIDIRECTIONAL PROTOCOL DECODERS?

There are two types of protocol decoder: single directional and bidirectional. In general, a single-directional protocol decoder denotes that a command has ended by using the delimiter of the command, whereas a bidirectional protocol

decoder uses both the delimiter of the command and the response code. If both directions of a session are not parsed (the state is not kept), it is possible that the system will apply signature logic incorrectly. This introduces the possibility of false positive detections.

Let's take the SMTP protocol as an example. SMTP stands for Simple Mail Transfer Protocol and is defined in RFC 5321 [1]. The normal flow of commands in SMTP is shown in Figure 1. The DATA is sent after the RCPT TO request.

```
HELO
250 welcome here
MAIL FROM: admin@blah.com
250 OK
RCPT TO:admin@winxpgold.com
250 OK
DATA
354 send the mail data, end with .
-
```

Figure 1: Normal flow of commands in SMTP.

A single-directional protocol decoder will assume that the bytes that follow the DATA command are data and will allow them to pass through without checking for exploits. Figure 2 shows a situation in which the DATA command is issued *before* the RCPT TO request; the SMTP server will still be in a command state and will accept the command. The single-directional protocol decoder will be expecting the bytes that follow the DATA command to be data and will allow them to pass through. A bidirectional decoder, on the other hand, requires both the DATA command and the response code 354 to go to DATA state.

```
HELO
250 welcome here
MAIL FROm:blah@mail.com
250 OK
DATA
554 no mail receiver
RCPT TO:admin@winxpgold.com
250 OK
XEXCH50 333333333333 2
501 command argument is not acceptable
-
```

Figure 2: The DATA command is issued before RCPT TO.

To reduce the possibility of false positives, it is recommended that an IDS/IPS system implement bidirectional protocol parsers.

IS THE IDS/IPS ABLE TO DECODE ENCRYPTED DATA?

Several protocols support the notion of using encryption to enable some form of privacy in support of security. The general problem with encryption is that it makes it difficult, if not impossible, for a man-in-the-middle (MiTM) implementation of IDS/IPS to interpret the raw

bytes correctly. For example, upon starting a session, an RPC request is made for secure services whereby a secure context is established. This secure context might include a shared session key, sequence number, verification state, and so on. The secure context is used to form a secure connection between the client and the server. The client can send an encrypted RPC message to the server using the generated session key, with an optional authentication header. Upon receiving the message, the server decrypts it with the session key before processing the RPC. So exploit variants or encrypted exploits can be generated for many RPC vulnerabilities – such as MS08-067 (CVE-2008-4250), which was a propagation vector of the infamous Conficker worm. If the detection device cannot decrypt the traffic then the encrypted exploits can bypass detection.

As well as RPC, encrypted traffic can appear on port 80 for HTTPS connections, port 465 for SMTP, port 995 for POP3 [2] and port 993 for IMAP [3].

A detection device must be able to decrypt encrypted traffic and inspect it. In some IDS/IPS implementations, scanning encrypted traffic for exploits is possible by providing the IPS with decryption keys. The IPS first decrypts the traffic and then forwards the data to its signatures.

DOES THE IDS/IPS PROVIDE SUPPORT FOR ENCODED DATA?

In many cases, protocols allow data to be encoded in various formats (encodings). These encodings are often published standards which can be used to transmit data. An IDS/IPS system acting as a MiTM should provide support for these various formats. If the IDS/IPS cannot return the encoded data to some ‘common/normal’ form, both the number and effectiveness of signatures will be impacted. Let’s consider a few encodings in HTTP, MIME and RPC.

Encodings in HTTP

The HTTP protocol is defined in RFC 2616 [4]. The URL field in HTTP can be used to exploit various vulnerabilities, hence many signatures are written to check the value of these fields. Signatures generally monitor the URL field in HTTP traffic.

The URL field can be encoded in many ways. The following are some of the encodings which are supported by various application web servers and can also be used by an attacker for encoding exploits:

- Hex encoding: this is an RFC-compliant encoding in which an ASCII value is replaced by its hexadecimal value. For example, 'A' is represented as '%41'.

- Double percentage encoding: this is based on normal hex encoding, the only difference being that the '%' value is replaced by its hex value, i.e. '%25'. In this type of encoding, 'A' is represented as '%2541'.
 - Double nibble hex encoding: this is based on the standard hex encoding method, in which each nibble is hex encoded. For example, 'A' can be encoded as '%%34%31'. '%34' resolves to 4 and '%31' resolves to 1; thus, the encoding resolves to 'A'.
 - Second nibble encoding: this differs from the first nibble encoding in that the second nibble value is encoded with a normal encoding. For example, 'A' is encoded as '%4%31'. '%31' resolves to 1 and '%41' resolves to 'A'.
 - *Microsoft %U encoding*: the format for this encoding is '%UXXXX', as shown in Figure 3. In this type of encoding, '%U' is followed by four hexadecimal digits. For example, 'A' can be represented as '%U0041'.

Figure 3: %U encoding in the GET request of HTTP.

- Mismatch encoding: here, various types of encoding like hex, double nibble, second nibble and *Microsoft %U* encoding are combined to encode a single character. For example, in hex ‘U’ is encoded as ‘%55’. So, using mismatch encoding, ‘%U0041’ will be encoded as ‘%550041’.
 - UTF-8 bare byte encoding: this is similar to UTF-8 encoding, the only difference being that UTF-8 byte sequences are not escaped with a percentage. Byte sequences are sent with the actual bytes.
 - Parameter evasion using POST and content encoding: if base64 is specified in the content encoding, parameter fields in the post request will be base64-encoded. Hence, the detection device will first have to decode the base64 and then check the stream for malicious content. Decoding of base64 can add extra overhead to the detection system.

Encodings in MIME

As per RFC 2047 [5], there can be two types of MIME encoding: ‘B’ encoding, which is similar to base64 encoding, and ‘Q’ encoding, which is similar

to quoted-printable content-transfer encoding. When a MIME message contains unknown RFC 2047 encoding, the detection device can either block the connection, assuming the encoding to be malformed, or it will decode the messages. RFC 2047 encodings provide a vector for evasion in the sense that the client can successfully decode messages in cases where the intrusion detection system is not able to decode them.

RFC 2045 [6] provides the content-transfer-encoding field, which allows the specification of an encoding type to enable eight-bit data to travel successfully through seven-bit transport mechanisms. Content-transfer encoding supports seven-bit, eight-bit, binary, quoted-printable and base64 encodings. The content-transfer-encoding field can be used to support other encodings as well, such as uuencode, mac-binhex40 and yenc. By encoding an exploit using an encoder that is supported by the email clients but not by the IPS, detection can be bypassed.

Encodings in RPC

The RPC protocol [7] is used to perform client-server communication. The protocol makes use of the external data representation protocol which standardizes the representation of external data in remote communications. In RPC protocol, the client tries to access a remote computer, and the server is a machine that implements network remote procedures. The client makes a remote procedure call to the server and receives a reply which contains the result of the call. RPC supports various transports: TCP, HTTP, UDP and SMB. The RPC messages require unique specification of a procedure to call, matching of response messages to request messages, and authentication of caller to service and service to caller. The data in RPC protocol can be represented in big-endian, little-endian, Unicode, EBCDIC or ASCII strings. The exploit-specific signatures in RPC are prone to evasion.

Some of the evasions that are a result of various encodings are discussed in the following sections.

Endianness selection: in the header of every DCE RPC request there exists a data representation field in which the byte ordering, character set and floating-point representation are specified. Little-endian is used as default. However,

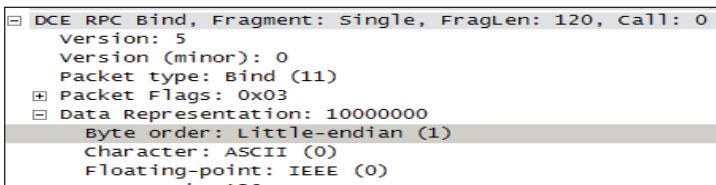


Figure 4: Endianness in the DCE header.

even if the flag is changed to big-endian, the RPC request can be treated as a valid request. Based upon the value of the flag, an intrusion prevention system should be able to parse the packet. The detection device can be bypassed if it is not able to differentiate between the big-endian and little-endian packets.

Unicode and non-Unicode evasion: the SMB header provides a two-byte Flag2 field which is used to determine whether the strings will be in Unicode or non-Unicode characters in the SMB header. Non-Unicode characters are used when the value of Flag2 is not set. Hence, all SMB commands, RPC functions and data will be in non-Unicode format. Based upon the Unicode or non-Unicode characters in the header, signatures should be able to check the incoming stream for exploits.

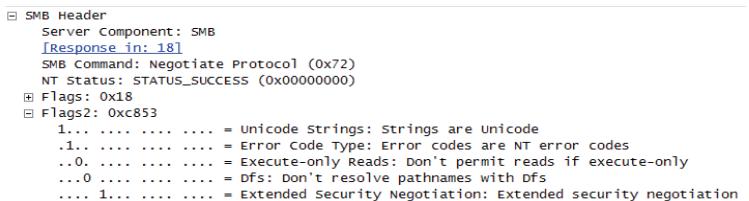


Figure 5: Flag2 with Unicode strings.

Where encoded data is concerned, the challenge is in making sure that the IDS/IPS system is capable of returning the encoded data to some normal form before signatures are applied. This allows the number of signatures required to address a given vulnerability to be kept to a minimum – for example, in the case of HTTP there will be at least eight signatures if the IPS does not provide support to decode data.

DOES THE IDS/IPS SUPPORT FORWARDING OF DATA FROM ONE PROTOCOL DECODER TO ANOTHER?

Several application-level protocols leverage the TCP/IP stack to ride on top of one another; failure of the IDS/IPS system to decompose raw bytes that use one or more protocols during an exchange generally results in missing attack vectors and, in the worst case, false negatives.

For example, the MS-RPCH (Remote Procedure Call over HTTP [8]) protocol tunnels RPC network traffic from an RPC client to an RPC server through a network agent referred to as an RPC over HTTP proxy. The protocol is applicable to network topologies where the use of HTTP- or HTTPS-based transport is necessary – for example, to traverse an application firewall where the application or computer systems communicating over the topology requires the use of the RPC protocol. This is used as an

attack vector/evasive measure for DCOM [9] exploits such as MS03-026 and MS03-039 which arrive on ports 135, 139 and 445.

The protocol decoder should be able to forward the MS-RPCH traffic data from HTTP to the DCOM protocol decoder. Similarly, the SMTP headers and the HTTP traffic should be forwarded to the MIME protocol decoder.

DOES THE IDS/IPS PROVIDE ANTI-EVASION MEASURES FOR APPLICATION-SPECIFIC EVASIONS?

In different applications a given protocol may be implemented in slightly different ways. As a result, protocol decoders for an IDS/IPS system need to relax the RFC compliance enforcement (i.e. implement it loosely) to account for the different implementations. Evasive methods appearing in protocols might not appear in all applications. The detection device should have application-specific anti-evasion measures.

Application-specific evasions in HTTP

HTTP formatting

The syntax for an HTTP request is as follows:

```
Method <space> URI <space> HTTP/Version <CRLF>
```

Some web servers accept a tab between the method and the URI, making requests such as those shown in Figure 6 valid.

GET	/exploit.cgi HTTP/1.0
POST	/exploit.cgi HTTP/1.0
HELLO	/exploit.cgi HTTP/1.0

Figure 6: A tab is accepted as a separator between the method and URI.

If the protocol decoders of an intrusion prevention system only check for a space between the method and URI, detection can be evaded simply by sending a tab between the method and URI. Besides space and tab, some web servers also accept 0x09, 0x0b, 0x0c and 0x0d as valid separators between the method and URI.

Some web servers also accept %00 as a valid separator between the method and URI. It should be noted that NULL characters are used to denote the end of the string: the intrusion detection and prevention system stops once %00 is reached and allows the URI to pass through. Hence protocol decoders which parse the method and URI should accept %00 as a separator between the method and URI.

The syntax of HTTP v0.9 as per RFC 1945 [10] is:

```
GET <space> URI <CRLF .>
```

Only three parameters are sent in HTTP v0.9, and no headers are returned. If the HTTP v0.9 requests are not parsed correctly, then the HTTP signatures can be evaded simply by sending an exploit using HTTP v0.9 syntax.

Forward slash/backward slash

Many web servers are flexible in accepting requests. For example, the request http://www.domain.com/index.html is similar to the request http://www.domain.com/index.htm. So if the detection device only checks for forward slash patterns it can be evaded by sending a backward slash pattern.

Method matching

Based on the implementation of CGI, it is often possible to use HEAD in place of POST. In some implementations, the method is ignored. Hence in many systems, an attacker can use the GET or the POST methods interchangeably in an exploit. If the detection device checks for a GET request followed by checking the URI for exploits, it can be evaded by using POST and the exploit URI pattern.

Case sensitivity

In many implementations of web servers, GET /exploit HTTP/1.0 is similar to GET /EXPLOIT HTTP/1.0. The signatures checking the URI for exploits must be case-insensitive.

Application-specific evasions in MIME

RFC 822, section 3.1.2, specifies that header fields are lines which are composed of a field name, followed by (':'), followed by a field body, and are terminated by CRLF. A separator is used to differentiate between the field names and the field body. Non-standard separators that are accepted by applications include a double colon, or the colon may be omitted altogether. If the MIME protocol decoders are not able to accept non-standard separators, they will not be able to separate the field name from the field body; signatures in turn will not be able to sanitize these fields and detection can be evaded.

RFC 2822 [11] states: ‘Strings of characters that include characters other than those allowed in atoms may be represented in a quoted string format, where the characters are surrounded by quote (DQUOTE, ASCII value 34) characters.’ Non-standard quoting includes quoting fields that should not be quoted, duplicating quotes, and the omission of leading or trailing quote characters from a string. Often, these non-standard quotations are accepted

by applications but are not accepted by detection devices. Hence, if an exploit uses non-standard quotings, these may be accepted by the application, and the detection device will fail to properly parse and sanitize the traffic, allowing the exploit to go undetected.

Quoting RFC 822 [12], ‘A comment is a set of ASCII characters which is enclosed in matching parentheses and which is not within a quoted string. The comment construct permits message originators to add text which will be useful for human readers, but which will be ignored by the formal semantics. Comments should be retained while the message is subject to interpretation according to this standard. However, comments must NOT be included in other cases, such as during protocol exchanges with email servers.’ When an unexpected RFC 822 comment is present, the MIME message is either regarded as malformed and blocked, or the protocol decoder fails to interpret it correctly, which can lead to failure to detect an exploit.

DOES THE IDS/IPS PROVIDE SUPPORT FOR THE REASSEMBLY OF SEGMENTED AND FRAGMENTED DATA?

It is possible for an attack to be spread over multiple packets. Protocols like MSTDS [13], Sun RPC, RPC and HTTP support fragmentation of packets while streaming. Since a server provides the capability of reassembling the disassembled packets, exploits can take advantage of this and spread across packets.

Taking the case of MSTDS, the protocol has the following structure:

Offset	Size	Description
0x0000	1	Type (0x01 for query)
0x0001	1	Status
0x0002	2	Length = X (big-endian)
0x0004	2	SPID (big-endian)
0x0006	1	Packet ID (big-endian)
0x0007	1	Window (unused, must be 0)
0x0008	X-8	Packet Data (Unicode)

To monitor for vulnerabilities, generally the Data field containing the name of stored procedures must be inspected. The Length field is a two-byte (16 bits) field in the header. If the TDS packet to be transmitted over the network is longer than the maximum 16-bit integer, then it must be split into smaller packet fragments. Each packet fragment, with the exception of the last, will contain the value 0x00

in the last packet indicator field to indicate that there are additional packet fragments to follow. On the receiving side, the full TDS packet payload is reassembled from these fragments.

In the case of HTTP, session splicing can be used to send an exploit across the packets. For example, one packet will contain ‘GET’, another will contain ‘/cgi’, another will contain ‘-bin’, and the last one will contain ‘HTTP/1.0’.

Similarly, fragmentation of RPC requests can occur. A normal piece of RPC data will contain a header and data, however, the entire RPC request can be split into multiple RPC requests. Since this is an application-level fragmentation, the IPS will have to reassemble the fragments of the packets. The IPS should have the capability of skipping the header of fragmented RPC packets and reassembling the RPC header and data. It should also check for malicious content in the packet.

In order for a detection device to prevent the spreading of an exploit across multiple packets, it is essential for it to assemble the packets in a session and then inspect them for exploits.

DOES THE IDS/IPS PROTECT AGAINST RFC COMPLIANCE EVASION?

RFC provides specifications for a protocol. Evasion often occurs when an IDS/IPS fails to correctly decode a protocol into its constituent fields. As a result, it is possible that one of two outcomes occurs: a false positive and/or a false negative, depending on the nature of the decoding and signature logic. RFC-specific evasions fall under this category.

RFC compliance evasions in HTTP

The URI <http://www.microsoft.com/en/aaaaaaaaaaaaaaaaaaaaaa/..us/default.aspx> descends into /en, then further descends into the aaaaaaaaaaaaaaaaaaaa directory, which may or may not exist. Following the next slash is a directory traversal, ../, which basically backs into /en/us. Hence the URL is similar to <http://www.microsoft.com/en/us/default.aspx> and is accepted by the web server as a valid request, pointing to the same web page.

Sometimes IDS/IPS devices only check for the first xx bytes of a request. Thus, by sending a large enough number of ‘a’ characters, the rest of the submitted request will be moved outside of the IDS system scan. So if the malicious pattern is ‘/en/us’ and the IDS/IPS only checks for the first 1k bytes, ‘/en/’ followed by 2k of ‘aaa’, followed by ‘/..us’ will successfully avoid detection by the IDS/IPS.

RFC compliance evasions in Remote Procedure Calls

Multiple binding UUID

In the RPC calling mechanism there is one bind request which can contain one UUID and one context ID. The server uses context ID to identify the UUID. Generally, IPS/IDS signatures check the UUID of vulnerable functions in the incoming stream and then parse the argument for malicious content. However, it is also possible for the server to receive multiple UUIDs and multiple context IDs for every single bind request. This is called multiple UUID bind and is a valid request. IPS rules that check for only one UUID and one context per bind request will allow the traffic to pass through, yet the multiple bind part of the UUID may be associated with a vulnerable function. The server will use the context ID and may make a call to the vulnerable function. To prevent multiple bind evasion, an IPS device should parse the bind request. If there are multiple binds and multiple context IDs, then it should keep track of vulnerable UUIDs and corresponding context IDs. If there is a vulnerable function call using that context ID, the IPS rules should monitor the functions for malicious content.

SMB CreateAndX path names

The path name ****SMBSOME\SERVICE\C\$ is treated in the same way as *\\$SMBSOME\SERVICE\C\$. So, if a DCERPC signature is trying to block the path name, it can be evaded by adding ***. In order to prevent evasion, the IPS device must be able to check for the presence of extra ‘\’s in the path name.

Bind to one UUID then alter context

A normal RPC call with a bind request contains a UUID with a context ID. The function opnum is called using that context ID. An opnum is an operation number or numeric identifier that is used to identify a specific RPC method or a method in an interface [14]. To open a new context for a different UUID over the same connection, the alter context DCERPC command [alter_ctx()] can be used. The alter context request leaves the previous context ‘on hold’. Alter context is required since, after binding to a specific interface, binding to another one over the same connection using bind () is not possible. However, the signature, which checks context ID, can be evaded by using alter_ctx().

In the first step of evasion, the normal UUID is associated with a context ID. The IDS or the signatures – which are checking the traffic on the basis of context ID – allow the traffic as normal traffic. Then an alternate context call is

used to link the vulnerable UUID with the original context ID. This is followed by a call to a vulnerable function containing the vulnerable interface (UUID), which is made by using the context ID. Since the detection device tracks the context ID associated with the non-vulnerable UUID, protection can be evaded by using alter context.

Prepend an ObjectID

In a normal RPC call, the arguments or the stub data generally appear after the opnum. However, it is possible for the opnum to be followed by the UUID, which is followed by the stub data. A detection device should be able to parse both scenarios. One of the methods to check such scenarios is to look up the value of the eighth bit in the packet flag. If the value of the eighth bit is set, the detection device should skip 16 bytes and check the start of the stub data.

Bind with authentication field

The Ctx field appears at the end of a normal bind request. The RPC protocol also makes provision for authentication of the client to the server, and the authentication fields (such as auth type, auth level) can appear after the Num Ctx. These fields will not be present in the normal bind request. If a detection device treats the extra bytes as an extension of the context ID it will generate an error. This can be avoided by checking for the value of the auth length in the header. A non-zero value denotes the presence of extra bytes in the header.

One-packet UDP function call

The RPC handshake consists of a 20-byte secret number. This can be avoided by setting the idempotent flag in RPCv4 requests. If the flag is set, the 20-byte secret number can be avoided, also making it feasible to guess the request source. Since the flag allows the sending of the two requests as a single request, and if the IPS rules are dependent upon the handshake process, a signature can be evaded by setting the flag.

Chaining SMB commands

SMB commands ending with ‘ANDX’ can be chained. This leads to the sending, for example, of SMB_COM_TREE_CONNECT_ANDX + SMB_COM_OPEN_ANDX + SMB_COM_READ in a single SMB request. If a detection device checks for one SMB command in an SMB header, then it can be evaded by sending multiple chained commands. To prevent this, the detection device must check the value of the ‘AndXOffset’ field – if the value of this field is zero, then there will not be any more commands.

Out of order chaining

The AndXOffset field stores the next SMB command, and every AndX command has the offset in the packet

to the following command. Hence the physical order does not have to match the logical order and an arranged packet can be built. The first command in the chain will be the first command in the packet. An intrusion detection device must have the ability to parse an SMB header with out-of-sequence command chaining; otherwise it will fail to calculate the number of SMB commands in the header.

Application-specific evasion in SMB

It does not matter to *Windows* SMB implementation if there is more data than needed in a command. The AndXoffset contains the offset of the next command and it is possible to insert random data between the commands. A detection device must be able to parse it correctly.

CONCLUSION

There are a variety of methods that attackers can use to thwart IDS/IPS systems. We have discussed several of these. To recap, web servers support various encodings such as hex, double percentage, double nibble hex, second nibble, *Microsoft %U*, and mismatch encoding. Detection devices should be able to decipher these encodings. To prevent evasion in SMTP, it is recommended that the IDS/IPS implement a bidirectional protocol decoder – that is, the decoder should be able to parse both the client and the server messages correctly. MIME provides an option of various encodings, and the detection device should be able to decode the traffic correctly. MSRPC is an evasion vector for DCOM-related vulnerabilities. A detection device should also be able to reassemble the packets and inspect them; otherwise an attack can be spread over packets. The RPC protocol is also prone to evasion. RPC provides various options of sending commands such as Unicode, non-Unicode, big-endian and little-endian format. A detection device also should be able to decipher these formats.

In this article we have looked at some of the commonly occurring evasion methods. For effective protection it is vital for intrusion prevention and detection systems to have anti-evasion measures.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude and thanks to Jimmy Kuo for his feedback on the article and to Patrick Nolan.

REFERENCES & FURTHER READING

- [1] <http://tools.ietf.org/search/rfc5321>.
- [2] <http://www.ietf.org/rfc/rfc1939.txt>.
- [3] <http://tools.ietf.org/html/rfc3501>.
- [4] <http://www.w3.org/Protocols/HTTP/1.1/rfc2616.pdf>.
- [5] <http://www.faqs.org/rfcs/rfc2047.html>.
- [6] <http://www.faqs.org/rfcs/rfc2045.html>.
- [7] <http://www.ietf.org/rfc/rfc1831.txt>.
- [8] [http://msdn.microsoft.com/en-us/library/cc243950\(PROT.13\).aspx](http://msdn.microsoft.com/en-us/library/cc243950(PROT.13).aspx).
- [9] [http://msdn.microsoft.com/en-us/library/cc201989\(PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc201989(PROT.10).aspx).
- [10] <http://www.ietf.org/rfc/rfc1945.txt>.
- [11] <http://www.faqs.org/rfcs/rfc2822.html>.
- [12] <http://www.faqs.org/rfcs/rfc822.html>.
- [13] [http://msdn.microsoft.com/en-us/library/dd304523\(PROT.13\).aspx](http://msdn.microsoft.com/en-us/library/dd304523(PROT.13).aspx).
- [14] [http://msdn.microsoft.com/en-us/library/cc232137\(PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc232137(PROT.10).aspx).
- [15] A look at whisker's anti-IDS tactics.
<http://www.wiretrip.net/rfp/txt/whiskerids.html>.
- [16] Multiple vendor MIME field multiple occurrence issue.
<http://research.corsaire.com/advisories/c030804-002.txt>.
- [17] Multiple vendor MIME field whitespace issue.
<http://research.corsaire.com/advisories/c030804-003.txt>.
- [18] Multiple vendor MIME field quoting issue.
<http://research.corsaire.com/advisories/c030804-004.txt>.
- [19] Multiple vendor MIME Content-Transfer-Encoding mechanism issue.
<http://research.corsaire.com/advisories/c030804-005.txt>.
- [20] Multiple vendor MIME RFC822 comment issue.
<http://research.corsaire.com/advisories/c030804-009.txt>.
- [21] Vulnerability Analysis and Defense for the Internet, Springer Publications.
- [22] Caswell, B.; Moore, H.D. Thermoptic Camouflage Total IDS Evasions. <http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Caswell.pdf>.
- [23] Legiment Techniques of IPS/IPS evasions.
http://null.co.in/papers/legiment_ajit.pdf.
- [24] HTTP IDS Evasion Revisited.
http://docs.idsresearch.org/http_ids_evasions.pdf.

FEATURE 2

BOTNETS, POLITICS AND HACKTIVISM – AN INTERESTING PARTNERSHIP

Terry Zink
Microsoft, USA

In 2010, the problem of botnets is apparent to everyone in the cyber security industry. Botnets are used to send spam, host fast flux domains, perform black search engine optimization, distribute viruses, and so forth. But the problem of botnets is not limited to the transmission of email.

POLITICAL CONNECTIONS

In today's world, hostilities between different nations may include cyber warfare and electronic espionage. Countries no longer need 'merely' to worry about physical attacks; they need to be concerned with attacks on their economic infrastructure. There are forms of cyber attack that can seriously cripple a country's infrastructure and which are almost as severe as a physical attack – such as a DDoS attack¹ on a country's banks, web servers, or root name servers.

However, while these cyber attacks are political in nature, they are not necessarily political in origin. It wouldn't take a lot for someone who is ideologically driven, and who has the necessary connections, to talk to his friends in the botnet space and coordinate a full-scale cyber attack against a particular target. The result would be largely the same as if a government had done it. For example, Internet search giant *Google* recently suffered a cyber attack originating from China in which sensitive information was either targeted or stolen [1], yet – despite US Secretary of State Hillary Clinton intimating that the Chinese government ought to own up to the attack – it is not known whether it was state-sponsored or driven by a private individual (or group) with very powerful connections.

Was Secretary Clinton right to accuse China of state-sponsored theft of (American) corporations' intellectual property? Or is it possible that there are individuals out there with the skills necessary to pull off such a sophisticated feat?

¹A denial-of-service (DoS) attack or a distributed denial-of-service (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely, see http://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=349367424.

The term 'hacktivism' is an amalgamation of the words 'hack' and 'activism'. It is defined as the non-violent use of illegal or legally ambiguous digital tools for political ends. Hacktivism is becoming increasingly common, and the complexity of these attacks makes it nearly impossible to determine whether they are state sponsored, or whether they have been perpetrated by an individual (or individuals) with access to an army of bots. The cost of technology has been driven down immensely thanks to Moore's Law [2], but unfortunately this also allows those with malicious intent to do a great deal of damage.

ESTONIA – STUDY OF A CYBER WARFARE ATTACK

Estonia is one of the most wired countries in eastern Europe. It relies on the Internet for a substantial portion of everyday life – communications, financial transactions, news, shopping and restaurant reservations to name just a few. Indeed, in 2000, the Estonian government declared Internet access a basic human right. It was this growing dependence on the Internet that left the country particularly vulnerable to a large-scale cyber attack in April 2007.



The attack is thought to have coincided with an event in downtown Tallinn. During the night of 26 April 2007, government workers relocated a Soviet-era monument commemorating World War II – 'the Bronze Soldier' – and also moved some war graves in downtown Tallinn. This sparked protests from some 500 ethnic Russian Estonians. For the Kremlin – and Russians in general – such a move in a former Soviet republic was considered a grave insult.

By 10 p.m. local time on 27 April 2007, digital intruders had begun probing Estonian Internet networks, looking for weak points and marshalling resources for an all-out assault. Most of the attacks that affected the general public were DDoS-type attacks ranging from various low-tech methods like ping floods, to the rental of botnets usually involved in spam distribution. Spamming of the commentaries of bigger news portals and website defacements, including that of the Estonian Reform Party, also occurred. Once they gained control of the sites, hackers posted a fake letter from Estonian Prime Minister Andrus Ansip apologizing for ordering the removal of the monument.

This was a concerted cyber attack on Estonia. Some observers reckoned that the onslaught on the country was of a sophistication not seen before. The case was studied intensively by other countries and military planners.

A couple of days after the attacks began, networks and routers in Estonia were being pressed to their limits. Although not all servers were taken offline, the functionality of the Internet in the country was severely compromised. Security specialists erected firewalls and barriers but as time passed, these barriers started to break down. Eventually, the government started taking down sites and making them available only to users within Estonia. This was seen as a temporary fix – and although it worked for a country as small as Estonia, it would not have worked for a larger nation where the traffic is much more international.

Two weeks later, the cyber war on Estonia intensified. On 9 May – the date Russia celebrates victory over Germany in World War II – the scale of the attacks increased. More than 50 websites and servers may have been disabled at once, with a data stream crippling many other parts of the system. This continued until late in the evening of 10 May – which was perhaps when the rental of the botnets and the contracts with the cyber mercenaries expired. After 10 May, the attacks slowly decreased as Estonian authorities managed to take botnets offline by working with phone companies and ISPs to trace the IP addresses of attacking computers and shut down their connections.

Many of the computers used in the attacks were traced back to machines in Russian government offices. At the time, the Estonian Foreign Minister accused the Kremlin of direct involvement in the attacks. However, Estonia's defence minister later admitted that he had no evidence linking the attacks to Russian authorities. What could not be determined was whether the computers involved were simply 'zombie' machines that had been hijacked by bots and which were not under the control of the Russian government, or whether they were actively being used and controlled by government personnel.

So who was responsible? At the time, Dmitry Peskov, the Kremlin's chief spokesman, told the BBC's Russian Service there was 'no way the [Russian] state [could] be involved in cyber terrorism' [3]. Two years later, in a panel discussion between Russian and American experts on information warfare in the 21st century, Russian State Duma politician Sergei Markov claimed that his assistant was responsible. According to Markov, his aide (who he did not name) had decided that 'something bad had to be done to these fascists' [4]. In other interviews in 2009, Konstantin Goloskokov, a 'commissar' of pro-Russian youth movement Nashi, claimed responsibility for the attacks [5]. Goloskokov had been in his early 20s and working as an

aide to Sergei Markov when he carried out the attacks, and he claims no regrets. While stressing that the Russian state had no involvement, he said he believed that the Internet represented the most effective weapon to avenge what he saw as a grave national insult [6].

Essentially, the Estonian attacks were a cyber riot: someone with some serious connections in the world of botnets decided to teach the government (of another country) a lesson – and nearly brought the country to a standstill in the process.

Estonia was particularly vulnerable to this type of attack, but the lesson is clear for the broader developed world. A concerted effort made by either a government or a person (or group of people) with a grudge or political agenda can wreak serious havoc on a country's economy. It is clear that, if Goloskokov's claims are true, one need not have state sponsorship in order to launch a crippling cyber attack.

GEORGIA – A REPEAT OCCURRENCE

A year later, a war in Central Asia was preceded by a cyber attack on a nation's infrastructure. The incident was the 2008 South Ossetia War, also known as the Russia-Georgia War [7].



The 1991–1992 South Ossetia War between Georgians and Ossetians left most of South Ossetia under de facto control of a Russian-backed, internationally unrecognized government. In 2004, the Georgian government embarked on a movement to retake South Ossetia. Whereas previously Russia had only sought to maintain the status quo, a brief battle in 2004 became a turning point for its policy in the region. Russia now felt that the security of the whole Caucasus region depended on the situation in South Ossetia, and took the side of the self-proclaimed republic. During 2008, both Georgia and Russia accused each other of preparing for war, and in August 2008 Georgia invaded South Ossetia and Russia invaded in response, ultimately forcing Georgia to withdraw.

Against this background of military force, Georgia, like Estonia a year before it, had been the victim of a

large-scale cyber attack. Two and a half weeks prior to the military action, the website of Georgian president Mikheil Saakashvili was the target of a DDoS attack and was knocked offline for more than 24 hours. A command-and-control (C&C) centre had taken aim at the site and flooded it with TCP, ICMP and HTTP requests. Three days before the invasion, the website for the South Ossetian *OSInform News Agency* was hacked and replaced with a feed from *Alania TV*, a Georgian TV station aimed at television audiences in South Ossetia (*Alania TV* later denied any involvement) [8].

In the lead-up to the conflict, there had been much activity on several Russian chat forums. This culminated in a series of coordinated cyber attacks against Georgia's Internet infrastructure. Several government websites were hacked and defaced, and more government sites were flooded in DDoS attacks and knocked offline. In response, the government was forced to relocate the servers to the United States, and the Georgian Ministry of Foreign Affairs resorted to using a *Google Blogspot* account to release information. Perhaps not so coincidentally, the date of the cyber attacks corresponded to the escalation of the military conflict.

Both public and private sector websites were attacked, including the following:

- The Ministry of Education and Science in Georgia
- The Parliament of Georgia
- The President of the Republic of Georgia
- Georgia's largest commercial bank
- The Association Press
- A private television company

Those responsible for the attack were not particularly secretive. In the time leading up to the attacks, several Russian chat forums carried lists of which government websites to target. Tools for carrying out DoS attacks were provided for download along with instructions on how to flood the Georgian websites. Lists of other Georgian sites that were known to be vulnerable to attack were also distributed. In other words, people were openly plotting to make a move against the Georgian government and making the necessary tools publicly available.

While the timing of the cyber attacks immediately prior to the Russian military intervention does seem almost too convenient not to have been coordinated by the government, it makes no sense for the government to plot their cyber war in plain sight. While the timing is suspicious, we must be careful not to mistake coincidence for conspiracy. A group of pro-nationalists with access to botnets can choose to do a lot of damage if they put their botnets together.

TWITTER – HISTORY DOESN'T REPEAT ITSELF, BUT IT RHYMES

One of my top ten spam stories of the year 2009 (see *VB*, January 2010, p.11) was that of *Twitter* suffering a DDoS attack. On 7 August the social networking site was hit hard enough to be taken down for several hours. Other social networking sites including *Facebook*, *LiveJournal*, *YouTube* and *Blogger* were also hit.

The attacks occurred close to the first anniversary of the Russia-Georgia war. A brief investigation revealed that a targeted attack had been launched against pro-Georgian blogger 'Cyxymu' who had accounts on each of the social networking services involved. Cyxymu, who posted extensively on the suffering of Georgian civilians during and after the war in Abkhazia, accused Russian authorities of trying to silence him using cyber attacks.

We still don't know exactly what happened, who was behind the attacks, or the reason for them, but we can speculate and use historical precedent to come up with a reasonable theory.

The attacks against the social networking sites coincided with a very large spam run. The messages in this spam run all contained links to Cyxymu's pages at *Blogger*, *Facebook*, *LiveJournal*, and so on. One theory is that Cyxymu was responsible for the spam run, and when people all across the Internet received the spam in their inboxes, they all started clicking on the links in the messages, driving piles of traffic to the sites. With so many people checking out Cyxymu's pages, *Twitter*, *Facebook*, *et al.* couldn't handle the load and shut down. In other words, the shutdown of the sites was an accident – Cyxymu was too good at proclaiming his message to the world.

Yet this theory is fraught with problems. First, a spam run like this would have to get past spam filtering services. It is not easy to bypass filters with only a handful of links before they get added to URL blocklists. Secondly, few users, if any, actually click on links in spam messages – particularly politically charged messages. There simply wouldn't have been enough traffic generated to take a site down. Several hundred thousand users would have had to access the pages simultaneously, which would have required the sending of several hundred million spam messages. No offence to Cyxymu, but it's unlikely that he single-handedly built the infrastructure necessary to send out enough spam in such a short time frame to bring down *Twitter*. It doesn't mesh well with what we know about the more sophisticated spamming operations that are in effect today.

A more credible theory is that the spam run was used as a cover. Certain pro-Russians were well aware that Cyxymu was preaching his message on the various social networking

websites, and decided that something had to be done to stop him. The attackers had botnets under their control which flooded the sites with DoS attacks and took them offline. The fact that all the sites were taken down at around the same time indicates that this was a coordinated attack – this was not the result of people clicking on links in their spam email. This theory makes a great deal more sense since a targeted flood of ping requests is much easier to achieve using a botnet than relying on users to click on links in spam messages.

Yet if this was the case, what was the purpose of the spam run with links to Cyxymu's pages? The organizers of the attack were attempting to discredit Cyxymu by making it look as if he was responsible for sending out a huge wave of spam advertising his pages. The attackers assumed that, when word got back to *Facebook* or *Twitter* that Cyxymu was spamming the rest of the world to drive traffic to their sites, they would see this as violating their Terms of Service and shut down his account. In other words, it was all a set-up; the attackers were attempting to frame him.

While containing some outlandish elements, the second theory is more credible than the first.

Who was behind the attack? Was it the Russian government? Did they engage in state sponsorship of cyber warfare? While it is possible that Russian authorities were involved, the attack follows a similar pattern to that of the previous two cases:

- The Estonian government was attacked by a pro-Russian independent player who claims to have been acting on his own behalf. This was sparked by what he saw as anti-Russian actions and was an attempt to 'make Estonia pay'.
- The Georgian government was (allegedly) attacked by a pro-Russian group or player, acting on their own behalf. This was sparked by what they saw as anti-Russian actions and was an attempt to 'make Georgia pay'.
- A number of social networking sites including *Twitter*, *Facebook* and *LiveJournal* were attacked by a pro-Russian group or player (one of which might have been the government). The attacks were sparked by what they saw as anti-Russian actions and were an attempt to 'make the blogger pay'.

The Russian government would have no need to get involved in matters like this because there are enough people out there who are sufficiently well connected in the malware space to launch sophisticated botnet attacks without state involvement. No doubt, some states may be pleased to see their opponents suffering from such sophisticated attacks, but they can plausibly deny any

involvement. Malware and botnets have uses other than sending out spam and pushing fake pills.

This is the difficulty when it comes to cyber warfare – state sponsorship is not required in order to launch attacks on other states. The face of warfare has evolved to include cyber riots, and those who are vulnerable are at risk even if the respective governments do not intend to actually attack each other.

CAN WE PUT IT ALL TOGETHER?

In the movies, we sometimes see hackers breaking into government systems or private corporations. These types of actions, while entertaining, used not to be realistic. Individual players acting on their own behalf didn't have the necessary resources to cripple a nation's infrastructure or pilfer a company's covert information.

Yet, as the cost of technology has fallen and botnets have proliferated, it has become much easier to accomplish these tasks. Foreign governments don't need to conduct cyber warfare, private citizens will do the job for them. We already have three examples of this.

And that brings us back to the issue of the attacks on *Google*. Who was responsible? Was it the government of China? Was it someone trying to steal information from *Google* and give it to a competitor? I don't know the answer, but neither of the above would surprise me.

REFERENCES

- [1] <http://www.bloomberg.com/apps/news?pid=20601103&sid=axOgT5A501fQ>.
- [2] http://en.wikipedia.org/w/index.php?title=Moore%27s_law&oldid=349110709.
- [3] <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.
- [4] http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html.
- [5] <http://www.itexaminer.com/pro-kremlin-activist-confesses-to-estonia-cyber-attack.aspx>.
- [6] <http://news.bbc.co.uk/2/hi/technology/8500555.stm>.
- [7] Wikipedia has a good summary of the timeline of the war: http://en.wikipedia.org/w/index.php?title=Timeline_of_the_2008_South_Ossetia_war&oldid=346178264.
- [8] For a full analysis of the Georgia cyber attacks, see CCDCOE's report at <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>.

FEATURE 3

'SIGNATURES ARE DEAD.' 'REALLY? AND WHAT ABOUT PATTERN MATCHING?'

Gyozo Papp
VirusBuster, Hungary

The title of this article echoes the sort of conversation that might take place between a security industry PR rep and a traditional anti-virus programmer. While accepting the increasing importance of behavioural analysis and detection, this article looks at how current detection technologies, from the simplest to the most complex, can be backed up by pattern matching, proving that it is a mature technology that is very much alive.

First, I must make a confession: I am not a virus analyst; I am a regular developer in an anti-virus company. Before that, I was involved in web technologies and I knew very little about malware and malicious content. I have been working in my current position for six years, during which time I have witnessed a technological revolution as the industry moved from signature-based detection to behaviour-based detection and cloud computing. However, I was still uncertain as to what the phrase 'signature-based detection' really meant and why it was said to have been superseded (or was simply 'dead'), while pattern matching continued to evolve in script languages.

THE ORIGINS

The definitions of the term 'anti-virus signature' in web encyclopedias go like this: 'a unique string of bits, or the binary pattern, of a virus' [1], 'a characteristic byte-pattern that is part of a certain virus or family of viruses' [2]. The term 'pattern' was what helped me understand this technology. The word 'signature' describes a possible set of byte variations derived from the common traits of a set of samples. There is quite an obvious analogy between signatures and regular expressions (regex): 'a regular expression is a pattern describing a certain amount of text' [3].

The power of regular expressions lies in metacharacters (nonliteral tokens) which do not match themselves, but which define rules as to how to match other tokens in a piece of text (see Figure 1). In the early days, an indifferent character could be skipped (this was only a single byte), then a couple of them could be skipped at the same time (as repetition operators or quantifiers were introduced),

and later more specific variants were introduced (character classes, alternation).

Features / regex tokens	Regex notation	VirusBuster notation
literal	literal	6c 69 74 65 72 61 6c
skip one	.	?
skip many (unlimited)	.*	<i>not supported</i>
skip many (at most N)	.{,N}	*(N)
forward (exactly N)	.{N}	+(N)
character classes	[0-9a-f]	[30-39 , 61-66]
alternation	(cat dog)	[63 61 74, 64 6F 67]
capturing	(...)	{N ... } (N = 0..F)
backreference	\N or \\$N (N = 1...9)	\$N (N = 0..F)

Figure 1: The basic regex features supported in VirusBuster sequences.

The next fundamental add-on was the concept of memory registers or variable support. So-called 'capturing' can store arbitrary content from a string so that it retains its flexibility. 'Backreference' can only match this stored content, therefore its accuracy is greater than that of simple wildcards. These were enough against simple virus variants. Figure 2 illustrates how capturing and backreference work.

ANOTHER LIFE

A closer look at Figure 1 reveals some minor deviations in our notation from normal regex implementations. The most apparent is that regex engines are character-based, because they are used almost exclusively in text processing. With the advent of Unicode, the terms 'character' and 'byte' (octet) stopped being interchangeable. However, malicious content still spreads in machine code, and therefore our grammar is still byte-based (see Figure 3). The most frequent repetitions (skips) earned special notations based on their analogy with shell wildcards (e.g. dir *.exe). It is worth noting that regex

```
for i=1 to UBound(kuhk)
    runner=runner&chr(kuhk(i)-2513)
next
Execute runner
```

```
[Ff]or i=1 to [Uu]bound( ([^\\])+
    runner=runner&chr( $1 - [0-9]+ )
[Nn]ext
[Ee]xecute runner
```

Figure 2: A simple script obfuscator illustrating how capturing and backreference work.
For the sake of readability both are in bold and other regex tokens are in italic.

```

B9 1F DC 02 00    mov  ecx, 2DC1Fh      B? {0 +(2) [02,03,04] 00 }
51                  push ecx ; dwSize   5?
33 C0              xor eax, eax     33 C?
50                  push eax ; lpAddress 5?
FF 15 6C 31 43 00 call ds:VirtualAlloc FF 15 +(2) 4? 00
...
BF 1F DC 02 00    mov  edi, 2DC1Fh ; dwSize [B?,C7 [45 ?, 85 ? FF FF FF]] $0
loc_40114E:
80 E5 B6          and ch, 0B6h      ...
8A 0C 16          mov  cl, [esi+edx] 8A [0?, 1?] [00-3F]
88 0A              mov  [edx], cl   88 [0?, 1?]
...
75 EC              jnz  short loc_40114E 75 [C0-F7]

```

Figure 3: Byte sequence captures buffer size which is referred to later entering a loop. The bitmask (B?) proves to be extremely useful when dealing with register encodings in x86 opcodes.

quantifiers and wildcards are not the same. The former can repeat any arbitrary expression, while the latter embodies a repeatable fixed expression, the dot (.) matching arbitrary bytes. As a consequence, wildcards can work with fewer backtrack states. However, scanning in a text-based context demands real quantifier support.

On the other hand, *VirusBuster* notation circumvents the most painful legacy of early regex implementations, which happened to use parentheses for two different purposes: grouping (mostly expressing precedence) and capturing [4]. Our grammar defines separate symbols and supports named capturing only, i.e. the capture must declare which variable to fill in.

However, there are subtle differences under the hood. While a regex engine matches one pattern (or at most a few) against arbitrary lengths of text at a time, a traditional AV scanner does almost the opposite. It has to check if any of countless signatures can be found anywhere amongst thousands of files. The great divide in the number of signatures, matching attempts and the various sizes of input results in a radically different implementation.

Neither the number of files nor their characteristics are under our control, and the proliferation of signatures was

Special features	Description	VirusBuster notation
rewind	move matching point back by N bytes	- (N)
reload	load enough bytes from source to finish the matching attempt	++(N) or --(N)
follow an address	continue matching at absolute position (A)	@ @ (A)
follow an offset	jump to a previously captured offset	++(\$N) or --(\$N)

Figure 4: The ‘irregular’ features in VirusBuster sequences.

not curbed effectively. So we found that the only way to retain performance levels was to reduce the number of superfluous matching attempts or at least the time wasted on evaluation of such. Literal bytes prevent a signature from matching virtually anything because literals are the least flexible parts of a signature. If they do not match at a given point, the signature as a whole will fail. We exploited this fact, in addition to more advanced text search algorithms [5]. The sooner the less flexible token is matched, the sooner the attempt is terminated.

REWIND

In order to achieve this, signatures must be converted to start with as many infrequent literal bytes as possible. The rewind wildcard (- (N)) was previously introduced into the grammar for the purpose of similar manual optimizations (Figure 4). It makes the engine skip backward in the target string, thus - (N) can be considered the opposite of + (N). Moreover, a fairly simple transformation based on this rewind token can move any literal from the middle of an arbitrary complex pattern to its beginning. The real revelation was that this transformation can be automated quite easily, so we were able to benefit from it without the need to modify a signature by hand. Byte prevalence statistics were aggregated from several typical desktop environments to define the most infrequent sequence candidates. The overall engine speed improved by 30%, surpassing our expectations.

The combination of rewind and skip wildcards may combat spaghetti codes where malicious code is split into small

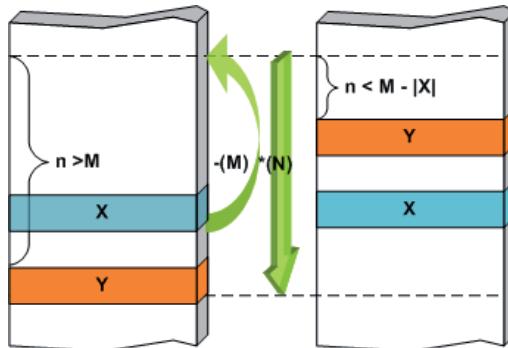


Figure 5: X-(M) * (N) Y: position-independent fragments in spaghetti code. N can be considered the diameter of the ‘spaghetti plate’.

blocks, shuffled and bound together using jump instructions. The physical layout in the file and the runtime trace of the instructions differ so much that it is commonly believed that ‘detection signatures on this kind of code are not efficient at all’ [6]. Figure 5 demonstrates the basic idea of how to write a signature that matches the code blocks in question regardless of their actual order. The exact order and the distance of X from Y may vary from sample to sample, but a single signature with the appropriate limits may match all. As the number of code blocks increases, the number of possible layouts grows exponentially, so other (pattern) constructs should be taken into consideration.

The example in Figure 6 shows another use of this technique in generic detection where a couple of string constants can be matched. Just one of these snippets would not be sufficient to indicate a threat, but their collective occurrence in a narrow range should raise suspicion. We will see how the signature is strengthened further in the next section.

RELOAD

An AV scanner usually does not scan the whole file; instead, in the hope of better performance and fewer false positives, it restricts signature detection to specific areas of the file where there is more chance of malicious content being found. This is the reason

why unlimited repetition is not supported in our grammar. Of course, sometimes the text being searched within is also adjusted before applying a regex. The significant difference lies in the time frame. In the case of regex, preprocessing is presumably carried out right before the matching, being aware of the actual needs. In contrast, the boundaries of the scanning areas in the AV engine are predefined, based on previous experiments, and can be changed slowly according to the required software modification.

However, occasionally the search may have to be extended beyond

these limits. Generic detections often stumble because randomly inserted junk bytes displace valuable bytes from the scanning area. The suspicion generated by the string constants in Figure 6 is confirmed by the malicious opcodes from the end of the scan area. Since the chances are that the actual code block is slipping away, the short forward skip (+20) is replaced with a reload command to ensure that the rest of the signature stays in the scanning buffer. Check the difference between the offsets outlined in yellow.

In other cases a brand new segment of a file should be scanned for specific sequences, for example because a new file infector is spreading in an uncovered area or if a file format which is rare or unknown to the current engine version has to be supported.

Both demands can be satisfied with reload functionality (Figure 8), an idea borrowed from Perl Compatible Regular Expression (PCRE) Library [7]. The reload tokens generate an interrupt toward the pattern matching module to check if the rest of the signature exceeds the boundaries of the current scanning area. If so, the engine tries to find the requested position in the source stream being scanned, which is the file or emulator’s virtual memory in the simplest cases. If it fails, the rest of the signature cannot match and the signature is discarded immediately. Otherwise, it loads the requested number of bytes into the

.00401150:	64 69 72 20-25 73 20 0D-0A 64 65 6C-20 22 25 73	dir %s Model "%s
.00401160:	22 00 00 00-53 45 52 56-45 52 00 00-70 63 69 64	" SERVER pcidump
.00401170:	75 6D 70 00-5C 5C 2E 5C-70 63 69 64-75 6D 70 00	ump \\.\pcidump
.00401180:	73 63 76 68-6F 73 74 2E-65 78 65 00-5C 73 79 73	scvhost.exe \sys
.00401190:	74 65 6D 33-32 5C 00 00-5C 3F 3F 5C-00 00 00 00	tem32\ N??\
.004011A0:	5C 23 79 73-24 65 6D 33-32 00 00-65 78 74 25	\system32 extx
.004011B0:	73 25 64 74 2E 65 78 65-00 00 00 00-73 79 73 74	sxdt.exe syst
.004011C0:	65 6D 33 32-5C 00 00 00 00-5C 00 00 00-74 65 25 73	em32\ \ texs
.004011D0:	25 64 74 2E-64 6C 6C 00-54 68 69 73-20 49 73 20	xdt.dll This Is
.004011E0:	50 45 43 00-5C 5C 2E 5C-70 63 69 64-75 6D 20 00	PEC \\.\pcidump
.004011F0:	73 63 76 68-6F 73 74 2E-65 78 65 00-5C 3F 3F 5C	scvhost.exe N??\
.004011G0:	00 00 00 00-6F 70 65 6E-00 00 00 00-5C 00 00 00	open \
.004011H0:	25 73 25 64-5F 78 65 65-78 2E 65 78-65 00 00 00	\sxd_xeex.exe
.004011I0:	5C 6H 69 6C-6C 64 6C 6C-2E 64 6C 6C-00 00 00 00	\killd11.dll
.004011J0:	53 45 52 56-45 52 00 00-54 54 65 2E-65 72 2E 65	SERVER TTee.e
.004011K0:	61 62 63 64-73 2E 73 73-00 00 00 00-00 00 00 00	abcds.ss
.004011L0:	8A 11 40 00-8A 11 40 00-00 00 20 00-20 00 20 00	\e40 \e40
.004011M0:	20 00 20 00-20 00 20 00-20 00 20 00-28 00 28 00	< <
	00 5C 3F 3F 5C 00 *(f0) "\0\\??\\\\0"	
x	25 73 25 64 *(10)	"%s%d"
	2E 65 78 65 00	".exe\b"
- (M)	- (f0)	"lay the table" with a spaghetti plate of 0x200
* (N)	* (200)	bytes wide, almost symmetrical to the current
		matching point ([-f0, +110]) for the following
		string:
y	00 53 45 52 56 45 52 00	"\0SERVER \0"
	++(20)	skip 0x20 bytes (with a possible reload)
	* (800)	and force the rest of signature to fit in scan buffer
	6a 00 6a 00 6a 02	skip irrelevant (probably junk) bytes
	6a 00 6a 00 ...	start of malicious x86 code

Figure 6: String resources, another dish in a spaghetti plate.

```

.004014C1: 6A00
.004014C3: 6A00
.004014C5: 6A02
.004014C7: 6A00
.004014C9: 6A00
.004014CB: 6800000040
.004014D0: FF7508
.004014D3: FF151C104000
.004014D9: 8945F0
.004014DC: 8B45F0
.004014DF: 8945F4
.004014E2: 83D8F000
.004014E6: 0F849D000000
.004014EC: FF7510
.004014EF: FF750C
.004014F2: 6A00
.004014F4: FF1518104000
.004014FA: 8945E8
.004014FD: 8B45E8
.00401500: 8945E4
.00401503: FF75E8
.00401506: 6A00
.00401508: FF1514104000
push    0
push    0
push    2
push    0
push    0
push    0400000000 ;'e '
push    d_lehp1[8]
call   CreateFileA ;KERNEL32
mov    [ebp1[0F0]],eax
mov    eax,[ebp1[0F0]]
mov    [ebp1[0F4]],eax
mov    eax,[ebp1[0F0]],0
cmp    .000401589 -1
jz    .000401589 -1
push    d_lehp1[010]
push    d_lehp1[00C]
push    0
push    0
call   FindResourceA ;KERNEL32
mov    [ebp1[0E8]],eax
mov    eax,[ebp1[0E8]]
mov    [ebp1[0E4]],eax
push    d_lehp1[0E8]
push    0
call   LoadResource ;KERNEL32

```

Figure 7: The continuation after the reload point of the sample and sequence in Figure 6.

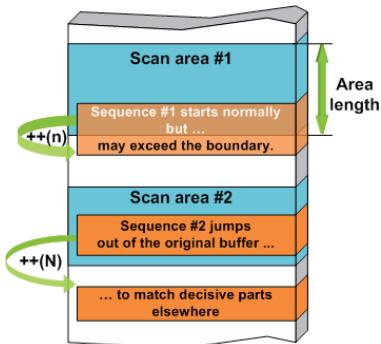


Figure 8: The two commonly used cases of RELOAD.

```

16 0 obj
<< /Type /Action /S /Launch /F << /F << /C /AAAAA
...>>
++(1500) *(500)
endobj
<< /JavaScript 29 0 R >>
endobj
27 0 obj
<< /Length 296 /Filter /FlateDecode >> stream
...

```

Figure 9: Jump to the next encoded stream if sled is discovered in the current scan area.

```

37 26
[E8, E9]
++(1)
[00 00 00, FF FF FF]
-(c0)
*(1e0)
8D 80 ? F5 FF FF[50 C3, E9]
-(90)
*(1e0)
[C2, 00] [92, 00] C1 C8 [11, 21]

```

Figure 10: The smallest, but efficient reload.

scanning buffer and continues the matching with the next token. The three reload tokens are extensions of the basic forward and rewind tokens (++(N) and --(N)) for relative

positioning (Figure 9) and the special address token (@@(A)) to follow absolute addresses pushed onto stack or file markers. Figure 9 shows the exploitation of a PDF document in JavaScript where the payload is displaced due to the 4KB spray. The spray is still in the scanning area, so a signature, start matching the spray and then reload, may succeed.

In Figure 10, a single skipped byte (+(1) or ?) is substituted for the reload token (++(1)) to ensure that enough bytes will be loaded into the scanning buffer and thus all three shuffled code junks can be matched in it. The skipped byte is the least significant byte of the target address of a CALL/JMP instruction.

FOLLOW

The combination of reload and capturing is also a particularly useful feature. If the positioning tokens (skip, forward, rewind and address) can accept captured variable content, it eventually enables the signature to parse and traverse low-level formats (Figures 11 and 12).

According to the addressing mode of the x86 CPU family, at least the multiplication of captured offsets should also be implemented.

A MATTER OF LIFE OR DEATH

After this overview of recent signature grammar, take a look at more general definitions of signature-based detection: 'A signature is a small piece of data which uniquely identifies an individual item of malware (...) Signatures can be made more flexible to allow for generic detection of similar items of malware' [8]. So, a single signature may detect a large number of viruses. Admittedly, this kind of generic detection is less likely to be effective against completely new viruses and is more effective at detecting new members of an already known family. Still, its significance cannot be neglected in view of its reported efficiency [9].

Figure 13 shows another interesting result of a more recent survey over our own malware collection. The vast majority of the top recognitions (i.e. those which detect the most samples) utilize signatures either on mere file fragments or on emulated data. Some signatures are considered strong enough to indicate the threat itself. In terms of numbers, three single signatures are responsible for detecting nearly one million samples, and about 30 signatures in certain combinations detect a tenth of our malware collection.

NO PRAYER FOR THE DYING

The main characteristic of pattern matching, however, is also its utmost weakness. It grabs the samples' common

```

68 {0 +(4) } capture the pushed address of Visual Basic's
@@($0) internal structure
56 42 35 21 jump to investigate this structure
check VB5! marker
.0040118C: 68 0134000 push    0004013C0 ;'VB5!' —t1
.00401191: E9 EFFFFFFF call    MSUBUM60.100 ;MSUBUM60 —t2
.00401196: 0000 add     [eax].al

```

Figure 11: The virtual address of Visual Basic internal structure.

```

+ (214) move to the form descriptor
{1 +(4) } capture virtual address of
@@($1) MdlInject Proc_2_1
- (4B) and follow it
1B 13 00 1B ... P-Code of SetThreadContext
and the others...

```

```

Project
  Forms
    Frm3
    UserControls
  Code
    Class1
    Frm3
  MdlInject
    Proc_2_0_40475C
    Proc_2_1_4061BC
    Proc_2_2_404218
    Proc_2_3_4038EC
    Proc_2_4_405BD0
  CallME
  MdKillers
  MdID
  MdDbg
  API

```

Figure 12: The matched P-codes at the end of the journey.

traits at a very low, machine level, and therefore this technique is susceptible to modification (think of server-side polymorphism). This sensitivity sometimes comes in handy. Static decryption of polymorphic malware can be strengthened if a signature can provide valuable input for the decoder component. (Even when real decryption is not possible, other cryptanalysis methods can be backed by advanced pattern matching to extract other characteristics strong enough to form detection.) Let us consider the signature matching a decoder fragment shown in Figure 14.

These values locate the encrypted content, making brute force iterations and superfluous decrypting steps unnecessary; on the whole it streamlines the operation and probably speeds up detection. This data collection and propagation technique can be utilized throughout an AV engine. Besides cryptanalysis, database-driven unpacking may take advantage of it in order

to boost emulation performance. During emulation, signatures identify substitutable code chunks which trigger built-in native implementations with proper parameters. This is also the primary source of input for malware-specific decision algorithms.

LIFE AFTER DEATH

Beside the feature richness there are other benefits of reusing software components. When we were planning the Win32 API-based behavioural detection, it was revealed that the natural representation of an API trace was a regular log file. The two main tasks in this scenario were to log API function calls and search in them for malicious API trace fragments. The former was quite straightforward; emulator hooks sent messages to a textual log file for the sake of readability. From that point, the search resembled text processing which was also quite simple with the hairy old regex-like pattern engine. The first version of the test engine was built within a week and was ready to explore the capabilities and limitations of this behavioural-based detection method. The following week, the first API trace detections were written by our virus analysts against real malware samples.

Of course, the final version superseded the proof of concept in more fields. The entire API trace search was split into a high-level API call order component and a low-level API argument monitoring component. The API call order was matched by a dedicated binary algorithm for maintainability purposes. However, our regex-like grammar served the low-level argument matching needs entirely, which should not have been a surprise in the light of the aforementioned. It actually performs better since just-in-emulation-time argument checking replaced the concept of log file. The fact is that we could use pattern matching with or without text processing both effectively and efficiently.

How did we benefit from the early prototype? First, it elongated the research period which, in turn, allowed us to evaluate special cases like anti-emulation and anti-debugging, emulation flaws and other shortcomings in more depth. More feedback helped us design more prudently. Second, it meant that the research and development could work in parallel, which guaranteed that, despite its complexity, the project would finish in time. Finally, using a tested and verified component made the whole concept a more robust and mature technology, even from the start.

CONCLUSION

The limitations of pattern matching are plain to see, but you may also catch a glimpse of how far it can be improved.

Malware name	Samples	Data collected from	Detection based on
Worm.Allapple.Gen	541,791	emulator	one signature
Packed/Upack	448,532	file	11 signatures offset from entry point and specific exception list
Trojan.OnlineGames.Gen.107	290,742	file	two signatures
Adware.Trymedia.E	240,324	file	checksums
Win32.Knat.A	231,598	file	one signature
Dialer.Zugang.Gen	223,781	file	1+2 signatures' combination
Trojan.DL.Swizzor.Gen!Pac.4	222,795	file	two signatures + constraints
PS-MPC_generic	201,437	file or emulator	10 signatures
Dialer.Agent.Gen	201,208	file	one signature
Win32.Virut.Gen	195,966	both file and emulator	dedicated decision algorithm

Figure 13: The classification of top 10 detections over the VirusBuster collection in July 2009.

```

xor edi, eax          33 F8
xor eax, eax          33 C0
add edi, 2             83 C7 02
mov ecx, offset [encoded_begin] B9 {E +(04) }
inc byte PTR ds:[ecx] FE 01
inc ecx               41
cmp ecx, offset [encoded_end] 81 F9 {F +(04) }
jnz short loc_1      75 F5
mov edi, 0B            BF 0B 00 00 00
inc eax               40
cmp eax, decode_repeat 3D {0 +(04) }
jnz short loc_2      75 E0
xor edi, edx          33 FA

```

Figure 14: The start and end offsets of the area to be decoded are captured and stored in the variable \$E and \$F, respectively. The number of iterations will be stored in variable \$O.

Even though hundreds of thousands of pieces of malware daily manage to evade signature detection and the concept of this reactive technology is no longer effective, the software component can be repurposed with success and numerous stunning features could be added to serve both static and dynamic detection methods better.

Nevertheless, regular expression is backed by the solid mathematical background of formal language theory. At the dawn of computer science, the term ‘regular’ was precise and adequate; it referred to the expressive power of the formal regular grammar (Type-3 grammars) in Chomsky’s hierarchy [10]. Although regex implementations still acknowledge this heritage in their names, they exceeded this strict limit quickly. We haven’t touched the conceptual details, but they can no longer be treated as regular grammars. Moreover, certain research and development [11] in this field looks very exciting and promising, especially, for example, parsing expression grammar [12].

A whole new generation of file format detections can be built on the top of that architecture which may have considerably shorter reaction time due to the managed code environment provided by such implementations. I think we should think twice before calling anything ‘dead’.

ACKNOWLEDGEMENTS

I would like to thank my colleagues, especially Gabor Szappanos and Robert Neumann, for their valuable feedback and helping me to understand how virus analysts squeeze out the most from the presented features.

REFERENCES

- [1] http://www.webopedia.com/TERM/V/virus_signature.html.
- [2] http://en.wikipedia.org/w/index.php?title=Computer_virus&oldid=337353875#Self-modification.
- [3] <http://www.regular-expressions.info/tutorial.html>.
- [4] <http://www.regular-expressions.info/brackets.html>.
- [5] Navarro, G.; Raffinot, M. Flexible Pattern Matching in Strings. Cambridge University Press, 2004 reprinted (ISBN-10:0521813077).
- [6] Ciubotariu, M. What next? Trojan. Linkoptimizer. Virus Bulletin, December 2006, p.6.
- [7] <http://regexkit.sourceforge.net/Documentation/pcre/pcrecallout.html>.
- [8] <http://www.virusbtn.com/resources/glossary/signature.xml>.
- [9] Szappanos, G. Exepacker Blacklisting, Virus Bulletin October 2007, p.14.
- [10] http://en.wikipedia.org/w/index.php?title=Chomsky_hierarchy&oldid=321254719.
- [11] Parrot Grammar Engine: http://docs.parrot.org/parrot/latest/html/docs/book/pct/ch04_pge.pod.html.
- [12] http://en.wikipedia.org/w/index.php?title=Parsing_expression_grammar&oldid=335106938.
- [13] Friedl, J. Mastering Regular Expressions, 2006 3rd Edition. O'Reilly (ISBN-13: 978-0596528126).

TUTORIAL

EXPLOIT KIT EXPLOSION – PART ONE

Mark Davis

Exploit kits used in drive-by browser-based attacks are a dime a dozen these days, with a new kit emerging in the wild every few weeks. A multitude of kits, a.k.a. packs, now exist after several years of PHP/SQL kit development in the criminal underground. Some kits are developed for private use, while others are sold for amounts ranging from a few hundred to several thousand dollars dependent upon sophistication and capabilities. Many kits appear to be Russian in origin, with Cyrillic characters appearing in comments, Russian login options, and reference in some cases to known Russian cybercriminals.

This is the first article in a two-part series introducing exploit kits. The second part will look at exploit vectors, URL identification, and risk associated with exploit kit attack vectors.

BASICS

Many have heard of exploit kits and/or understand the basic nature of a drive-by attack using such a kit, but fewer know them by name. Names for kits, unlike malcode, are often assigned by the creator, used in logos, logon screens, in comments within kits and advertisements online in various underground forums. While not exhaustive, a fairly comprehensive list of exploit kits used in malcode attacks in the wild is as follows:

Adpack	Mypolysploit
Adrenalin	Napoleon Sploit Kit
Armitage	Neon
Crimepack	Neosploit
Eleonore	Nuc Pack (Nuclear)
Fiesta	Nuke
Firepack	Papka Pack
Fragus	Pheonix
FSPack	SEO Sploit Pack
G-pack	Shamans Dream Pack
Icepack	Siberian Exploit Pack
JustExploit	Smartpack
Liberty	Sploit25
Luckysploit	Tornado
Max\$ Sploit System	Unique Pack
mPack	Webattacker
Multisploit	YES!

This list does not include other types of web-based C&Cs used to manage DDoS attacks, botnets, or other frameworks and is limited to actual exploit kits used in drive-by attacks. Some of the most recent kits to emerge include the Siberian Exploit Pack, Shaman's Dream Pack, and Papka Pack, while the older packs in the wild include Webattacker, mPack and Neosploit. Yes!, Fragus, Eleonore, Fiesta, Unique Pack, Liberty, Luckysploit and Neosploit are some of the more commonly used (and effective) kits in the wild in 2010. The kits commonly include authentication for administrative login in Russian, English, and/or other languages.

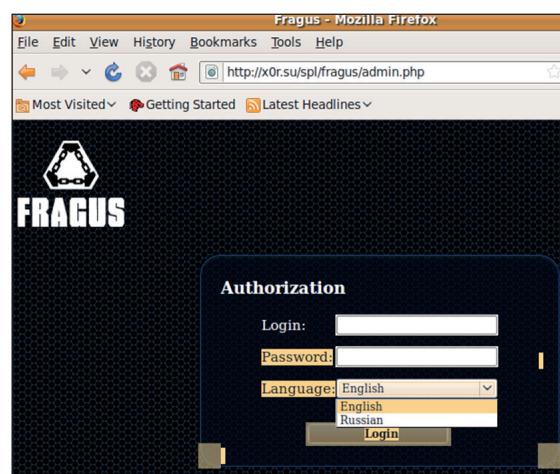


Figure 1: Fragus supports English and Russian login options.

After logging into an exploit kit, statistics on infections and/or zombie reports are typically presented to the admin.

Since the emergence of exploit kits there has been a notable change in browser use. In the beginning, *Internet Explorer* was the primary vector but now *Firefox* and *Opera* are commonly included, as is *Safari* in some cases, as seen in the Fragus statistics shown in Figure 2. Information on the operating systems in use is also collected to aid developers in targeting specific browsers and operating systems of interest. Geographic location is of great importance for several reasons including possible counter-intelligence against researchers, monetization needs (such as money mules in specific countries), proxy needs (tunnel through a specific geographic region or country), affiliate financial rewards for compromises within a specific country or geographic region, and/or others.

Exploit kits also allow a remote file to be uploaded as part of payload management when exploitation is successful.

Options such as 'Add file' by Fragus help kit developers to protect their own intellectual material. Rather than

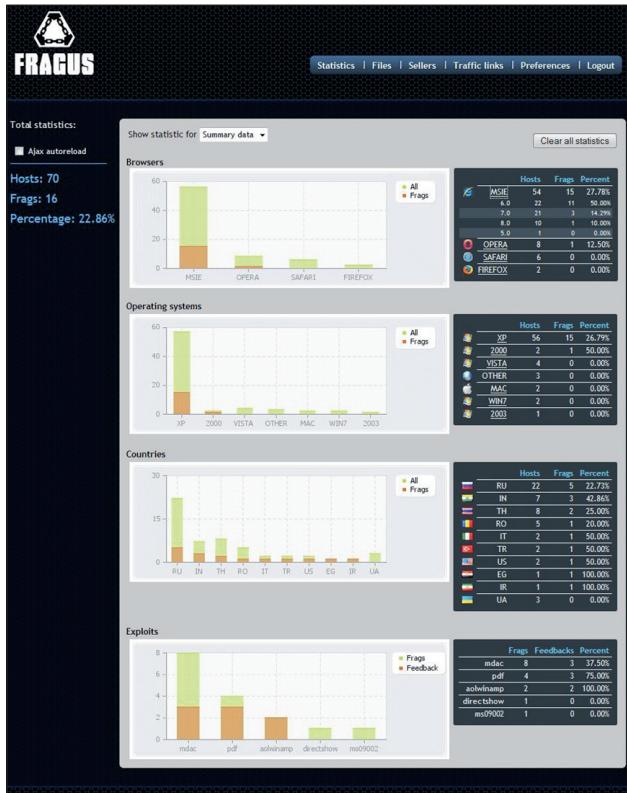


Figure 2: Fragus statistics include bar graphs and core data for exploit metrics.

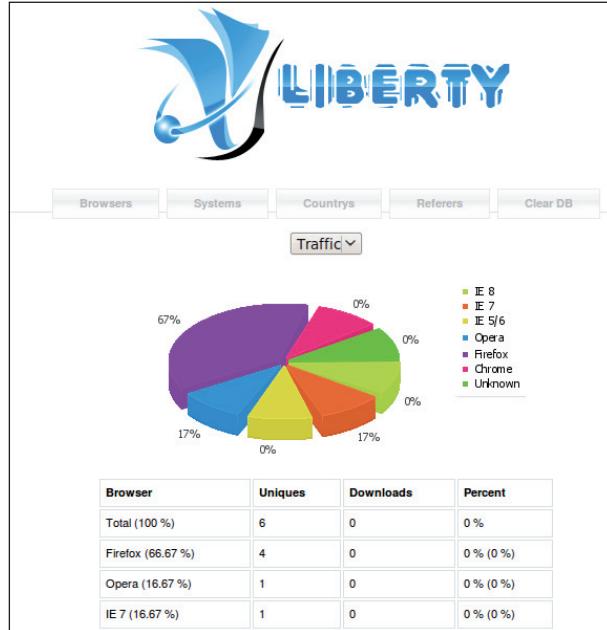


Figure 3: Liberty details traffic to an exploit kit site by browser, showing Firefox as the main browser.

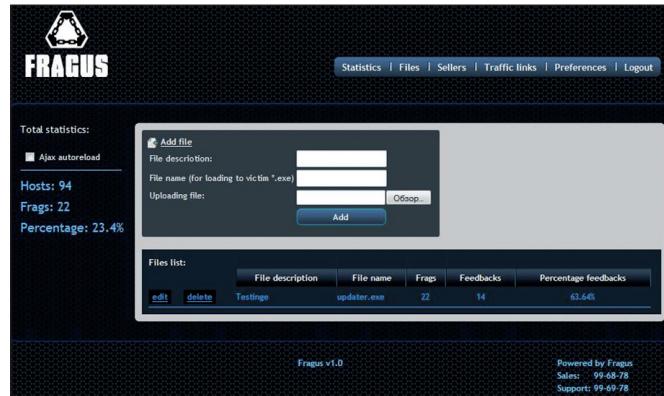


Figure 4: Fragus 'Add file' allows a file to be uploaded for use with the kit.

deliver raw files to clients they can configure a server or compromised computer with an exploit kit. Some developers will do this as part of a service offering for operating and/or maintaining an exploit kit purchased by a client. As a result, clients need only use a web-based interface to upload and/or manage an attack rather than configure and set up a server for PHP/SQL exploit kit capabilities, and without the need to manage back-end files.

Referrals are often included in kits as a way to track where attackers get the best traffic for exploitation. For example, if ten sites are compromised and configured for iFrame redirection to an exploit kit site, a referral page can be consulted to see the top referrals and areas of success. Such metrics enable attackers to manage iFrame and server compromise efforts for maximum success.

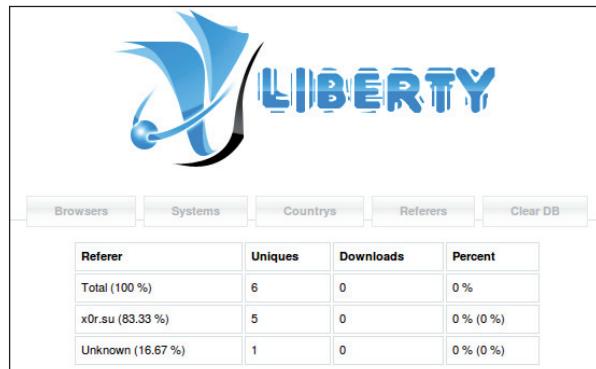


Figure 5: The Liberty 'Referers' [sic] page reveals that x0r.su is responsible for 83% of traffic to the exploit kit.

Note that words like 'referral' and 'referrers' are frequently misspelled by the developers of exploit kits.

Demonstration kits are frequently distributed via online forums and file-sharing sites. Such demonstration kits have

COMPARATIVE REVIEW

limited functionality and do not include core exploit files. Most kits look very similar, with about a dozen different PHP pages for managing core functionality, reporting and management of payloads, along with a few standard exploits used in the kit (but rarely a comprehensive set of exploits).

Fragus files	YES! 2.0 files
<DIR> images	<DIR> admin
<DIR> secure	<DIR> css
<DIR> exploits	<DIR> images
<DIR> files	<DIR> js
<DIR> templates	<DIR> scripts
.htaccess	<DIR> wallpapers
browser.php	frame.php
config.php	index.php
GeoIP.dat	login.php
geoip.php	sample.php
javascript.php	serv.php
pchart.php	<DIR> etc
shellcode.php	<DIR> img
tahoma.ttf	<DIR> load
.htaccess	<DIR> sall
admin.php	index.html
click.php	<DIR> exe
directshow.php	log.dat
load.php	<DIR> include
pdf.php	403.php
robots.txt	404.php
show.php	.bmp
sql.sql	close.bmp
stat.php	geoip.dat
	geoip.inc
	icon.bmp
	index.html
	spl.php
	vars.php
	config.php
	dump.sql
	funcs.php
	functions.php
	hosttest.php
	index.php
	load.php

The next article will detail the functionality of common PHP and SQL elements of such kits. In addition, we will look at interesting metrics around exploits used in kits, the success of exploits in the wild, and mitigation elements such as unique URI elements and exploit characteristics will be overviewed.

VB100 – WINDOWS XP SP3

John Hawes

Our last comparative on *Windows XP* (see *VB*, April 2009, p.15) saw a record number of entries, with what seemed like an enormous 39 products taking part. This record was broken late last year with our first look at the gleaming new *Windows 7* platform when 43 products took part. As we came around to *XP* once more, we expected to see yet another new record set, but when the test deadline came, all expectations were exceeded by a seemingly endless flood of submissions arriving in the lab team's inboxes. With new arrangements made to allow the participation of products that require Internet access to install and acquire updates, even the simple task of acquiring the products for the test became a serious test of our time and resources. Network connections slowed to a crawl thanks to the multiple large downloads, and our storage capacity began to fill ominously. All test systems were in constant use as the less flexible solutions were installed, activated, updated and snapshots taken for testing.

In the end, a monster 60 products were accepted into the test, although we made it clear to vendors who submitted multiple entries that we would only be able to test them all if time allowed. With just a month to plough through all these products, it was clearly going to be a busy time, and after some trial runs in recent tests we had plans to add yet further to the selection of performance data being gathered. As soon as circumstances allowed, we buried ourselves in the lab with plenty of hot drinks and notepaper, preparing for the long haul. If you have a day or two to spare to read through this report, we hope you'll find some of our findings informative.

PLATFORM AND TEST SETS

Despite its now venerable age, the *XP* platform remains the most popular operating system on the planet, with most estimates agreeing that it runs on more than 50% of all computers worldwide. It is now, in a manner of speaking, a grandparent – succeeded by two newer generations of the *Windows* operating system – and is a full year into the ‘extended support’ phase, with the plug finally due to be pulled in four years. It seems likely that large numbers of users will stick by it for much of that time, thanks to the stability and simplicity of use for which it has acquired such a strong reputation.

Running yet another test on the platform (our tenth so far, including 64-bit editions) required little effort in the set-up phases; test images from the last round were dug

out, and a few adjustments made to fit in with changes to the lab network set-up, but no major work needed doing before fresh images were created. The systems were thus running bare *XP Professional SP3*, with no additional updates, and a handful of tools such as PDF viewers and archive tools, as per our standard operating procedure. With the unprecedented popularity of this comparative, a batch of new systems were also roped in for the test, with a near-identical environment installed on slightly more powerful hardware; these would be used for the donkey work of the big slow scans of the large test sets, while all performance-related tests would be run on the standard set of matching machines.

At the core of our performance tests are the speed sets, originally built by harvesting all files from a selection of *Windows* systems of varying degrees of lived-in-ness and dividing them by file type. These remain unchanged from the last several tests and although we hope to freshen them up in the near future, their content remains fairly reflective of normal ratios of different types of files. The content of these sets is deliberately made as common and widely used as possible, to minimize the possibility of false alarms, as the speed sets are counted as part of the false positive test. The system drive of the test machine is also considered part of the false positive test, although this should not cause any problems for any reasonably cautious product. Much of the testing using these sets is automated, and some adjustments were made to the automation scripts this month in order to gather further data from the test systems while the tests were being run; details of the methods used for this will be provided below.

The main bulk of our false positive test is labelled simply the ‘clean set’, and this saw some considerable expansion this month, with various new packages added including files harvested from a number of machines and CDs acquired by the lab team in recent months – a number of games and several sets of disk-burning utilities prominent among them. The set has also been pared down to exclude more obscure and insignificant items, and we plan to continue this process of tuning the set to reflect the more important items in future. For this month’s test, the set contained close to half a million files.

Compiling the infected test sets has been considerably simplified of late by some improvements in automation. Ever larger numbers of new samples flood in from a growing range of sources, and are put through various types of checks and analyses before being considered for our test. These include static checking of file types and parameters, classification processes and dynamic analysis of behaviours. To save time in the tight comparative schedule, we tried to get as much of this work done as possible prior to building the sets, but as ever with the RAP sets being compiled well

into the allotted time period many of these checks had to be left until testing was well under way. For this month’s test, the four weekly RAP sets seemed somewhat more even than usual, with between 8,000 and 9,000 samples in each. The trojans set was built with samples gathered in the month or so between the end of the last RAP period and the start of this one, and a considerable expansion was made to our set of worms and bots, with samples from the same period adjudged to fit into this category added to the set. The polymorphic set saw only minimal adjustments, with a number of W32/Virut strains that had recently fallen off the WildList added to the set in expanded numbers.

The WildList set itself was aligned with the latest list available on the test set deadline of 20 February, which meant that the January list (released on 17 February) just made the cut. This list included the usual smattering of new samples, dominated by Autorun and Koobface worms and online gaming password stealers. What immediately stood out, however, was yet another strain of W32/Virut, which had appeared on the list since our last test. As always, large numbers of samples were replicated from the original control sample, each one checked to prove it capable of infecting other files, and the set was closed at a total of 2,500 Virut samples – which should be plenty to thoroughly exercise each product’s capabilities at detecting this complex polymorphic virus in all its disguises. Also of note this month was the return of an old complex polymorphic threat, W32/Polip, which first appeared in mid-2006 and has remained in our polymorphic sets for some time. Again, some 2,500 samples were moved to the WildList set to represent this threat.

PERFORMANCE AND RESOURCE USAGE MEASUREMENTS

For some time now we have been including a variety of performance measurements along with the detection results in these comparatives; a few years ago we added on-access speed measurements to the on-demand throughput figures, and with such an epic test before us, now seemed the perfect moment to further add to our data.

Throughout this month’s test, we planned to take a selection of measurements of the usage of system resources – such as RAM and CPU cycles – at various stages and to see what data could be harvested from them for presentation in these pages. In the final reckoning, with the publication deadline already disappearing behind us and much work still to do, it seemed sensible to pull as much of this data together as possible into a simple and easy-to-read format. To this end we have focused on two simple measures: the total available memory and the percentage of CPU cycles in use, and split them into two types of measurement – with the system idle,

On-demand tests	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum	0	100.00%	105	97.96%	191	89.11%	1255	89.39%		1
AhnLab	0	100.00%	424	91.75%	8	99.59%	5703	51.78%		2
Alwil	0	100.00%	28	99.46%	507	93.28%	197	98.33%		
Arcabit	0	100.00%	747	85.47%	1319	79.03%	5781	51.12%	6	
Authentium	0	100.00%	140	97.28%	3	99.85%	1759	85.13%	4	
Avanquest	0	100.00%	46	99.11%	1989	65.32%	446	96.23%	1	
AVG	0	100.00%	17	99.67%	26	98.79%	284	97.60%		
Avira (Personal)	0	100.00%	11	99.79%	0	100.00%	148	98.75%		
Avira (Professional)	0	100.00%	11	99.79%	0	100.00%	148	98.75%		
BitDefender	0	100.00%	24	99.53%	0	100.00%	618	94.78%		
Bkis (Gateway Scan)	3	99.58%	807	84.31%	2773	51.85%	6551	44.61%		
Bkis (Home Edition)	18	97.50%	847	83.53%	2776	51.20%	6551	44.61%		
Bullguard	0	100.00%	18	99.65%	0	100.00%	316	97.33%		
CA (ISS)	0	100.00%	432	91.60%	958	92.06%	5184	56.17%		
CA (Threat Manager)	0	100.00%	430	91.64%	958	92.06%	5063	57.19%		
Central Command	0	100.00%	109	97.88%	191	89.11%	1229	89.61%		1
Check Point	1	99.9999%	56	98.91%	9	99.91%	379	96.80%		5
Defenx	0	100.00%	109	97.88%	191	89.11%	1251	89.42%		1
Digital Defender	0	100.00%	135	97.37%	191	89.11%	1338	88.69%		1
eEye Digital Security	104	99.99%	282	94.52%	288	83.47%	2764	76.63%	3	
Emsisoft	974	99.95%	10	99.81%	1285	78.59%	202	98.29%	1	1
eScan	0	100.00%	18	99.65%	0	100.00%	320	97.29%		3
ESET	0	100.00%	23	99.55%	0	100.00%	172	98.55%		
Filseclab	1548	97.97%	310	93.97%	9913	41.20%	1881	84.10%	5	1
Fortinet	0	100.00%	330	93.58%	30	99.09%	3099	73.80%	1	
Frisk	0	100.00%	185	96.40%	0	100.00%	1997	83.12%	1	
F-Secure (Client Security)	0	100.00%	18	99.65%	0	100.00%	532	95.50%		
F-Secure (PSB Workstation)	0	100.00%	18	99.65%	0	100.00%	532	95.50%		
G DATA	0	100.00%	4	99.92%	0	100.00%	11	99.91%		
Ikarus	973	99.95%	3	99.94%	1285	78.59%	142	98.80%		1
iolo	0	100.00%	186	96.38%	3	99.85%	1984	83.23%	1	

(Please refer to text for full product names)

On-demand tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
K7	0	100.00%	56	98.91%	0	100.00%	463	96.09%		1
Kaspersky (Anti-Virus 2010)	0	100.00%	45	99.12%	0	100.00%	255	97.84%		
Kaspersky (Anti-Virus 6)	1	99.9999%	74	98.56%	1	99.999%	545	95.39%		
Kingsoft (Advanced)	0	100.00%	1008	80.40%	2382	56.61%	10525	11.02%		
Kingsoft (Standard)	0	100.00%	934	81.84%	2382	56.61%	9352	20.93%		
Kingsoft (Swinstar)	6	99.17%	659	87.18%	3350	47.72%	6625	43.99%	1	
Lavasoft	0	100.00%	15	99.71%	1994	65.16%	107	99.10%	2	
McAfee Total Protection	0	100.00%	31	99.40%	4	99.997%	484	95.91%		
McAfee VirusScan	0	100.00%	46	99.11%	1	99.999%	786	93.35%		
Microsoft	1	99.9999%	30	99.42%	0	100.00%	543	95.41%		
Nifty Corp.	1	99.9999%	71	98.62%	1	99.999%	673	94.31%		5
Norman	104	99.99%	284	94.48%	293	82.92%	2789	76.42%	3	
PC Tools (Internet Security)	0	100.00%	25	99.51%	0	100.00%	243	97.95%		
PC Tools (Spyware Doctor)	0	100.00%	25	99.51%	0	100.00%	245	97.93%		
Preventon	0	100.00%	135	97.37%	191	89.11%	1338	88.69%		1
Proland	0	100.00%	111	97.84%	191	89.11%	1308	88.94%		1
Qihoo	0	100.00%	23	99.55%	11	99.98%	354	97.01%		
Quick Heal	0	100.00%	188	96.34%	5	99.51%	1955	83.47%		
Rising	0	100.00%	620	87.94%	1130	70.02%	5435	54.05%		
SGA Corp.	0	100.00%	26	99.49%	0	100.00%	364	96.92%		
Sophos	0	100.00%	44	99.14%	0	100.00%	554	95.32%		3
SPAMfighter (VIRUSfighter Plus)	0	100.00%	136	97.36%	191	89.11%	1360	88.50%		
SPAMfighter (VIRUSfighter Pro)	0	100.00%	135	97.37%	191	89.11%	1338	88.69%		
Sunbelt	0	100.00%	15	99.71%	1994	65.19%	121	98.98%	2	
Symantec (Endpoint Protection)	0	100.00%	38	99.26%	0	100.00%	324	97.26%		
Symantec (Norton Antivirus)	0	100.00%	21	99.59%	0	100.00%	392	96.69%		
Trustport	0	100.00%	3	99.94%	0	100.00%	23	99.81%		
VirusBuster	0	100.00%	109	97.88%	191	89.11%	1229	89.61%		
Webroot	0	100.00%	36	99.30%	0	100.00%	483	95.92%		

(Please refer to text for full product names)

and during heavy file accessing activity. The latter measures were all taken during our standard on-access tests, and while the data could possibly be split into different sets and so on for greater granularity, it seemed preferable to keep things simple.

The measures were taken using the *Windows Performance Monitor* via a command-line tool run as part of the normal test scripts. Figures for the RAM and CPU usage were taken every 15 seconds during the on-access speed tests while files from the speed sets and the system drive were being accessed by our opener tool, and their MD5 checksums taken. These figures were trimmed of the highest and lowest ten per cent to minimize anomalous data, and then averaged. Idle times were taken from several five-minute periods left alone throughout the course of each product's test period, again with snapshots every 15 seconds, trimmed and averaged, and both sets of figures were compared with baselines generated on identical systems with no security software present.

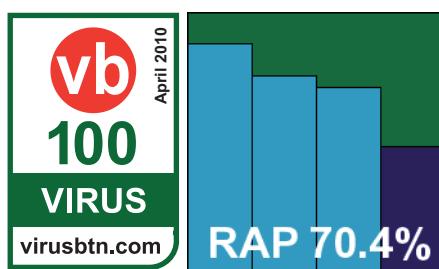
The final figures were calculated as the percentage increase from the baseline measures to the figures taken with each product installed and running. This should give some indication of the impact of the product on the system, although there are, of course, a number of provisos. The figures should not be taken as a definitive indicator of relative performance during all computing activities – these initial measures are something of a trial, for now presenting purely academic information on fairly unnatural behaviour. We hope in future to introduce a series of such measures taken during more generally applicable activities, to provide a more complete and accurate benchmark of variations in performance between products. As always, we aim to continue to improve and expand the value of our tests.

Speaking of which, let's start looking at those products.

Agnitum Outpost Security Suite Pro 6.5.2514.0685

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	89.39%
Worms & bots	97.96%	False positives	0

First on the test bench this month was Agnitum's *Outpost* suite. This was provided, with the latest updates



included, as a single executable which surprised us by being a mere 51MB. Some initial problems soon revealed that this was not the full package, and a retry at downloading gleaned a much more substantial 86MB file. The installation process involved quite a number of steps, most of which related to setting up the firewall component. In all, it took around three minutes to complete and a reboot was required to finalize the installation.

The interface is clear and businesslike, with much of the focus on the firewall and intrusion-prevention components. A small amount of space in the configuration section is dedicated to the anti-malware settings, and provides some basic controls which proved ample for our requirements. The test ran through smoothly with no notable issues, apart from an interesting 'training mode' pop-up requesting permission for our file-opening utility to run.

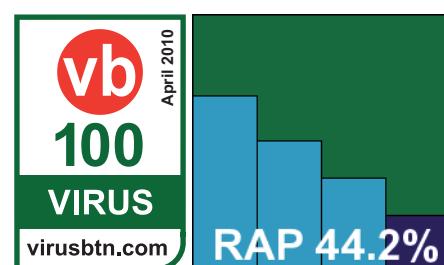
Scanning speeds were fairly good on demand – initially somewhat slow thanks to the thorough default settings, but improving notably in the 'warm' scans, once files had become familiar. In our new performance measures, it seemed fairly light on both CPU and RAM usage, especially given the complexity of the product.

In the detection tests, after the initial false start we soon gathered some useful logs, which showed solid coverage across the standard sets and a good coverage of the reactive part of the RAP test, with a sharp drop in the proactive week. The core components of the certification sets were handled without problems though, and *Agnitum* takes the first of what promises to be a record batch of VB100 awards earned this month.

AhnLab V3 Internet Security 8.0.26

ItW	100.00%	Polymorphic	99.59%
ItW (o/a)	100.00%	Trojans	51.78%
Worms & bots	91.75%	False positives	0

AhnLab also provided its product with updates rolled in, with the installer executable measuring around 81MB.



The set-up process was pretty speedy, with only a few 'next' clicks and it was all done in under a minute, with no reboot required. The product interface is simple and clean, with professional-looking configuration panels for the pickier

user, and it all seems to run quite sensibly. The only confusing aspect is the division of detections into malware and spyware, with separate logging and treatment of each; this resulted in occasional moments of confusion when items appeared not to have been detected but in fact the detections had simply been logged in a different place.

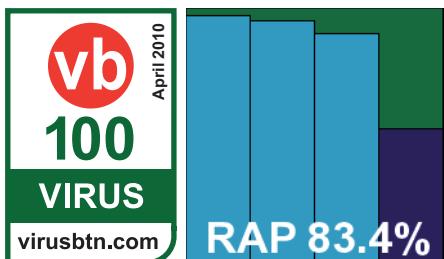
From there on the test ran smoothly without interruption. On-demand scanning speeds seemed fairly middle-of-the-road, with no caching of results to enhance speed. On access things were much better, with some very light lag times, and the new performance figures showed a similar dichotomy, with pretty low RAM drain but much more standard impact on CPU cycles.

Detection results were a little below par in the trojans and RAP sets, but pretty decent in the polymorphic and worms and bots sets; the WildList was handled with no problems, and with no false alarms in the clean sets *AhnLab* earns a VB100 award.

Alwil avast! free antivirus 100224-1

ItW	100.00%	Polymorphic	93.28%
ItW (o/a)	100.00%	Trojans	98.33%
Worms & bots	99.46%	False positives	0

Alwil's thoroughly refreshed version of *avast!* was enthusiastically reviewed in these pages a few months ago (see *VB*,



January 2010, p.17), and we looked forward to seeing it back on the test bench. The company opted to enter only its free version for this test, having included both the free and professional editions in the recent *Windows 7* comparative. The product was provided with the latest updates in a compact 41MB executable, and installed in remarkable time. Only two steps were involved – one of these offered to install the *Google Chrome* browser for greater security online, while the other recommended users contribute to a community data-collection scheme. No reboot was required, and everything was happily up and running in seconds.

The new GUI remains extremely impressive both in its clear functionality and its sheer beauty. It ran fast and nimbly, with excellent responsiveness and rock-solid stability. While the new performance stats showed fairly notable increases in both RAM and CPU usage, the scanning speeds and

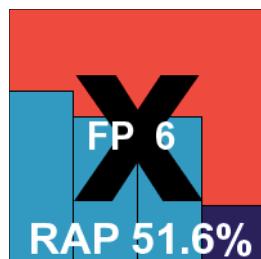
on-access throughput measures were excellent, especially the 'warm' times, making for some splendid figures.

Detection rates were also extremely impressive across the board, with only a rather steep decline in the RAP 'week +1' set worthy of note; no issues were observed in the clean sets or the WildList, and the free version of *avast!* is a worthy winner of a VB100 award.

Arcabit ArcaVir 2010 10.2.3204.4

ItW	100.00%	Polymorphic	79.03%
ItW (o/a)	99.86%	Trojans	51.12%
Worms & bots	85.47%	False positives	6

Arcabit's ArcaVir also comes pre-updated, as a 90MB executable. The first action on launching is to offer the choice of Polish or English language, reflecting the product's home market. Having made a selection, nothing seemed to happen for almost a minute while it prepared itself, and then the full installation process began. This went through the standard handful of steps before setting about its business. The process seemed to run swiftly but lingered again – while claiming to have '0 seconds' remaining – for almost two minutes. When it eventually finished, a reboot was demanded, and the whole process took four or five minutes in all. On some occasions we had some problems with the install completing, seeing errors regarding a 'configurator' module, and indeed on these occasions we noted some rather bizarre and unpredictable behaviour with little relation to the settings advertised in the interface.



The GUI itself is bright and colourful and seems fairly clearly laid out; it offers basic and advanced modes, with the latter most suitable for our requirements. It provided most of what we needed to get our work done fairly readily, and lumbered through the tests quite steadily. Some oddities were observed measuring the depth of archive scanning, when it seemed that enabling archive handling on access actually reduced the depth to which self-extracting zip files were scanned (while switching on most other types to a reasonable depth).

In the performance tests, CPU and RAM usage were not too extreme, and on-access lag times pretty light, while on-demand throughput was fairly average. In the infected sets however, several W32/Virut samples seemed to trip it up, causing the product to hang rather badly. We eventually managed to nurse it through the tests by removing samples

On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum	0	100.00%	115	97.76%	191	89.11%	1373	88.39%
AhnLab	0	100.00%	424	91.75%	8	99.59%	5713	51.70%
Alwil	0	100.00%	20	99.61%	507	93.28%	172	98.55%
Arcabit	1	99.86%	751	85.39%	1319	79.03%	5811	50.87%
Authentium	0	100.00%	193	96.25%	3	99.85%	2061	82.58%
Avanquest	-	-	-	-	-	-	-	-
AVG	0	100.00%	30	99.42%	26	98.79%	421	96.44%
Avira (Personal)	0	100.00%	15	99.71%	41	100.00%	169	98.57%
Avira (Professional)	0	100.00%	12	99.77%	0	100.00%	165	98.61%
BitDefender	0	100.00%	30	99.42%	0	100.00%	651	94.50%
Bkis (Gateway Scan)	3	99.58%	807	84.31%	2773	51.85%	6551	44.61%
Bkis (Home Edition)	18	97.50%	847	83.53%	2776	51.20%	6551	44.61%
Bullguard	0	100.00%	18	99.65%	0	100.00%	316	97.33%
CA (ISS)	0	100.00%	432	91.60%	958	92.06%	5184	56.17%
CA (Threat Manager)	0	100.00%	430	91.64%	958	92.06%	5063	57.19%
Central Command	0	100.00%	113	97.80%	191	89.11%	1319	88.85%
Check Point	1	99.9999%	99	98.07%	9	99.91%	858	92.75%
Defenx	0	100.00%	115	97.76%	191	89.11%	1373	88.39%
Digital Defender	0	100.00%	140	97.28%	191	89.11%	1421	87.99%
eEye Digital Security	123	99.99%	284	94.48%	338	81.83%	2960	74.97%
Emsisoft	-	-	-	-	-	-	-	-
eScan	0	100.00%	24	99.53%	0	100.00%	346	97.07%
ESET	0	100.00%	71	98.62%	0	100.00%	392	96.69%
Filseclab	2595	97.91%	295	94.26%	11413	37.25%	1718	85.48%
Fortinet	0	100.00%	330	93.58%	30	99.09%	3171	73.19%
Frisk	0	100.00%	192	96.27%	0	100.00%	2070	82.50%
F-Secure (Client Security)	0	100.00%	22	99.57%	0	100.00%	541	95.43%
F-Secure (PSB Workstation)	0	100.00%	22	99.57%	0	100.00%	541	95.43%
G DATA	0	100.00%	6	99.88%	0	100.00%	26	99.78%
Ikarus	973	99.95%	3	99.94%	1285	78.59%	142	98.80%
iolo	0	100.00%	186	96.38%	3	99.85%	1984	83.23%

(Please refer to text for full product names)

On-access tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
K7	0	100.00%	61	98.81%	0	100.00%	730	93.83%
Kaspersky (Anti-Virus 2010)	0	100.00%	79	98.46%	0	100.00%	376	96.82%
Kaspersky (Anti-Virus 6)	1	99.9999%	94	98.17%	1	99.999%	590	95.01%
Kingsoft (Advanced)	0	100.00%	1011	80.34%	2382	56.61%	10549	10.81%
Kingsoft (Standard)	0	100.00%	937	81.78%	2382	56.61%	9375	20.74%
Kingsoft (Swinstar)	-	-	-	-	-	-	-	-
Lavasoft	2	99.72%	25	99.51%	2004	65.03%	257	97.83%
McAfee Total Protection	0	100.00%	36	99.30%	0	100.00%	601	94.92%
McAfee VirusScan	0	100.00%	49	99.05%	1	99.999%	788	93.34%
Microsoft	1	99.9999%	64	98.76%	0	100.00%	764	93.54%
Nifty Corp.	1	99.9999%	56	98.91%	1	99.999%	348	97.06%
Norman	110	99.99%	285	94.46%	338	81.83%	2944	75.11%
PC Tools (Internet Security)	0	100.00%	27	99.47%	0	100.00%	271	97.71%
PC Tools (Spyware Doctor)	0	100.00%	27	99.47%	0	100.00%	260	97.80%
Preventon	0	100.00%	140	97.28%	191	89.11%	1421	87.99%
Proland	0	100.00%	112	97.82%	191	89.11%	1310	88.92%
Qihoo	0	100.00%	23	99.55%	42	99.79%	409	96.54%
Quick Heal	0	100.00%	351	93.17%	42	96.49%	5274	55.41%
Rising	0	100.00%	620	87.94%	1130	70.02%	8376	29.18%
SGA Corp.	0	100.00%	31	99.40%	0	100.00%	397	96.64%
Sophos	0	100.00%	23	99.55%	0	100.00%	392	96.69%
SPAMfighter (VIRUSfighter Plus)	0	100.00%	427	91.70%	191	89.11%	1384	88.30%
SPAMfighter (VIRUSfighter Pro)	0	100.00%	140	97.28%	191	89.11%	1421	87.99%
Sunbelt	-	-	-	-	-	-	-	-
Symantec (Endpoint Protection)	0	100.00%	26	99.49%	0	100.00%	309	97.39%
Symantec (Norton Antivirus)	0	100.00%	17	99.67%	0	100.00%	209	98.23%
Trustport	0	100.00%	6	99.88%	16	100.00%	34	99.71%
VirusBuster	0	100.00%	113	97.80%	191	89.11%	1319	88.85%
Webroot	0	100.00%	58	98.87%	0	100.00%	539	95.44%

(Please refer to text for full product names)

as they caused problems. An updated DLL file was provided by the developers to demonstrate that the product had been fixed, and this seemed to render it much more stable, so the issue seems to have been a temporary one that existed around the time of the product submission date. The scan of the large clean set proved problematic too, as it seemed to run for some time but then simply vanished as soon as there were no eyes on the screen, providing no evidence that it had completed. Eventually a full run through the set was managed using only the on-access component.

Detection rates recorded here may not be entirely accurate thanks to the numerous files which were moved aside to ensure the product made it to the ends of the various scans, but it achieved some reasonable figures. Given the large number of crashes and the need to remove several Virut samples it would have been difficult to justify granting a VB100 award, but there was no need to worry about whether to make any exceptions to our usual rules as it was observed that the product had missed a single file in the WildList set on access, thanks to an incomplete set of extensions being scanned. It also alerted incorrectly on several files in the clean sets. *ArcaVir* thus does not reach the required standard for a VB100 award this month.

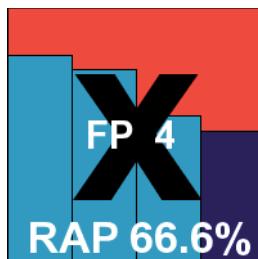
Authentium Command Anti-Malware 5.1.1

ItW	100.00%	Polymorphic	99.85%
ItW (o/a)	100.00%	Trojans	85.13%
Worms & bots	97.28%	False positives	4

Authentium's Command product comes as a minimalist 12MB installer executable. It is provided with a special manual updating scheme for our purposes, involving an additional 22MB cab file containing the definitions. Without this extra stage, the actual set-up is extremely fast and simple, with just a couple of steps including applying a licence key; no reboot is needed and the product is providing protection within a minute.

The interface is equally simple and unfussy, with a limited selection of options but providing some sensible defaults and a few useful extras. Navigation is very easy thanks to the lack of clutter, and responsiveness and stability seemed very solid throughout testing. Scanning speeds were fairly low, and on-access overheads a little on the high side, but RAM usage was much more impressive.

Detection rates were fairly decent across the infected sets, with a gradual decline across the RAP sets as expected. The

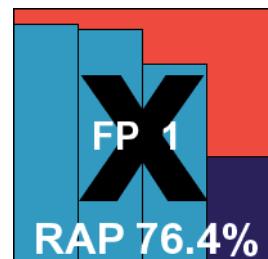


WildList was handled without problems, but in the clean sets a handful of items were alerted on, including a version of the *Adobe Reader 6* installer which the product labelled a rootkit. *Authentium* therefore does not qualify for a VB100 award this month.

Avanquest Double Anti-Spy Professional 1.4.4.4

ItW	100.00%	Polymorphic	65.32%
ItW (o/a)	N/A	Trojans	96.23%
Worms & bots	99.11%	False positives	1

The first of this month's bevy of newcomers is from *Avanquest*, a company whose name was familiar to me at least thanks to their highly active publicity department sending out frequent press releases on a wide range of products in many fields. The company's foray into anti-malware is named *Double Anti-Spy* and boasts a dual-engine approach using technology from *Sunbelt* and *Agnitum* as the twin prongs of its defensive fork. With this approach the installer is necessarily large – at 194MB without even the latest updates. The installation process is fast, slick and professional, with only online updates available. Application of an activation key and a reboot were included in the process.



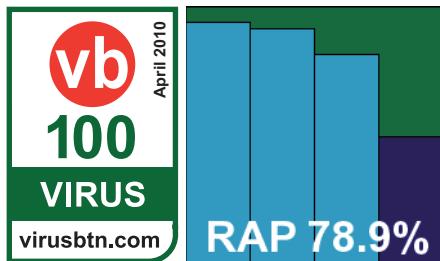
The interface is fairly simple, bulbous and colourful, with a fairly basic level of configuration – much of the layout is reminiscent of *Sunbelt* products. Running through the initial stages of the test seemed fairly straightforward, with the product operating properly and responding well to intervention. Both RAM and CPU usage were understandably heavy, and on-demand scans were long and slow, but file access lags were pretty light once the product had seen and recognized clean items.

When we got to the detection tests things got a little more tricky. Initial runs through the infected sets not only took a long time, thanks to the in-series approach of the twin engines, but were also prone to crashes, with error messages warning of services failing. Eventually, after much gentle nurturing, we managed to complete a full set of runs through the main test set, and an equally troublesome run through the RAP set showed some decent scores. On access, things were far worse, with crashes occurring repeatedly despite slowing down the file-accessing tools. After a cascade of crashes the system became barely responsive, but usually came back to life after a fairly aggressively

imposed reboot. In the end we recorded some good scores in the trojans set and nothing missed in the WildList. However, a single false alarm occurred in the clean sets, and with no on-access scores at all it was not possible to award Avanquest a VB100 for this performance.

AVG Internet Security Network Edition 9.0.733

ItW	100.00%	Polymorphic	98.79%
ItW (o/a)	100.00%	Trojans	97.60%
Worms & bots	99.67%	False positives	0



AVG's suite solution remains unchanged from several tests in the past year or so. With its many components the installer

comes in at a fairly sizeable 110MB, with all updates and an activation key included for us in the pre-prepared submission. The installation process runs through only a handful of steps, and completes in a couple of minutes with no need to reboot, but at the end it insists on an 'optimization' scan to check the machine and get itself settled in. This didn't take long though, and we were soon moving along nicely.

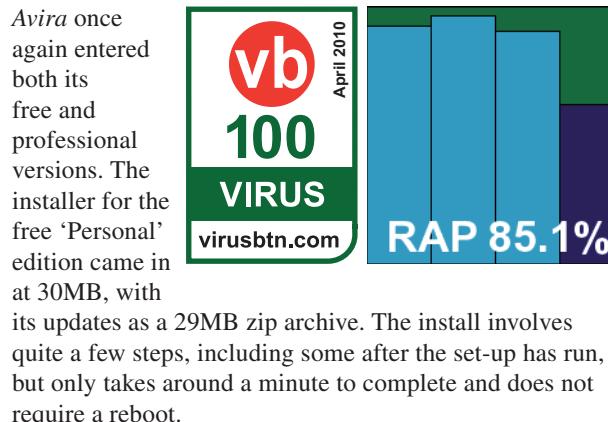
The GUI is a little cluttered with all the different suite components, many of which seem to overlap somewhat. However, we found the advanced configuration pleasingly clear with all the required options kept together in one place, which made for easy manipulation.

On-demand scanning speeds were pretty sluggish, and access lag times fairly hefty too, while memory and processor usage was high, but did not challenge the biggest drainers on the charts.

Detection rates were fairly decent across the test sets – a little behind the front-runners in the RAP table perhaps, but still highly commendable. No issues were encountered in the WildList or clean sets, stability was solid throughout, and AVG comfortably earns another VB100 award.

Avira AntiVir Personal 9.0.0.418

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.75%
Worms & bots	99.79%	False positives	0

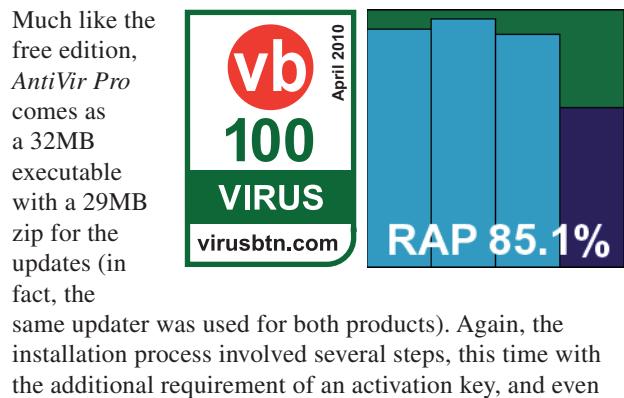


The interface is almost identical to the more familiar 'Pro' version. The fairly simple layout may be a little baffling at first for newcomers – particularly when setting up on-demand scans; it seems that only whole drives can be selected, so for our scans we used the right-click option to scan separate folders. One of the other differences between the free and pro editions is the response to on-access detections; the free edition has no option to simply block access by default, instead presenting a pop-up requiring a response. For our large on-access run through the infected test sets we resorted to leaving a heavy cup on the enter key and leaving the room for a while.

Scanning speeds were very good, and on-access lag times very low, while RAM and CPU impact was barely perceptible. In the final reckoning scores were as excellent as ever across the sets, with no issues in the WildList or clean sets, and Avira's free edition earns its second VB100 award in as many attempts.

Avira AntiVir Professional 9.0.0.738

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.75%
Worms & bots	99.79%	False positives	0



Reactive and Proactive (RAP) detection scores	Reactive			Reactive average	Proactive week +1	Overall average
	week -3	week -2	week -1			
Agnitum Outpost Security Suite Pro	87.61%	75.41%	70.84%	77.95%	47.75%	70.40%
AhnLab V3 Internet Security	68.25%	50.57%	36.40%	51.74%	21.65%	44.22%
Alwil avast! free antivirus	96.55%	94.69%	89.78%	93.67%	52.72%	83.44%
Arcabit ArcaVir 2010	67.58%	57.78%	57.51%	60.96%	23.43%	51.58%
Authentium Command Anti-Malware	81.41%	75.54%	57.85%	71.60%	51.55%	66.59%
Avanquest Double Anti-Spy Professional	93.63%	91.68%	78.21%	87.84%	42.19%	76.43%
AVG Internet Security Network Edition	93.55%	91.35%	81.26%	88.72%	49.28%	78.86%
Avira AntiVir Personal	92.28%	96.19%	90.32%	92.93%	61.59%	85.10%
Avira AntiVir Professional	92.28%	96.19%	90.32%	92.93%	61.59%	85.10%
BitDefender Antivirus 2010	89.03%	70.53%	63.31%	74.29%	51.85%	68.68%
Bkis Bkav Gateway Scan	47.93%	43.70%	32.05%	41.23%	21.96%	36.41%
Bkis Bkav Home Edition	47.93%	43.70%	32.05%	41.23%	21.96%	36.41%
Bullguard Antivirus	94.55%	86.08%	82.11%	87.58%	63.16%	81.47%
CA Internet Security Suite Plus	67.23%	59.42%	64.28%	63.65%	53.20%	61.04%
CA Threat Manager	68.69%	60.56%	65.78%	65.01%	55.35%	62.59%
Central Command Vexira Antivirus Professional	88.47%	77.32%	71.10%	78.96%	48.28%	71.29%
Check Point Zone Alarm Suite	94.45%	95.52%	92.35%	94.11%	78.15%	90.12%
Defenx Security Suite 2010	88.26%	77.26%	71.14%	78.89%	48.34%	71.25%
Digital Defender Antivirus	87.42%	76.03%	69.06%	77.50%	47.64%	70.04%
eEye Digital Security Blink Professional	66.47%	57.84%	50.75%	58.35%	45.70%	55.19%
Emsisoft a-squared Anti-Malware	99.13%	99.42%	97.62%	98.72%	71.30%	91.87%
eScan Internet Security for Windows	94.42%	85.75%	80.46%	86.88%	62.60%	80.81%
ESET NOD32 Antivirus	94.08%	94.11%	89.18%	92.46%	78.04%	88.85%
Filseclab Twister Anti-TrojanVirus	82.74%	76.74%	67.69%	75.72%	67.66%	73.71%
Fortinet FortiClient	72.87%	69.75%	64.54%	69.05%	23.15%	57.58%
Frisk F-PROT	79.34%	72.52%	56.15%	69.34%	49.92%	64.48%
F-Secure Client Security	91.22%	83.97%	66.53%	80.57%	55.26%	74.24%
F-Secure PSB Workstation Security	91.22%	83.97%	66.53%	80.57%	55.26%	74.24%
G DATA Antivirus 2010	99.09%	98.86%	91.14%	96.37%	65.25%	88.59%
Ikarus virus.utilities	98.93%	99.29%	94.64%	97.62%	68.42%	90.32%
iolo System Mechanic Professional	79.28%	72.47%	56.15%	69.30%	49.95%	64.46%

Reactive and Proactive (RAP) detection scores contd.	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1			
	week +1					
K7 Total Security	90.85%	85.44%	58.94%	78.41%	50.14%	71.34%
Kaspersky Anti-Virus 2010	93.55%	96.03%	93.23%	94.27%	77.36%	90.04%
Kaspersky Anti-Virus 6 for Windows Workstations	93.24%	95.79%	92.38%	93.80%	76.47%	89.47%
Kingsoft Internet Security 2010 Advanced Edition	32.16%	24.31%	21.93%	26.13%	17.61%	24.00%
Kingsoft Internet Security 2010 Standard Edition	37.64%	36.53%	26.45%	33.54%	21.88%	30.63%
Kingsoft Internet Security 2010 Swinstar Edition	42.62%	38.34%	28.81%	36.59%	22.34%	33.03%
Lavasoft Ad-Aware Professional Internet Security	96.96%	96.35%	82.57%	91.96%	62.12%	84.50%
McAfee Total Protection	94.64%	92.87%	84.84%	90.78%	66.01%	84.59%
McAfee VirusScan Enterprise	90.83%	89.17%	82.72%	87.57%	63.61%	81.58%
Microsoft Security Essentials	91.14%	93.06%	74.15%	86.12%	55.52%	78.47%
Nifty Corp. Security 24	93.45%	94.31%	85.59%	91.12%	62.36%	83.93%
Norman Security Suite	66.36%	57.81%	50.30%	58.16%	45.75%	55.06%
PC Tools Internet Security 2010	93.21%	92.55%	76.19%	87.32%	34.49%	74.11%
PC Tools Spyware Doctor	93.22%	92.58%	76.20%	87.34%	34.53%	74.13%
Preventon AntiVirus	87.42%	76.03%	69.06%	77.50%	47.64%	70.04%
Proland Protector Plus Professional	87.71%	76.26%	70.82%	78.26%	48.13%	70.73%
Qihoo 360 Security	93.88%	84.32%	73.68%	83.96%	56.51%	77.10%
Quick Heal AntiVirus 2010	78.68%	69.61%	63.17%	70.49%	44.58%	64.01%
Rising Internet Security 2010	59.40%	42.67%	34.77%	45.62%	25.07%	40.48%
SGA Corp. SGA-VC	94.36%	85.88%	79.65%	86.63%	62.08%	80.49%
Sophos Endpoint Security and Control	95.90%	93.43%	90.74%	93.36%	75.43%	88.88%
SPAMfighter VIRUSfighter Plus	87.43%	76.03%	69.06%	77.51%	47.59%	70.03%
SPAMfighter VIRUSfighter Pro	87.25%	75.84%	68.98%	77.36%	47.61%	69.92%
Sunbelt VIPRE AntiVirus Premium	96.97%	96.45%	83.53%	92.31%	66.10%	85.76%
Symantec Endpoint Protection	91.37%	90.35%	65.00%	82.24%	31.15%	69.47%
Symantec Norton Antivirus	91.77%	90.76%	66.49%	83.00%	33.24%	70.56%
Trustport Antivirus 2010	98.67%	96.09%	96.74%	97.17%	79.66%	92.79%
VirusBuster Professional	88.47%	77.32%	71.10%	78.96%	48.28%	71.29%
Webroot AntiVirus with SpySweeper	96.48%	94.12%	89.90%	93.50%	74.40%	88.72%

with some additional stages to respond to after the install proper. The whole process was complete within two minutes.

With the GUI closely resembling the free edition but providing a selection of small upgrades which made our task much easier (no heavy crockery required this time), we powered through the tests without incident. Once again performance was pretty splendid in every measurement, with only on-demand speeds not quite matching the very best on the tables.

Detection rates were, as expected, pretty identical to the free version; again no issues were observed in the core sets, and a second VB100 award goes to *Avira* in this test.

BitDefender Antivirus 2010 13.0.19

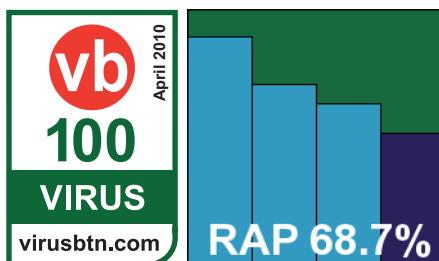
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	94.78%
Worms & bots	99.53%	False positives	0

BitDefender's 2010 product was provided as a 126MB executable with updates etc. rolled in, and required just three clicks of a button to install. With no reboot needed, everything was complete in under a minute.

The interface has an interesting approach, providing three different levels of layout and sophistication. On the first run it offers a choice of modes, from novice to expert, and each level seems to tweak both the default set-up (such as the number of prompts and questions presented to the user) and the configuration options to be found. We mainly stuck with the 'expert' mode, with everything clearly presented and a very good depth of configuration provided.

All the tests ran through smoothly with no stability problems, and in the performance tests scanning speeds seemed a little slower than the very best, but memory and processor usage were impressively low.

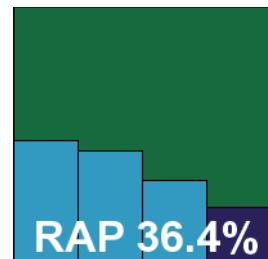
In the detection tests, decent scores were achieved across the board, and a solid level was obtained in the RAP sets. Alongside its interesting approach to GUI design and reliable, stable behaviour, clean runs through the clean and WildList sets earn *BitDefender* a VB100 award.



Bkis Bkav Gateway Scan 2759

ItW	99.58%	Polymorphic	51.85%
ItW (o/a)	99.58%	Trojans	44.61%
Worms & bots	84.31%	False positives	0

The second newcomer on this month's roster and one of the most interesting, *Bkis* hails from Vietnam, has been in business for over a decade, and is the only new entrant this month to use in-house technology alone. Two products were entered, with the 'Gateway Scan' edition coming in as a 210MB executable, with updates rolled in. Installation is a super-fast process, requiring only a couple of clicks and taking less than 30 seconds, although a reboot is needed at the end.



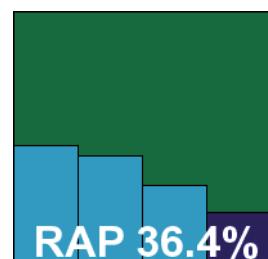
The interface is pared down and simple, but provides most of the required options in a simple fashion. It ran smoothly throughout, with no stability problems despite the heavy burden of our tests. Scanning speeds were somewhat on the slow side, with similarly hefty lag times on access, but memory drain was impressively low.

Detection rates were pleasingly high in the polymorphic and worms and bots sets, with a little work still to do to catch up with the leaders in the trojans and RAP sets. In the WildList, coverage was strong for a newcomer, but a small handful of items were missed. The clean sets were handled without problems though, and although no VB100 award can be granted this month, it looks likely that *Bkis* will qualify for certification very soon.

Bkis Bkav Home Edition 2759

ItW	97.50%	Polymorphic	51.20%
ItW (o/a)	97.50%	Trojans	44.61%
Worms & bots	83.53%	False positives	0

The home edition of *Bkav* is pretty similar to the gateway version – to the naked eye at least. The installer came in as a 205MB executable with all the updates thrown in, and again ran at a lightning pace, this time completing in just 20 seconds before requesting a reboot. Again the layout proved a pleasure to work with, and as with the gateway edition the product proved stable and reliable throughout.

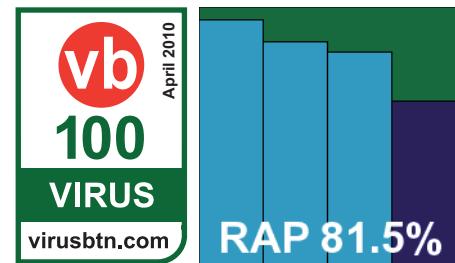


As with the other product, speeds were not amazing, but memory usage was even lower. Detection rates mirrored the gateway version fairly closely, with slightly lower scores in some sets, most likely thanks to less aggressive heuristics required by desktop users.

Again a handful of other items recently added to the WildList were missed, slightly more than the Gateway version, but with no false positive problems and a generally highly impressive product, *Bkis* shows great promise.

Bullguard Antivirus 9

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.33%
Worms & bots	99.65%	False positives	0



Bullguard is an old hand at the VB100 by now, with a solid record of entries and passes. The 82MB installer ran along swiftly, with

just a handful of steps for the user to work through and no reboot needed to get protection in place in under a minute. The installation process is enlivened by a rather odd-looking child in a boxing helmet reminding the user that the product is in trial mode.

The design of the *Bullguard* GUI is somewhat unusual, not to say eccentric, with some interesting use of language and some fairly non-standard extras, but it soon becomes clear how to operate things and is actually quite efficient. Default settings are very thorough, including full coverage of our archive sets by default in both modes.

With these thorough settings scanning speeds were slow and overheads were high, as might be expected, especially in the archives set. CPU and RAM usage was likewise fairly heavy.

Detection rates were slightly better than those of *BitDefender*, the supplier of the product's main detection engine, and were thus very solid indeed. No issues emerged in the clean or WildList sets, and *Bullguard* thus earns a VB100 award.

CA Internet Security Suite Plus 6.0.0.272

ItW	100.00%	Polymorphic	92.06%
ItW (o/a)	100.00%	Trojans	56.17%
Worms & bots	91.60%	False positives	0

It has become the norm for CA to submit both its consumer and business products for testing. The current home-user

suite was reviewed here in depth recently (see *VB*, March 2010, p.19). The product requires online activation, and was thus installed on the deadline date, allowed to connect for its activation and updates, and then cut off from the web until we were ready to start testing. An initial 144MB installation package was updated online, and the process was reasonably straightforward and speedy.

The interface, as discussed in our recent review, is quite unusual and provides minimal options, but seemed fairly responsive and ran stably throughout the test. Things moved along rapidly, helped by some intelligent caching of results which sped up the 'warm' times considerably, especially in the on-access runs where it is most likely to make a difference. Memory usage was fairly high, although CPU cycles were not overly drained.

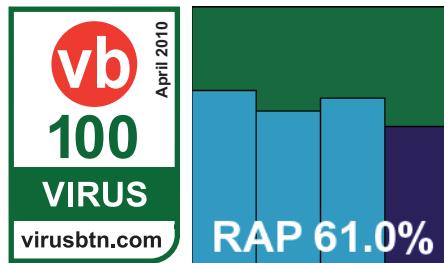
Detection rates were much improved on recent tests, with some solid scores in the RAP sets, and with no problems in the WildList or clean sets, the product earns itself another VB100 award.

CA Threat Manager 8.1.660.0

ItW	100.00%	Polymorphic	92.06%
ItW (o/a)	100.00%	Trojans	57.19%
Worms & bots	91.64%	False positives	0

CA's business offering is the now quite venerable *Threat Manager*, formerly known as *eTrust* and still bearing the

eTrust name in some places. Provided some time ago as an archive of the full CD contents, measuring some 390MB in total, the install process has several stages, including several EULAs which require scrolling through and a section gathering detailed data on the user. CA again requested the product be allowed to activate online, so the product was set



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	2.29	18.00	2.29	8.81	391.41	8.81	12.81	76.44	12.81	128.99	343.96	128.99
AhnLab	11.13	11.18	11.13	25.39	25.95	25.39	10.38	10.47	10.38	9.64	9.38	9.64
Alwil	213.25	277.23	7.57	40.49	49.44	37.58	29.03	30.99	29.78	43.00	43.00	24.00
Arcabit	7.02	6.98	7.02	14.86	14.68	14.86	24.14	26.36	24.14	14.95	15.40	14.95
Authentium	5.56	5.61	5.56	12.33	12.26	12.33	18.80	19.60	18.80	11.73	12.14	11.73
Avanquest	0.61	0.61	0.61	4.12	4.60	4.12	1.09	1.53	1.09	2.15	1.56	2.15
AVG	0.68	0.68	0.47	11.74	11.71	2.32	6.82	6.61	6.71	4.98	4.61	4.65
Avira (Personal)	4.34	4.27	4.34	33.55	33.55	33.55	19.43	18.20	19.43	9.64	15.40	9.64
Avira (Professional)	4.09	4.20	4.09	39.80	38.50	39.80	20.66	18.80	20.66	19.84	15.88	19.84
BitDefender	24.98	26.66	24.98	16.37	17.14	16.37	5.45	5.59	5.45	3.45	3.79	3.45
Bkis (Gateway Scan)	99.01	77.01	N/A	3.34	3.34	3.34	4.99	4.90	4.99	4.30	4.06	4.30
Bkis (Home Edition)	99.01	99.01	1.05	3.17	3.17	3.03	4.99	4.93	4.25	4.30	4.11	2.90
Bullguard	4.10	4.09	4.10	26.39	28.90	26.39	11.08	10.42	11.08	8.82	9.38	8.82
CA (ISS)	2.80	2.81	2.80	31.31	29.54	31.31	25.48	25.20	25.48	21.50	20.64	21.50
CA (Threat Manager)	1.27	1386.14	1.27	23.60	117.42	23.60	10.97	55.93	55.93	9.21	33.29	9.21
Central Command	7.81	7.90	2.39	20.69	20.78	20.51	17.50	16.50	12.40	13.76	12.90	10.53
Check Point	1.94	1.95	1.94	16.37	16.25	16.25	6.10	6.27	6.10	6.18	6.45	6.18
Defenx	1.12	14.99	1.12	15.01	391.41	15.01	6.23	22.48	6.23	4.76	51.59	4.76
Digital Defender	3.24	3.24	0.66	10.48	10.63	2.50	13.03	12.26	2.91	12.43	10.32	2.81
eEye Digital Security	1.49	1.50	1.49	1.80	1.77	1.80	0.80	0.80	0.80	0.59	0.58	0.58
Emsisoft	5.48	5.58	N/A	6.33	6.62	6.33	7.85	8.75	7.85	6.66	7.82	6.66
eScan	126.01	126.01	N/A	3.46	3.46	N/A	0.84	0.84	N/A	0.62	0.62	N/A
ESET	3.62	3.62	3.62	12.90	12.83	12.90	13.33	13.98	13.33	12.58	12.74	12.58
Filseclab	1.24	1.23	1.22	19.99	19.25	19.17	5.73	5.54	5.49	5.32	4.80	5.32
Fortinet	3.90	4.52	3.90	7.26	8.37	7.26	19.94	21.63	19.94	9.38	10.02	9.38
Frisk	7.30	7.33	7.30	11.10	11.32	11.10	26.66	31.41	26.66	18.76	19.47	18.76
F-Secure (Client Security)	6.68	2772.27	6.68	16.77	1565.63	60.22	10.28	114.66	29.40	49.14	343.96	27.15
F-Secure (PSB Workstation)	6.66	2772.27	6.66	361.30	2348.44	64.34	13.49	327.59	36.40	93.81	343.96	28.66
G DATA	2.52	2772.27	2.52	18.06	1174.22	18.06	10.42	229.31	10.42	8.97	343.96	8.97
Ikarus	23.69	23.69	N/A	11.32	11.32	11.32	13.18	12.13	13.18	14.95	10.86	14.95
iolo	6.58	6.60	N/A	11.32	11.24	N/A	14.89	12.07	N/A	8.53	12.43	N/A

(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
K7	7.24	7.30	7.24	9.66	9.74	9.66	29.78	29.03	29.78	20.23	19.11	20.23
Kaspersky (Anti-Virus 2010)	4.11	1386.14	4.11	30.70	391.41	30.70	16.38	48.79	16.38	11.86	79.38	11.86
Kaspersky (Anti-Virus 6)	4.68	1386.14	4.68	37.28	587.11	37.28	11.47	69.49	11.47	13.23	147.41	13.23
Kingsoft (Advanced)	1.55	1.55	1.55	24.46	25.67	24.46	5.49	5.28	5.49	22.93	14.74	22.93
Kingsoft (Standard)	1.52	1.53	1.52	23.02	23.14	23.02	5.32	5.24	5.32	16.64	12.74	16.64
Kingsoft (Swinstar)	5.25	5.21	N/A	37.28	40.14	N/A	32.76	30.17	N/A	25.17	24.57	N/A
Lavasoft	63.01	72.95	N/A	12.17	12.30	12.17	2.46	2.57	2.46	3.50	3.34	3.50
McAfee Total Protection	1.66	2.03	1.66	9.87	50.50	9.87	5.15	15.81	5.15	8.32	36.85	8.32
McAfee VirusScan	86.63	89.43	1.97	13.05	13.08	11.98	7.62	7.10	7.62	6.11	4.37	4.30
Microsoft	2.61	2.52	2.61	13.31	13.27	13.31	19.60	19.60	19.60	10.12	12.14	10.12
Nifty Corp.	2.38	924.09	2.38	17.33	195.70	17.33	6.48	34.23	6.48	6.25	26.46	6.25
Norman	1.12	1.13	1.12	2.47	2.47	2.47	2.33	3.45	2.33	1.59	2.45	1.59
PC Tools (Internet Security)	1.42	1.47	0.51	6.02	25.39	6.02	6.35	6.20	6.35	5.37	5.29	5.37
PC Tools (Spyware Doctor)	2.13	2.22	0.69	31.74	23.48	31.74	8.19	8.25	8.19	7.82	7.48	7.82
Preventon	3.23	3.22	N/A	10.04	10.06	10.04	13.03	12.20	13.03	12.28	10.22	12.28
Proland	7.05	7.04	7.05	19.73	20.16	19.73	7.77	7.67	7.77	5.93	5.49	5.93
Qihoo	1.52	1.52	1.52	5.21	4.99	5.21	1.15	1.03	1.15	0.75	0.84	0.75
Quick Heal	3.57	3.58	2.58	38.50	37.58	38.50	9.93	9.72	9.40	3.75	9.92	8.74
Rising	1.43	1.45	1.43	6.97	7.07	6.97	3.49	3.51	3.49	5.76	5.86	5.76
SGA Corp.	2772.27	2772.27	N/A	24.85	27.15	N/A	15.60	17.24	N/A	85.99	515.94	N/A
Sophos	252.02	277.23	2.48	15.55	15.71	14.45	21.43	23.16	17.11	12.43	11.47	9.05
SPAMfighter (VIRUSfighter Plus)	3.11	3.07	3.11	8.68	9.68	8.68	10.42	9.28	10.42	11.59	6.88	6.88
SPAMfighter (VIRUSfighter Pro)	56.58	53.31	56.58	10.12	10.12	10.12	16.62	17.11	16.62	10.32	10.32	10.32
Sunbelt	102.68	102.68	2.21	13.77	13.73	13.50	2.40	2.39	2.39	3.39	3.12	3.10
Symantec (Endpoint Protection)	2.35	2.24	2.35	14.41	15.71	14.41	8.79	8.92	8.79	6.11	6.22	6.11
Symantec (Norton Antivirus)	4.93	693.07	693.07	29.17	260.94	29.17	13.57	55.93	55.93	13.58	43.00	13.58
Trustport	1.25	1.27	1.25	7.03	7.40	7.03	5.10	4.87	5.10	3.30	3.36	3.30
VirusBuster	7.72	7.77	7.74	20.16	20.25	20.16	15.92	15.29	11.52	79.38	206.38	79.38
Webroot	2.56	2.53	2.56	11.65	11.65	11.65	10.38	9.10	10.38	8.53	5.73	8.53

(Please refer to text for full product names)

up in advance and an image taken on the deadline date after allowing a final update.

The interface is somewhat old-fashioned these days, and in places a little fiddly to use but thanks to our familiarity with its quirks we got through things without any problems. Logging is somewhat tricky, with any large logs overwhelming the viewer system, but deciphering the file format has become second nature after many years and requires just a few judicious sed commands to strip out the oddness and render it into readable text.

Performance measures were similar to the consumer product, with high RAM usage tempered by low CPU impact, while scanning speeds were improved in the warm runs, although not as significantly as in the home-user solution.

Detection figures were also similar to those of the consumer product, with the clean and WildList sets handled immaculately, thus earning *CA* its second VB100 award this month.

Central Command Vexira Antivirus Professional 6.2.54

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	89.61%
Worms & bots	97.88%	False positives	0

A new one to this lab team, but not quite to the VB100, *Vexira* last appeared in these pages in June 2006 (see *VB*, June 2006, p.11).

On its return to the test bench, the impossibly named *Central Command* provided its latest product as a 55MB executable with a hefty 118MB update archive, which was added manually in a nice simple way. Running the install required clicking through quite a few steps, but the process ran swiftly, needed no reboot, and was all done in under two minutes.

The interface was immediately familiar when it appeared, being essentially the *VirusBuster* GUI in a different colour scheme. This inspired confidence straight away, and after wrestling briefly with the slightly fiddly layout we soon had things running smoothly.

Things moved very nicely indeed through the speed tests, with some decent on-demand speeds and some feather-light

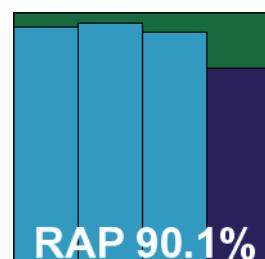
lag times; similarly light were CPU and RAM usage figures, which barely registered on the scales.

In the final reckoning we observed some pretty good scores all round, with the RAP sets particularly impressive, and with no problems in the clean sets and complete coverage of the WildList, *Vexira* earns itself its first VB100 award, and our congratulations.

Check Point Zone Alarm Suite 9.1.008.000

ItW	99.99%	Polymorphic	99.91%
ItW (o/a)	99.99%	Trojans	96.80%
Worms & bots	98.91%	False positives	0

Check Point seems to have adopted a strategy of entering its *Zone Alarm* product to our test on an annual basis – which has paid off, with two passes in the last two *XP* tests.

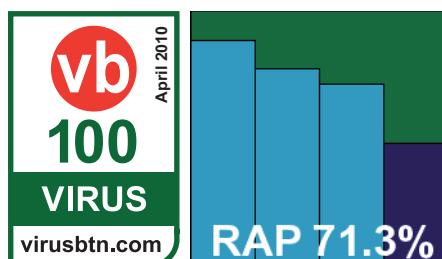


This time, the suite product was initially thought to need online access to update until a workaround was figured out, and a main product of 120MB was updated with a full set of the latest updates, measuring over 90MB, without problems. The installation process was reasonably simple and quick, with a very fast ‘pre-scan’ and the offer of a ‘browser security’ toolbar included, but did require a reboot to complete.

The interface seemed pretty unchanged from previous entries and perhaps a little old-fashioned, but remained pleasingly simple and clear to operate and offered plenty of configuration options for the more experienced and demanding user. It ran very smoothly and stably throughout the testing and seemed solid and well built.

In the performance tests, neither scanning throughput nor lag times were especially impressive, but drain on processor cycles and memory was not overly substantial, making for a good overall balance.

Detection rates were as excellent as we have come to expect from the *Kaspersky* engine that is included in the product, with especially good scores in the later RAP sets. In the clean sets a few alerts were raised, but as these identified mIRC as an IRC client and RealVNC as a remote access tool, they were pretty accurate and could not be mistaken for false alarms. In the WildList set, all looked pretty clear until it was noted that a single sample of W32/Virut had not been detected, spoiling *Check Point*’s chances of a VB100 award this month and boding ill for several other products based on the same engine.



Defenx Security Suite 2010 3062.452.0727

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	89.42%
Worms & bots	97.88%	False positives	0

Another newcomer, Swiss-based *Defenx* contacted us shortly before the test deadline and was quickly included on the

roster. The product was provided with updates included as an 85MB executable, and ran through a number of set-up stages mainly referring to firewall options, some community participation and training mode settings, with a reboot to finish off and the whole process taking about four minutes. The product itself was recognizable from the moment the GUI appeared, being essentially *Agnitum's Outpost* with a different colour scheme.

This made set-up and use pretty straightforward thanks to our experience with *Outpost*, and the test ran through rapidly and without any problems. On-demand speeds were excellent after initial familiarization with the sets, and on-access lags likewise improved greatly after the first run. RAM usage was a trifle on the high side.

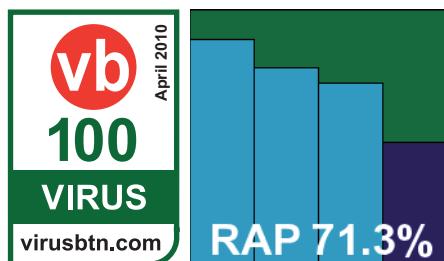
Detection rates were solid, with a generally good showing all around, and with no problems in either the clean or WildList sets, *Defenx* ably earns a VB100 award on its first attempt.

Digital Defender Antivirus 1.1.67

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	88.69%
Worms & bots	97.37%	False positives	0

Yet another newcomer, and another based on the ubiquitous *VirusBuster* engine. *Digital Defender* is a technology partner with

Prevention, which took part in the *Windows 7* test a few months ago (see *VB*, December 2009, p.16), and the



products are pretty similar. *Digital Defender* came as a 47MB installer with updates included, had the standard handful of steps to the set-up and was complete in 30 seconds, with no need for a reboot.

The interface is simple and clear, but manages to provide most of the configuration required by all but the most demanding of users. It ran through the tests quickly and stability was solid throughout. On-demand scans were not super fast, but overheads – especially memory use – were low in the extreme, barely registering any impact on the system at all.

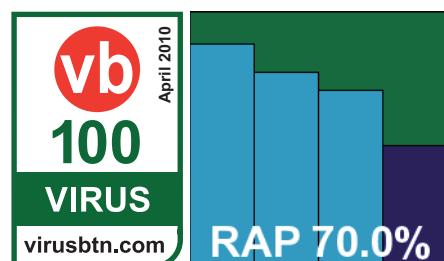
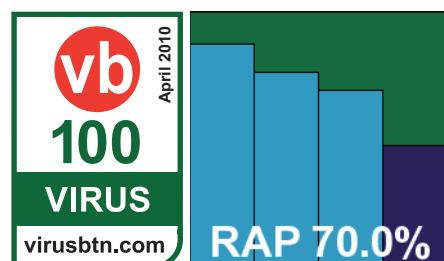
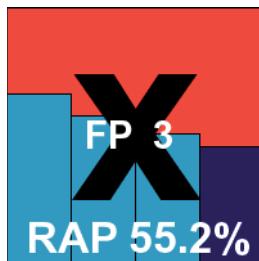
Detection rates were pretty decent, with a steady decline across the RAP sets, but this is only to be expected and the clean and WildList sets were handled without difficulty. With no serious problems and much to commend, *Digital Defender* also joins the ranks of the newly VB100 certified this month.

eEye Digital Security Blink Professional 4.6.0

ItW	99.99%	Polymorphic	83.47%
ItW (o/a)	99.99%	Trojans	76.63%
Worms & bots	94.52%	False positives	3

Blink is another fairly regular participant in our comparatives on desktop platforms, and has become quite familiar as a solid and interesting product. The product as provided was a fair size, with a 114MB main installer and an additional 49MB of updates, to cover the numerous component parts included (of which anti-malware protection is just one). The install process has a fair number of steps, thanks again to the multiple components and the need for an activation key, but doesn't need a reboot to complete and is all done in about three minutes. The interface is fairly clear and simple to navigate, but on-access protection appears not to take effect on-read, and instead tests were run by writing sample files to the system.

Tests proceeded without major incident, although they took some time as on-demand scans were slow, even over the clean set – this is mainly due to the use of the *Norman Sandbox* to thoroughly check unrecognized files. On-access measures look extremely light, but as there was no true on-read protection in place this is an unfair comparison with others in the test; increase in memory usage was still fairly noticeable.



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	0.01	0.00	0.00	0.10	0.00	0.00	0.16	0.04	0.04	0.19	0.04	0.04
AhnLab	0.02	0.02	NA	0.04	0.03	0.04	0.09	0.08	0.09	0.09	0.09	0.09
Alwil	0.03	0.00	0.15	0.04	0.00	0.05	0.11	0.00	0.22	0.19	0.00	0.33
Arcabit	0.00	0.00	0.14	0.05	0.05	0.05	0.03	0.03	0.03	0.02	0.02	0.05
Authentium	0.04	0.04	0.07	0.12	0.10	0.08	0.19	0.17	0.05	0.22	0.22	0.08
Avanquest	0.01	0.00	NA	0.07	0.01	NA	0.36	0.05	NA	0.27	0.07	NA
AVG	0.00	0.00	0.02	0.08	0.07	0.07	0.12	0.11	0.12	0.17	0.16	0.19
Avira (Personal)	0.01	0.00	0.05	0.03	0.00	0.03	0.05	0.03	0.05	0.06	0.05	0.06
Avira (Professional)	0.01	0.00	0.04	0.02	0.00	0.03	0.05	0.04	0.06	0.06	0.06	0.06
BitDefender	0.01	0.00	0.45	0.04	0.00	0.04	0.14	0.01	0.14	0.18	0.01	0.18
Bkis (Gateway Scan)	0.01	0.01	NA	0.23	0.22	0.23	0.12	0.12	0.12	0.17	0.16	0.17
Bkis (Home Edition)	0.01	0.01	NA	0.23	0.23	0.23	0.12	0.13	0.12	0.17	0.17	0.17
Bullguard	0.25	0.25	0.25	0.05	0.04	0.05	0.14	0.14	0.14	0.18	0.18	0.18
CA (ISS)	0.01	0.01	0.15	0.03	0.02	0.05	0.04	0.03	0.22	0.04	0.03	0.33
CA (Threat Manager)	0.01	0.01	NA	0.03	0.03	0.03	0.09	0.08	0.09	0.06	0.05	0.06
Central Command	0.00	0.00	NA	0.04	0.04	0.04	0.02	0.02	0.04	0.08	0.09	0.10
Check Point	0.01	0.01	NA	0.04	0.02	0.04	0.12	0.11	0.12	0.12	0.12	0.12
Defenx	0.01	0.00	NA	0.06	0.00	0.06	0.13	0.02	0.13	0.20	0.02	0.20
Digital Defender	0.00	0.01	0.09	0.09	0.09	0.09	0.01	0.01	0.05	0.02	0.01	0.09
eEye Digital Security	0.00	0.00	NA	0.00	0.00	0.00	0.01	0.01	0.01	0.01	0.01	0.01
Emsisoft	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
eScan	0.00	0.00	0.17	0.05	0.01	0.01	0.06	0.00	0.02	0.04	0.00	0.06
ESET	0.00	0.00	NA	0.01	0.01	0.01	0.07	0.07	0.07	0.05	0.05	0.05
Filseclab	0.00	0.01	NA	0.02	0.02	0.02	0.11	0.11	0.11	0.01	0.01	0.01
Fortinet	0.20	0.00	0.20	0.13	0.01	0.13	0.07	0.00	0.07	0.14	0.01	0.14
Frisk	0.01	0.01	NA	0.08	0.08	0.08	0.02	0.02	0.02	0.03	0.03	0.03
F-Secure (Client Security)	0.01	0.01	NA	0.07	0.00	NA	0.15	0.03	NA	0.06	0.03	NA
F-Secure (PSB Workstation)	0.01	0.01	NA	0.07	0.00	NA	0.12	0.00	NA	0.03	0.01	NA
G DATA	0.08	0.00	0.54	0.07	0.00	0.08	0.18	0.02	0.18	0.24	0.02	0.24
Ikarus	0.04	0.04	NA	0.08	0.08	0.08	0.06	0.06	0.06	0.07	0.07	0.07
iolo	0.04	0.04	NA	0.10	0.10	NA	0.16	0.15	NA	0.18	0.17	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
K7	0.02	0.00	NA	0.09	0.00	0.09	0.03	0.01	0.03	0.05	0.01	0.05
Kaspersky (Anti-Virus 2010)	0.01	0.01	0.03	0.05	0.00	0.05	0.13	0.04	0.13	0.14	0.04	0.15
Kaspersky (Anti-Virus 6)	0.01	0.00	0.39	0.05	0.00	0.04	0.13	0.04	0.14	0.14	0.04	0.15
Kingsoft (Advanced)	0.00	0.00	NA	0.03	0.00	0.03	0.18	0.00	0.18	0.05	0.00	0.05
Kingsoft (Standard)	0.00	0.00	NA	0.03	0.00	0.03	0.18	0.00	0.18	0.05	0.00	0.05
Kingsoft (Swinstar)	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Lavasoft	0.00	0.00	NA	0.07	0.02	NA	0.01	0.00	NA	0.30	0.07	NA
McAfee Total Protection	0.01	0.00	NA	0.08	0.01	0.08	0.13	0.00	0.13	0.21	0.01	0.21
McAfee VirusScan	0.01	0.01	0.44	0.08	0.04	0.07	0.16	0.08	0.15	0.24	0.13	0.23
Microsoft	0.01	0.00	NA	0.07	0.00	0.07	0.05	0.00	0.05	0.08	0.00	0.08
Nifty Corp.	0.01	0.00	NA	0.05	0.01	0.05	0.13	0.02	0.13	0.14	0.02	0.14
Norman	0.01	0.01	NA	0.09	0.09	0.09	0.29	0.28	0.29	0.34	0.34	0.34
PC Tools (Internet Security)	0.01	0.00	NA	0.15	0.01	NA	0.03	0.02	NA	0.03	0.02	NA
PC Tools (Spyware Doctor)	0.01	0.00	NA	0.12	0.04	NA	0.19	0.20	NA	0.25	0.23	NA
Preventon	0.00	0.00	NA	0.09	0.09	0.09	0.01	0.00	0.05	0.02	0.01	0.09
Proland	0.00	0.00	NA	0.04	0.01	0.04	0.02	0.01	0.05	0.00	0.00	0.12
Qihoo	0.00	0.01	NA	0.01	0.00	0.00	0.04	0.03	0.04	0.04	0.03	0.04
Quick Heal	0.04	0.04	NA	0.02	0.02	0.02	0.10	0.09	0.10	0.10	0.10	0.10
Rising	0.02	0.02	NA	0.14	0.13	0.14	0.18	0.17	0.18	0.15	0.19	0.15
SGA Corp.	0.00	0.00	NA	0.04	0.00	NA	0.12	0.01	NA	0.02	0.02	NA
Sophos	0.00	0.00	0.34	0.06	0.06	0.06	0.04	0.03	0.04	0.08	0.08	0.09
SPAMfighter (VIRUSfighter Plus)	0.01	0.01	NA	0.10	0.10	0.10	0.03	0.03	0.08	0.06	0.06	0.13
SPAMfighter (VIRUSfighter Pro)	0.00	0.00	NA	0.09	0.09	0.09	0.01	0.00	0.01	0.02	0.01	0.02
Sunbelt	0.01	0.00	NA	0.06	0.01	0.06	0.38	0.04	0.38	0.27	0.05	0.27
Symantec (Endpoint Protection)	0.01	0.01	NA	0.06	0.06	0.06	0.09	0.08	0.09	0.11	0.10	0.11
Symantec (Norton Antivirus)	0.01	0.01	NA	0.05	0.06	0.05	0.08	0.08	0.08	0.09	0.08	0.09
Trustport	0.04	0.01	1.35	0.20	0.02	0.22	0.30	0.09	0.32	0.44	0.06	0.47
VirusBuster	0.00	0.00	NA	0.04	0.04	0.04	0.03	0.02	0.04	0.09	0.09	0.10
Webroot	0.01	0.01	NA	0.09	0.08	0.09	0.08	0.08	0.08	0.17	0.14	0.17

(Please refer to text for full product names)

Detection rates were generally pretty decent, but in the WildList set imperfect coverage of the latest W32/Virut strain was evident, with the sandbox improving things somewhat on-demand. In the clean sets there were also a handful of samples misidentified as malware, and so *Blink* is denied a VB100 award this month.

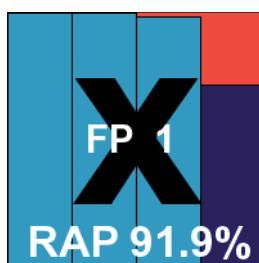
Emsisoft a-squared Anti-Malware 5.0.0.31

ItW	99.95%	Polymorphic	78.59%
ItW (o/a)	N/A	Trojans	98.29%
Worms & bots	99.81%	False positives	1

Yet another new arrival, and one which has been anticipated for some time thanks to an excellent reputation for high detection rates, *Emsisoft's a-squared* incorporates the *Ikarus* engine along with some improvements of its own. The installer package is a 75MB executable, and online updating was insisted on by the vendor. The install process took only a few moments, but it took a while longer to get things up and running thanks to the online activation and updating process.

Once installed, we found the product very attractive, with a crisp and colourful GUI adorned with a delightful rotating golden Trojan horse. There appeared to be a decent range of configuration options provided, in a pleasant and accessible manner. On investigating further, however, we found that the on-access component was unresponsive to various stimuli; this remained the case despite various efforts – restarting the module and the test systems, installing afresh and so on. The version of the product in use, with full on-read protection included, is at an early stage of beta, so such problems are to be expected, but we were disappointed not to be able to test the product fully. A quick investigation of more recent releases – produced a week or two after the test deadline – showed that the issues had been resolved and a much more rugged, stable on-access component was being provided even to beta users.

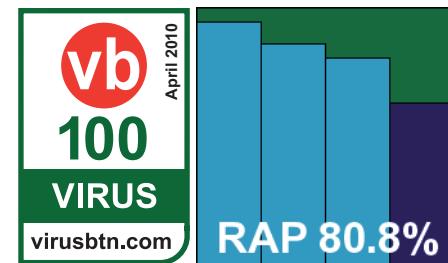
Without the on-access component there seemed to be little point running the full range of performance tests, but the on-demand scan times were fairly middle-of-the-road. Running through the detection tests, we had some further issues as the product seems to maintain all detection data in memory until a scan is complete, rather than writing out to a log as it goes, so on attempting large scans with lots of data to store it had a tendency to collapse under



the pressure. Fortunately, a command-line scanner is also provided, and this proved much more stable. With some data finally in, some truly superb results were observed, with all sets completely demolished, the RAPs especially looking set for a top-of-the-table score. Sadly, in the WildList set a batch of Virut samples were not detected – which would have been enough to deny *Emsisoft* a VB100 award even had its on-access component been fully operational – and a single false alert in the clean sets also denies it the chance to take up a prime position on our aggregate RAP charts. Despite these teething problems, we expect to see *a-squared* becoming a force to be reckoned with in the near future.

eScan Internet Security for Windows 10.0.1058.653

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.29%
Worms & bots	99.65%	False positives	0



From a newcomer to one of our most regular entrants; *eScan* has been a fixture in our comparatives for many years, and has gone from strength to strength in recent tests. The latest version comes as a fairly large 112MB executable, with a rather long and drawn-out installation process involving numerous prompts and dialogs.

The GUI is very nicely designed and unfussy, providing a decent level of configuration, although some options are notable by their absence – such as the choice to scan inside archive files to a greater level than the rather scanty defaults. At times the product was rather slow to respond to clicks, especially when accessing on-demand scan browse windows, and some of the on-demand speed scans took rather a while to get through. File access lag times were not insanely heavy though, and memory usage remained fairly low until serious activity was demanded of the product.

In the detection test, however, scores were exemplary, with excellent rates in most sets and a reliably high level across the reactive part of the RAP sets. With nothing missed in the WildList and nothing of note in the clean sets other than a few warnings of corrupted files, *eScan* comfortably wins yet another VB100 award.

Archive scanning		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Agnitum Outpost Security Suite Pro	OD	2	√	√	√	√	√	√	√	√
	OA	X	X/N	X/N	X/N	X	X/N	X	X/N	√
AhnLab V3 Internet Security	OD	X	√	X	X	√	√	X	√	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast! free antivirus	OD	X/N	X/N	√	X/N	X/N	X/N	X/N	X/N	X/N
	OA	X/N	X/N	√	X/N	X/N	X/N	X/N	X/N	√
Arcabit ArcaVir 2010	OD	2	√	√	√	√	√	√	√	√
	OA	X/2	X/5	√/5	X/5	X/5	X/5	X/5	X/5	√
Authentium Command Anti-Malware	OD	5	5	5	5	√	5	2	5	√
	OA	X/4	X/4	X/4	X/4	X/N	X/4	X/2	X/4	X/N
Avanquest Double Anti-Spy Professional	OD	X	X	√	√	X	√	X	√	√
	OA	X	X	√	X	X	X	X	X	X
AVG Internet Security Network Edition	OD	√	√	√	√	√	√	√	√	X/N
	OA	X	X	X	X	X	X	X	X	X/N
Avira AntiVir Personal	OD	√	√	√	√	√	√	√	√	√
	OA	X	X/N	X/N	X/N	X/N	X/N	X/N	X/N	√
Avira AntiVir Professional	OD	√	√	√	√	√	√	√	√	√
	OA	X	X/N	X/N	X/N	X/N	X/N	X/N	X/N	√
BitDefender Antivirus 2010	OD	√	√	8	√	√	√	8	√	√
	OA	X/N	X/N	X/N	2/N	X/N	X/N	X/N	1/N	√
Bkis Bkav Gateway Scan	OD	X	X	X/1	X/1	X	X/1	X	X/1	√
	OA	X	X	X	X	X	X	X	X	√
Bkis Bkav Home Edition	OD	X	X	X/1	X/1	X	X/1	X	X/1	√
	OA	X	X	X	X	X	X	X	X	√
Bullguard Antivirus	OD	√	√	8	√	√	√	8	√	√
	OA	√	√	√	√	√	√	√	√	√
CA Internet Security Suite Plus	OD	X	9	9	X	9	9	9	X	√
	OA	X	X	X	1	X	X	X	1	√
CA Threat Manager	OD	X	√	X	√	√	√	√	√	√
	OA	X	X	X	1	X	X	X	1	√
Central Command Vexira Antivirus Professional	OD	2	√	√	X/N	X	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X/N
Check Point Zone Alarm Suite	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Defenx Security Suite 2010	OD	2	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Digital Defender Antivirus	OD	1	1	1	1	X	1	X	1	√
	OA	1	1	X	X	X	1	X	1	X/N
eEye Digital Security Blink Professional	OD	X	4/N	1	4/N	4/N	4/N	2/N	4/N	√
	OA	X	X	X	X	X	X	X	X	√

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.

Archive scanning contd.		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Emsisoft a-squared Anti-Malware	OD	2	2	2	2	2	1	2	✓	
	OA	-	-	-	-	-	-	-	-	-
eScan Internet Security for Windows	OD	X	X	8	X	✓	X	X	X	✓
	OA	X/1	X/✓	X	X/✓	X	X/✓	X/1	X/✓	✓
ESET NOD32 Antivirus	OD	✓	✓	✓	✓	✓	✓	5	✓	✓
	OA	X	X	X	X	X	X	X	X	✓
Filseclab Twister Anti-TrojanVirus	OD	5/✓	3/✓	3/✓	4/✓	1	4/✓	X	5/✓	✓
	OA	X	X	X	X	X	1	X	2	X
Fortinet FortiClient	OD	X	✓	✓	✓	✓	✓	✓	4	✓
	OA	X	9	✓	✓	✓	✓	✓	4	✓
Frisk F-PROT	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X	X	2	2	X	X	X	2	✓
F-Secure Client Security	OD	X/✓	✓	✓	✓	✓	✓	8	✓	X/✓
	OA	X	X	X	X	X	X	X	X	X
F-Secure PSB Workstation Security	OD	X/✓	✓	✓	✓	✓	✓	8	✓	X/✓
	OA	X	X	X	X	X	X	X	X	X
GDATA Antivirus 2010	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	✓	✓	4/✓	✓	✓	✓	8/✓	8/✓	✓
Ikarus virus.utilities	OD	2	2	2	2	2	2	3	2	✓
	OA	2	2	2	2	2	2	3	2	✓
iolo System Mechanic Professional	OD	X	X	5	X	X	X	X	5	X
	OA	X	X	5	X	X	X	X	5	X
K7 Total Security	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	1	X	1	1	X	X	X	1	X
Kaspersky Anti-Virus 2010	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X/4	X/4	1	X/4	X/4	X/5	X/1	X/2	✓
Kaspersky Anti-Virus 6 for Windows Workstations	OD	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X/✓	X/✓	X/✓	X/✓	X/✓	X/✓	X/✓	X/✓	✓
Kingsoft Internet Security 2010 Advanced Edition	OD	X	✓	X	✓	✓	✓	✓	✓	✓
	OA	X	X	X	X	X	X	X	X	✓
Kingsoft Internet Security 2010 Standard Edition	OD	X	✓	X	✓	✓	✓	✓	✓	✓
	OA	X	X	X	X	X	X	X	X	✓
Kingsoft Internet Security 2010 Swinstar Edition	OD	-	-	-	-	-	-	-	-	-
	OA	-	-	-	-	-	-	-	-	-
Lavasoft Ad-Aware Professional Internet Security	OD	X	X	✓	X	X	1	X	1	✓
	OA	X	X	✓	X	X	X	X	X	X
McAfee Total Protection	OD	2	✓	✓	✓	✓	✓	✓	✓	✓
	OA	X	X	X	X	X	X	X	X	✓
McAfee VirusScan Enterprise	OD	X/2	X/✓	X/✓	X/✓	X/✓	X/✓	X/✓	X/✓	✓
	OA	X/2	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.

Archive scanning contd.		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Microsoft Security Essentials	OD	√	√	√	2	2	2	√	√	√
	OA	X	X	1	X	X	X	X	1	√
Nifty Corp. Security 24	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	X	X	√
Norman Security Suite	OD	X	√	1	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
PC Tools Internet Security 2010	OD	2	√	√	√	X	√	√	√	√
	OA	X	X	√	X	X	X	X	X	X
PC Tools Spyware Doctor	OD	2	√	√	√	X	√	√	√	√
	OA	X	X	√	X	X	X	X	X	X
Preventon Antivirus	OD	1	1	1	1	X	1	X	1	√
	OA	1	1	X	X	X	1	X	1	X/√
Proland Protector Plus Professional	OD	2	√	√	√	X	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X/√
Qihoo 360 Security	OD	√	√	8	√	√	√	8	√	√
	OA	X	X	X	X	X	X	X	X	X/√
Quick Heal AntiVirus 2010	OD	X/2	X/5	X	2/5	X	2/5	X/1	2/5	X/√
	OA	2	X	X	1	X	X	X	1	X/√
Rising Internet Security 2010	OD	X	X	√	√	√	√	√	√	√
	OA	X	X	√	X	X	X	X	X	√
SGA Corp. SGA-VC	OD	X	X	X	X	X	X	X	X	X
	OA	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/√
	OA	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
SPAMfighter VIRUSfighter Plus	OD	1	1	1	1	X	1	X	1	√
	OA	X/1	X/1	X	X	X	X/1	X	X/1	X/√
SPAMfighter VIRUSfighter Pro	OD	X	4	4	4	X	4	√	5	√
	OA	X	X	2	X	X	X	X	X	X
Sunbelt VIPRE AntiVirus Premium	OD	X	X	√	X/√	X	X/√	X	X/√	√
	OA	X	X	X	X	X	X	X	X	√
Symantec Endpoint Protection	OD	3/√	3/√	3/√	3/√	3/√	3/√	1/5	3/√	√
	OA	X	X	X	X	X	X	X	X	√
Symantec Norton Antivirus	OD	√	√	√	√	√	√	5	√	√
	OA	X	X	X	X	X	X	X	X	√
Trustport Antivirus 2010	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	√
VirusBuster Professional	OD	2	√	√	X/√	X	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot AntiVirus with SpySweeper	OD	X	√	5	5	√	√	5	√	√
	OA	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.

ESET NOD32 Antivirus 4.2.35.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.55%
Worms & bots	99.55%	False positives	0

ESET is another VB100 stalwart, with an unrivalled record of clean sheets. The product is provided as a pre-updated executable of just 37MB, and the installation process remains pretty much unchanged from many previous experiences. With just a handful of stages to get through, including the unusual step of forcing the user to make a choice on whether to detect 'potentially unwanted' software or not (presumably allowing the product greater freedom to detect certain types of nasty without threat of reprisals), the process is all done within under a minute and a half, with no need to reboot.

The interface and configuration screens are as solid, slick and stylish as ever, and everything has an air of quality about it. The only issue we observed was a lack of clarity in the more advanced and unusual on-access controls, where what seemed to be options to allow archives to be scanned appeared not to function as intended – but this could have been a misunderstanding on our part of the purpose of the controls in question.

Running through the tests in short order, scanning speeds were solid and dependable, while on-access lag times were excellent, with RAM and CPU usage both at the lower end of the scale.

In the infected sets detection rates were splendid, with another excellent showing in the RAP sets, and with yet another test untroubled by WildList misses or false alarms, ESET further extends its remarkable unbroken run of VB100 awards.

Filseclab Twister Anti-TrojanVirus 11.68.65389

ItW	97.97%	Polymorphic	41.20%
ItW (o/a)	97.91%	Trojans	84.10%
Worms & bots	93.97%	False positives	5

Filseclab has become a pretty regular competitor in our comparatives in the last couple of years, continuing to enter

gamely despite not yet having achieved VB100 certification. The product arrived as a 52MB download direct from the public website, with the updater from the same source at 14MB. The set-up runs through in a few steps, and although an error message pops up at the end, all seems to have completed properly.

The interface is busy and bustling with controls, options and modules. The on-access protection seems a little unusual, kicking in shortly after file reads – thus alerting on malicious activity, but not necessarily blocking the reading or writing of malicious files. As such, the measures taken in our performance tests – which show minimal memory usage and file access lag times – may not be entirely comparable with other products under test this month. On-demand scans were a little on the slow side.

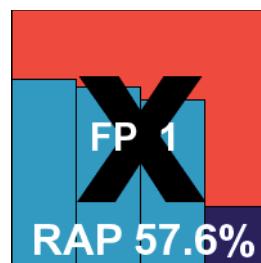
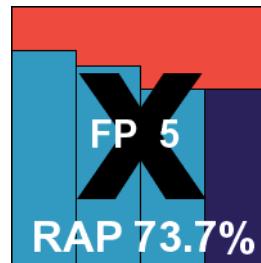
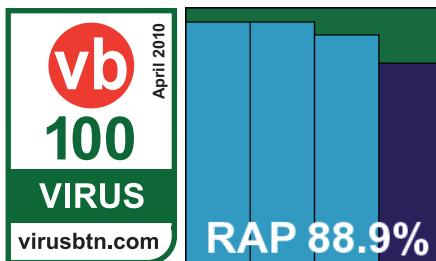
Detection rates were pretty decent – a little lower than desirable in the polymorphic set but with some very solid scores in the RAP sets. The WildList set was covered fairly well, with a few samples missed and imperfect coverage of the latest Virut strain. With a handful of false positives in the clean sets Filseclab still has a little way to go before earning that precious first VB100 award.

Fortinet FortiClient 4.1.2.138

ItW	100.00%	Polymorphic	99.09%
ItW (o/a)	100.00%	Trojans	73.80%
Worms & bots	93.58%	False positives	1

Fortinet's FortiClient arrives as a minute 8MB package, but with a nice big 134MB updater accompanying it. The installation process is fast and easy – just a handful of clicks, a licence key and no reboot required to round things off, followed by a simple manual updating process. The product interface is cleanly designed and well laid out, easy to navigate with an excellent depth of configuration as befits its business credentials.

Scanning times were not super fast, and on-access overheads initially fairly hefty, although much improved on subsequent runs. Memory drain was fairly notable, with CPU usage more middle-of-the-road.

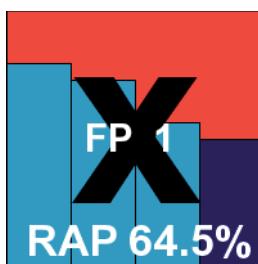


Product	RAM use increase – idle system	RAM use increase – heavy file access	CPU use increase – heavy file access	Product	RAM use increase – idle system	RAM use increase – heavy file access	CPU use increase – heavy file access
Agnitum Outpost	6.52%	8.56%	14.93%	K7 Total Security	8.50%	6.85%	20.51%
AhnLab V3	5.36%	5.62%	25.08%	Kaspersky 2010	8.60%	10.25%	13.44%
Alwil avast!	13.25%	14.64%	30.41%	Kaspersky Anti-Virus 6	8.52%	9.79%	12.38%
Arcabit ArcaVir	10.50%	11.05%	21.63%	Kingsoft I.S. 2010 Advanced	7.60%	6.64%	16.94%
Authentium Command	7.13%	6.86%	35.14%	Kingsoft I.S. 2010 Standard	13.12%	10.25%	15.61%
Avanquest Double A-S	16.89%	22.08%	21.86%	Kingsoft I.S. 2010 Swinstar	N/A	N/A	N/A
AVG I.S.	10.58%	14.17%	28.05%	Lavasoft Ad-Aware	8.80%	11.49%	18.21%
Avira AntiVir Personal	2.44%	3.51%	15.52%	McAfee Total Protection	4.62%	7.75%	16.64%
Avira AntiVir Pro	5.56%	4.39%	20.14%	McAfee VirusScan	5.57%	8.05%	17.81%
BitDefender Antivirus 2010	4.71%	7.59%	24.06%	Microsoft Security Essentials	6.05%	7.01%	17.28%
Bkis Bkav Gateway	5.21%	5.93%	33.65%	Nifty Corp. Security 24	7.07%	9.60%	20.41%
Bkis Bkav Home	3.73%	3.46%	33.88%	Norman Security Suite	8.11%	14.52%	30.26%
Bullguard Antivirus	23.26%	24.70%	31.64%	PC Tools I.S. 2010	11.85%	9.96%	14.43%
CA I.S.S. Plus	20.04%	19.65%	15.08%	PC Tools Spyware Doctor	8.73%	12.05%	31.48%
CA Threat Manager	20.05%	17.10%	15.99%	Preventon Antivirus	8.97%	7.05%	23.66%
Central Command Vexира	3.22%	2.78%	21.85%	Proland Protector Plus	10.26%	10.64%	13.47%
Check Point Zone Alarm	7.11%	9.21%	18.42%	Qihoo 360 Security	3.41%	5.95%	10.38%
Defenx Security Suite	12.27%	13.19%	17.76%	Quick Heal 2010	11.74%	14.61%	27.63%
Digital Defender	7.40%	6.22%	24.38%	Rising I.S. 2010	3.95%	6.61%	28.52%
eEye Digital Security Blink	13.70%	12.28%	12.47%	SGA Corp. SGA-VC	13.23%	13.09%	17.55%
Emsisoft a-squared	N/A	N/A	N/A	Sophos Endpoint	8.69%	7.24%	25.42%
eScan I.S.	4.05%	9.57%	11.54%	SPAMfighter VIRUSfighter Plus	6.63%	5.97%	23.71%
ESET NOD32	5.70%	6.53%	20.73%	SPAMfighter VIRUSfighter Pro	6.93%	6.64%	16.02%
Filseeclab Twister	7.48%	7.02%	22.76%	Sunbelt VIPRE	6.47%	9.91%	26.01%
Fortinet FortiClient	16.59%	19.22%	19.61%	Symantec Endpoint Protection	12.78%	14.45%	11.03%
Frisk F-PROT	7.32%	7.11%	27.28%	Symantec Norton	16.65%	11.22%	20.96%
F-Secure Client Security	7.42%	9.31%	17.17%	Trustport 2010	12.91%	18.05%	22.06%
F-Secure PSB	9.44%	8.15%	17.00%	VirusBuster Professional	3.76%	3.11%	22.27%
G DATA 2010	8.43%	8.46%	27.23%	Webroot SpySweeper	7.90%	14.23%	23.37%
Ikarus virus.utilities	10.74%	7.90%	27.56%				
iolo System Mechanic	17.41%	16.56%	28.19%				

Detection rates seemed generally improved over recent tests, with some especially notable increases in the RAP scores once again. The WildList was covered without difficulty, but in the clean sets a single item was alerted on with a generic detection – enough to upset *Fortinet's* chances of a VB100 award this month.

Frisk F-PROT 6.0.9.3

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	83.12%
Worms & bots	96.40%	False positives	1



Frisk's F-PROT is available as a trial on the company's public website, with the initial download an MSI file of a mere 26MB. It runs through the standard set of steps in just a few moments, all done in just 30 seconds or so with no reboot required. The definitions file is somewhat larger, at 47MB, and is simply dropped in place manually to complete the set-up process.

The interface hasn't changed in a long time, with its simple clean lines and basic configuration settings, and it operates easily and responds well. Running through our tests, we saw some reasonable scanning speeds and not overly intrusive overheads. In the infected sets, a number of error messages hinted at problems with the product, but scans seemed to complete without issues and the on-access protection remained solid.

With tests complete and results in, we saw some pretty decent scores in the main sets, with RAP scores declining steadily across the weeks. The WildList was handled well, but in the clean set the same *Adobe Reader* file that caused problems for *Authentium* was mislabelled, thus denying *Frisk* a VB100 award this month.

F-Secure Client Security 9.00 build 851

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	95.50%
Worms & bots	99.65%	False positives	0

F-Secure once again entered two products for this comparative, with the main client solution provided as a 57MB installer with an updater of 83MB. The install is fairly lengthy, with a number of steps and some notable pauses in between various stages; at the end a reboot is required, with the whole process taking several minutes.

After the first reboot, the interface insisted it was still installing, and the on-access component appeared not to have turned on, but we assumed this was due to the absence of web connectivity, and after a second reboot all seemed fine.

The performance tests were worked through without incident, with some slowish times on the first run but pretty startling improvements in the warm scans. Both memory and CPU usage were pretty low throughout.

We had noted in recent tests some stability issues with the displaying of lengthy log files, but these seem to have been resolved and data was all obtained without difficulty. In the detection tests, the standard sets were covered excellently, while the RAP scores started very high but dropped steadily towards the later weeks. The core certification sets were handled cleanly, and a VB100 award is comfortably earned.

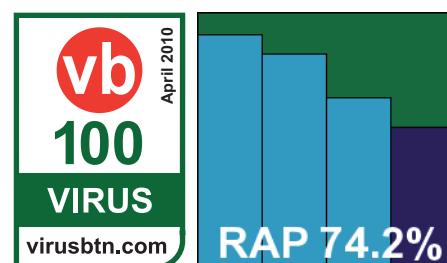
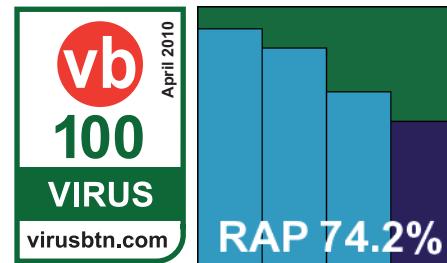
F-Secure PSB Workstation Security 9.00 b149

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	95.50%
Worms & bots	99.65%	False positives	0

The second of *F-Secure's* entries is presumably more business-oriented, but looks and feels pretty identical to the *Client Security*

solution. The initial installer is slightly larger at 69MB, with the same updater used, and the set-up process was much the same. The design and layout of the interface is likewise pretty similar; a clean and cool look with simple, minimalist controls and options.

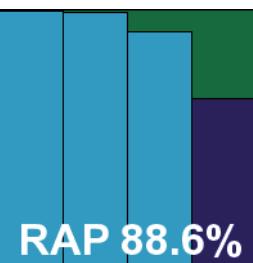
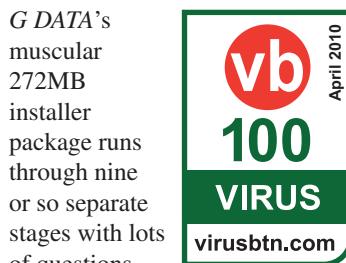
Scanning speeds were also along the same lines as the previous entry, improving remarkably on the second and subsequent runs through the sets, and fairly light on RAM and processor cycles. With the same set of definitions, scores were essentially the same throughout with, as



expected, no problems in the WildList or clean sets. A second VB100 award goes to *F-Secure* this month.

G DATA Antivirus 2010 20.2.4.1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.91%
Worms & bots	99.92%	False positives	0



The interface is attractively designed with some lovely clean lines, and good simple access to all areas of controls. An excellent level of detail is provided for all types of configuration, making the product suitable for the most demanding power user as well as the more trusting novice.

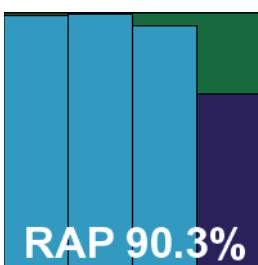
With the fairly thorough default settings, scanning speeds and access times were fairly slow and sluggish, but sped up excellently on subsequent repeat runs, while memory usage was impressively low for a dual-engine product.

Those dual engines really come into play in the detection tests, where truly superb detection levels were attained across the sets, with even the later weeks of the RAP sets handled well. With no issues in the WildList or clean sets, *G DATA* easily earns another VB100 award.

Ikarus virus.utilities 1.0.182

ItW	99.95%	Polymorphic	78.59%
ItW (o/a)	99.95%	Trojans	98.80%
Worms & bots	99.94%	False positives	0

Ikarus put in an excellent performance in the RAP sets on the last occasion it entered, and we were looking forward to more of the same after the good showing of the *Emsisoft* solution (which uses the *Ikarus* engine). The product is supplied as an ISO image of the installer CD, at 195MB all told, with an updater of 54MB. The set-up runs



through in numerous stages, including the installing of the *Microsoft .NET* framework, making for a somewhat lengthy process, but no reboot is needed at the end.

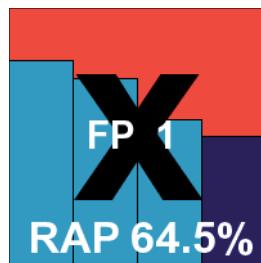
The interface is still rather simplistic and a little wobbly at times, but it provides some basic configuration options. Running scans is also a bit confusing, with little information provided as to the progress of scans. However, they did complete in the end and all the required data was acquired.

Scanning speeds were a little slow, and on-access overheads were not super light, but RAM and CPU usage was not excessive. In the detection tests, as expected the trojans and RAP sets were demolished completely, with truly heroic scores in just about every subsection, while false positives were remarkable for their absence. Sadly, in the WildList set a smattering of samples of the latest W32/Virut strain were not detected, denying *Ikarus* a VB100 award despite an excellent performance in general.

iolo System Mechanic Professional 9.56

ItW	100.00%	Polymorphic	99.85%
ItW (o/a)	100.00%	Trojans	83.23%
Worms & bots	96.38%	False positives	1

It has been a few years since *iolo*'s first few entries in the VB100, and it was good to see it back on board. The company's current flagship product, *System Mechanic*, is widely sold in high street outlets and has had some great reviews for its clean-up and optimization components.



The product was provided as a 64MB installer, requiring Internet connection to update, so it was set up on the deadline day and an image of the test machine taken for later testing. The installation process is rather lengthy, including numerous prompts related to the many components, and required a reboot to complete. The interface is very professional looking, running stably and responsively throughout our tests despite some seriously intense pressure. Little configuration is provided for the anti-malware component, with so many other modules to cover in a single GUI, but the defaults are sensible and it all seems to work nicely.

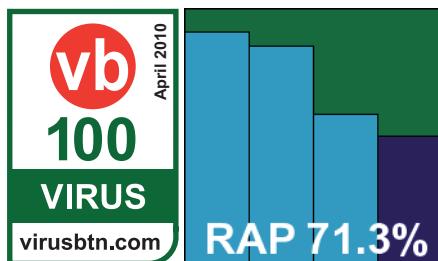
In the speed tests, on-demand scans were not the fastest, with some fairly notable slowing down in the file access times and a sizeable chunk of memory used up. Although the logs were difficult to convert from a rather odd format into more usable text, we got results in the end and detection was found to be generally pretty good throughout,

declining fairly sharply across the RAP sets. Comparing these numbers with others already recorded and perusing the titles of the installation folders gave away the secret of the provider of the core anti-malware components: *Authentium*. Unfortunately, this meant the same false positive which upset *Authentium*'s chances came into play again here, and *iolo* doesn't quite meet the VB100 requirements this month. However, a solid performance hints at much better things to come.

K7 Total Security 10.0.00.29

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.09%
Worms & bots	98.91%	False positives	0

K7 has become a regular fixture in our tests over the last few years, steadily building a solid reputation and considerable respect from the lab team



for simple, solid performances. The install of the current version arrives as a 52.2MB executable and runs lightning-fast, completing in the blink of an eye with just three clicks from the user; no reboot is required.

The interface is colourful and attractive, and laid out clearly and simply. A good level of configuration is made available to fine-tune the behaviour of the product in most respects. Running through all the tests, the product proved stable and reliable despite the heavy stresses, and the on-demand scanning speeds were on the good side of average. On-access lag times were respectable to start with and improved greatly on re-runs, with RAM and CPU footprints also good.

Moving on to the detection tests, some splendid scores were achieved in the standard sets and the earlier RAP sets, with a fairly steep decline into the freshest and proactive sample sets. With only a single suspicious alert in the clean set, and no problems handling the WildList, *K7* adds to its tally of VB100 awards with another fine performance.

Kaspersky Anti-Virus 2010 9.0.0.736

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.84%
Worms & bots	99.12%	False positives	0

Kaspersky also entered two products for this month's test, with the company's retail home-user solution up first. This is

supplied as a 68MB executable, with updates provided as an archived copy of the online databases (the archive measuring a hefty 360MB). The installation process runs through several stages, including a request for a licence code. Although licence files were supplied, there was no obvious way to load them in, and the product seemed averse to accepting any codes typed in, so we proceeded with a trial version only. No restart was required to get protection in place.

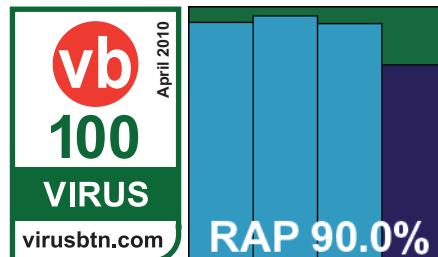
The green-and-red-heavy interface is big on clarity, with large fonts and simple phrasing making for simple and error-free navigation. Beneath the novice-friendly veneer, configuration is provided in enough depth to satisfy the most demanding of power users. This made running through the tests something of a breeze, with scanning speeds only average at first but benefiting hugely from some intelligent caching on subsequent runs. On-access overheads were similarly unobtrusive, while memory usage was perhaps a little above average but CPU cycle impact fairly low.

In the infected sets, detection rates came in even better than we had expected, with excellent figures across all sets. A remarkable steadiness in the reactive portion of the RAP sets supports the company's reputation for rapid reaction to newly emerging threats. Despite our worries after seeing issues with other products using the *Kaspersky* technology, no problems were encountered in the WildList, and with the clean sets also handled well *Kaspersky* solidly earns another VB100 award.

Kaspersky Anti-Virus 6 for Windows Workstations 6.0.4.1212

ItW	99.99%	Polymorphic	99.99%
ItW (o/a)	99.99%	Trojans	95.39%
Worms & bots	98.56%	False positives	0

Kaspersky's second entry is, we assume, a more corporate-focused one, provided as a 62MB installer package, with the same batch of files also used to update from. Again the install process runs through numerous stages, many related to the firewall components, and a reboot is required, with further configuration on restart.



The interface is pretty similar to the 2010 edition in most respects, with good clarity and excellent configuration options. Speed and performance measures closely mirrored the home-user product, while detection rates were slightly lower in most sets but still achieved a generally excellent level, especially in the RAP sets.

The clean sets were handled without issues, but in the WildList set the same single sample of Virut which caused problems earlier went undetected – hinting that the 2010 edition uses some advanced detection skills not included in version 6. *Kaspersky Anti-Virus 6* is thus denied a VB100 award this month by a whisker.

Kingsoft Internet Security 2010 Advanced Edition 2008.11.6.63

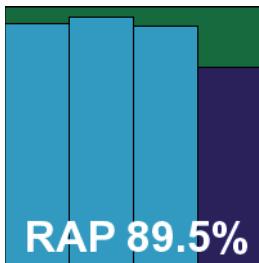
ItW	100.00%	Polymorphic	56.61%
ItW (o/a)	100.00%	Trojans	11.02%
Worms & bots	80.40%	False positives	0

Kingsoft submitted a trio of products for the test in something of a hurry as the deadline clashed with the new year holidays in

China. The *Advanced* edition was provided as a 46MB executable with updates included, and installed simply in just a handful of steps, completing in 30 seconds or so and not requiring a reboot.

The interface is unchanged from several previous tests – simple and clear with a good level of controls provided, and it seemed stable and responsive throughout testing. Scanning speeds were unexciting, and lag times a little above medium but showing signs of improvement on re-running. Memory use and CPU impact were on the better side of average, though.

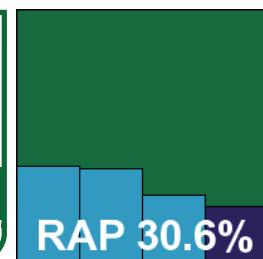
In the infected sets, scores were generally pretty feeble, with some real problems in the trojans sets and RAP scores starting low and heading downwards sharply. The WildList was handled adequately though, and with no problems in the clean sets *Kingsoft's Advanced* product meets the requirements for a VB100 award.



Kingsoft Internet Security 2010 Standard Edition 2008.11.6.63

ItW	100.00%	Polymorphic	56.61%
ItW (o/a)	100.00%	Trojans	20.93%
Worms & bots	81.84%	False positives	0

The *Standard* edition of *Kingsoft's* product is nearly indistinguishable from the *Advanced* one in most respects, with an identical install process



and interface. Scanning speeds were also remarkably similar, but memory usage was notably higher.

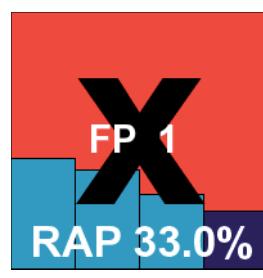
Also higher were detection rates in the trojans and RAP sets, suggesting that the hurried submission had perhaps led to some errors in the updating of the *Advanced* edition; while still not great, the improvements take the scores out of the disastrous zone into the merely weak.

However, the WildList was again covered cleanly, and with the clean sets also handled without problems *Kingsoft* wins a second VB100 award for its *Standard* edition.

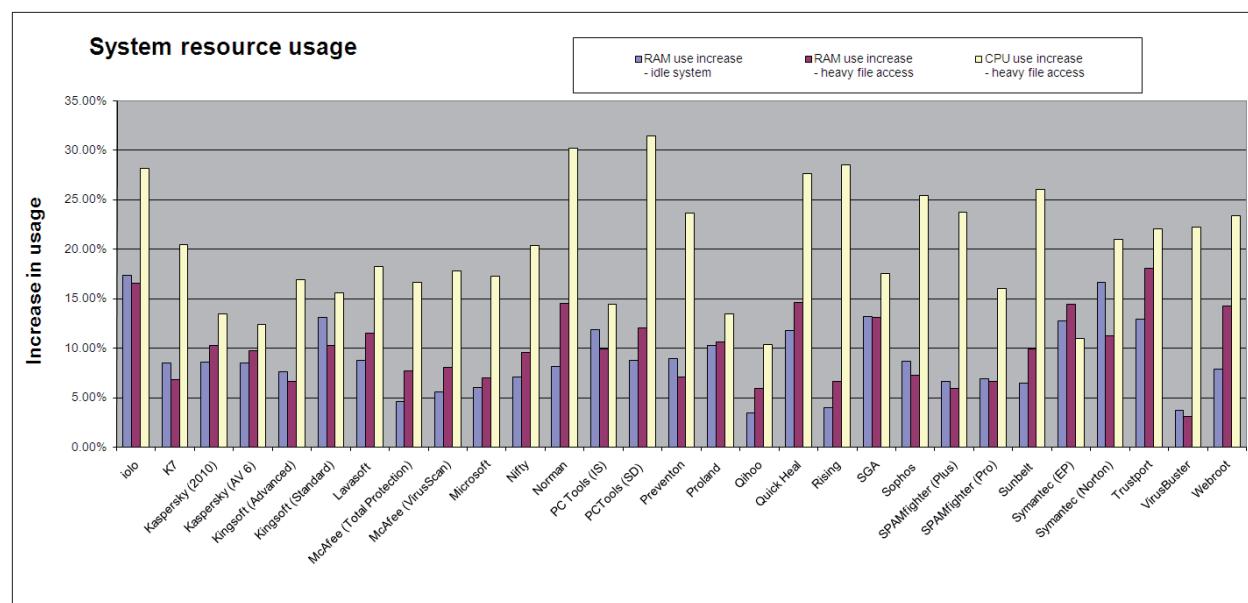
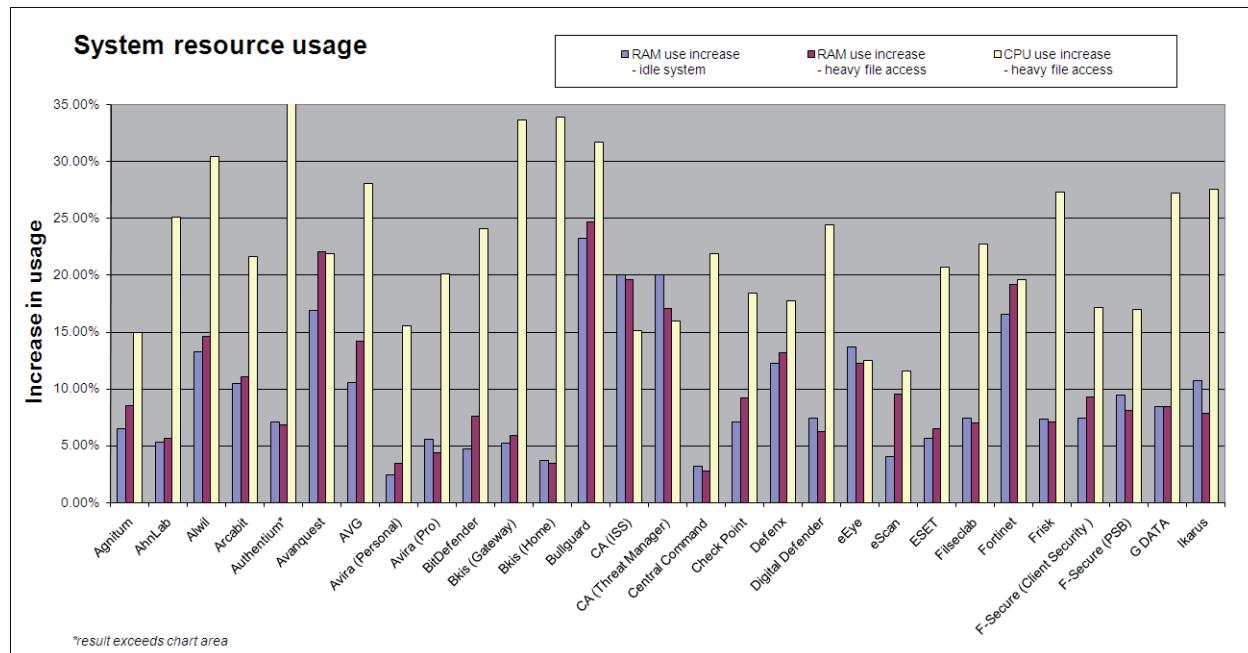
Kingsoft Internet Security 2010 Swinstar Edition 2010.01.13.06

ItW	99.17%	Polymorphic	47.72%
ItW (o/a)	N/A	Trojans	43.99%
Worms & bots	87.18%	False positives	1

Kingsoft's third entry, labelled ‘Swinstar’, is apparently a bleeding-edge preview of the company’s upcoming technology, as hinted at by the version numbers. The miniature 29MB installer takes only two clicks to run through and is done in seconds; no reboot is needed.



The redesigned interface remains simple, gaining perhaps a little glitz and glamour but still seem fairly easy to use, with a decent level of configuration. Not all of the options provided seemed fully functional however, as despite all our efforts we could not persuade the on-access component to respond at all, even to execution of malicious files. Even more bizarrely, the Eicar test file was not detected even



in the apparently functional on-demand mode. Thus, our archive depth and performance measures were rendered useless; on-demand scanning speeds were recorded, and proved to be somewhat quicker than the previous editions, putting them on the better side of average.

Detection rates were also notably improved, although still not reaching the heights of decent. A handful of W32/Virut samples were missed in the WildList set, compounding the absence of on-access protection to prevent *Kingssoft's* third entry this month from earning a VB100 award.

Lavasoft Ad-Aware Professional Internet Security 8.2.0

ItW	100.00%	Polymorphic	65.16%
ItW (o/a)	99.72%	Trojans	99.10%
Worms & bots	99.71%	False positives	2

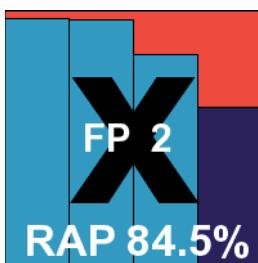
This month, *Lavasoft's* renowned *Ad-Aware* makes its long-awaited debut in our VB100 tests. After being impressed by the product in a standalone review some time ago (see VB, September 2008, p.14), we've been waiting for on-read detection to be enabled before it could be pushed

through our tests, and were

excited to see it finally arrive on the test bench. The installer was a fairly sizeable 151MB, and ran through in not too many steps, one of which was the offer of a toolbar, taking a minute or so in total and needing a reboot to finish off. After restarting, the system seemed to take some time to come to.

The interface is fairly simplistic, with access to controls a little confusing and, when found, not very detailed. Nevertheless, running through the standard performance tests was not a problem, with some fairly good throughput times and pretty light on-access overheads – although memory usage was perhaps a little on the high side.

In the infected sets things were a little less straightforward. Initial runs through the test sets failed numerous times, with the scans – and on occasion the entire system – coming to a grinding halt. Part of the cause of this seemed to be the approach to scanning, which insists on storing all detection data in memory and not writing anything out to logs until after actions have been applied to detected items. This meant that after running scans over large-ish infected sets – which took a few hours even on trimmed down portions of the standard test sets – we had to wait for the disinfection and removal process to complete before any data could be gathered. As this could take up to ten times as long as the scan itself, it left much more



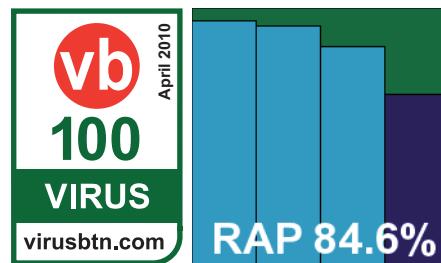
opportunity for problems to emerge, and as the memory usage built steadily, errors cropped up regularly – at one point the main process tried to absorb 2GB of memory before collapsing under its own weight. Similar problems emerged during the on-access tests too, but eventually, by splitting the sets into smaller and smaller chunks and re-running tests until they ran through to completion, we managed to gather some usable figures. Of course, this kind of scenario would be unlikely (although not impossible) in the real world, but we do expect products to be fairly resilient when under pressure.

In the final reckoning, some pretty decent detection scores were achieved, especially in the RAP sets, with the numbers as well as the stability issues hinting at a change of engine provider since we last looked at the product. In the WildList however, a pair of items were not picked up on access, thanks to a fairly common file extension being missed from the list of types to scan by default. A couple of false positives in the clean sets confirmed that *Lavasoft* would not qualify for a VB100 award this month.

McAfee Total Protection 10.0.570

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	95.91%
Worms & bots	99.40%	False positives	0

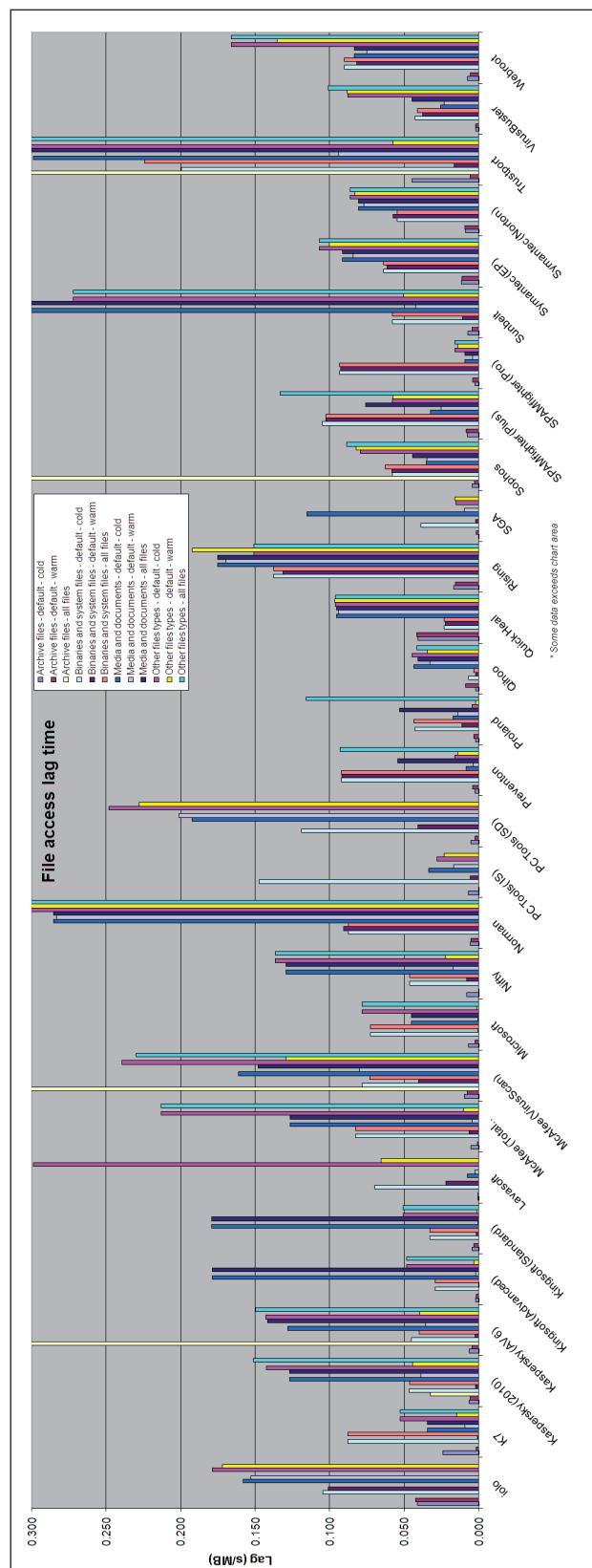
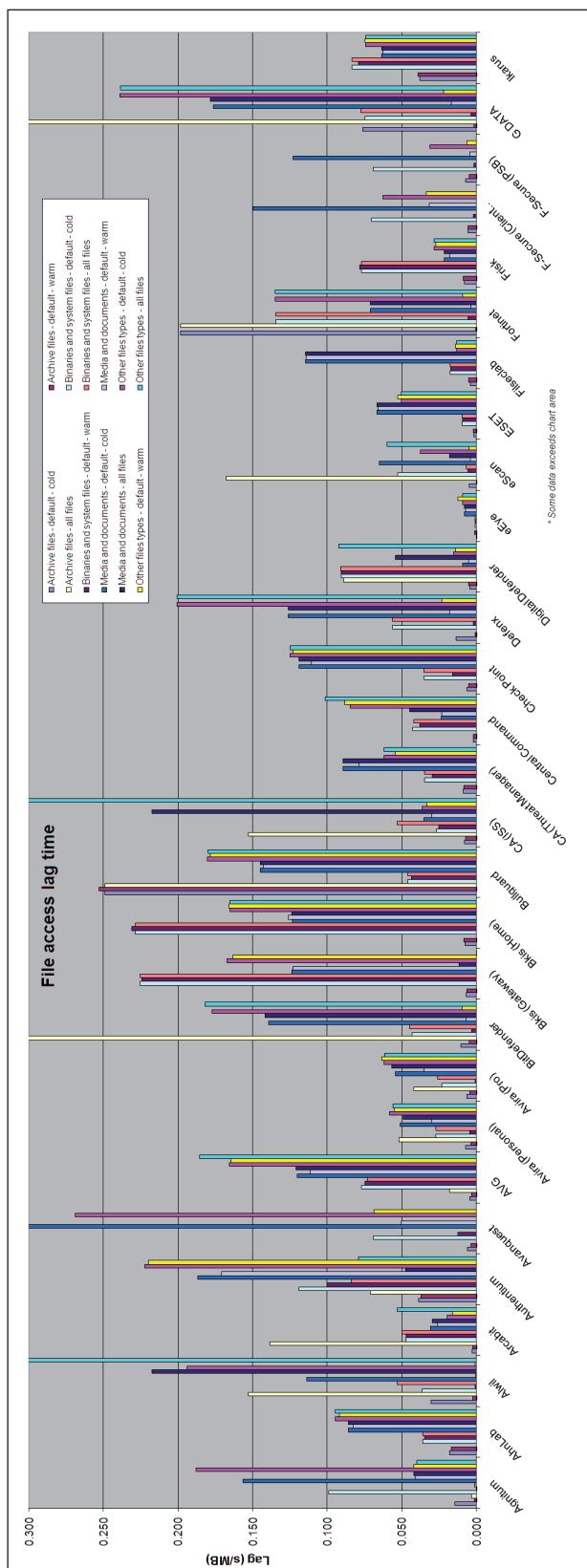
Back to another regular, *McAfee* products having taken part in VB100s since the dawn of time. The company has recently



RAP 84.6%

started submitting its consumer product lines as well as its corporate offerings, and these have caused us a few minor difficulties thanks to the apparent absence of any facility for installing or updating without web access, but having made special provisions for such products this was less of a hassle than usual this month. The original installer downloaded from the company's website measures only 2.8MB, and when run pulls the remainder of the product down, with over 100MB coming through in the initial run; the process is fairly simple and idiot-proof, taking at most a few minutes to get everything done with no reboot needed at the end.

The interface of this version is slightly different from the others we've looked at lately, and seems to buck the trend towards colourfulness and curvy lines in consumer



products. This one is grey, bleak and boxy, rather bewildering to navigate, at times slow to respond and provides minimal configuration options, but behind the brittle exterior it seems to run smoothly and solidly with not a whisper of stability problems.

On-demand scans were good and fast, while file access lags were a little slower than some, and memory and CPU usage seemed light. The infected test sets were handled excellently, with some good scores in the RAP sets too, and with no problems in the WildList or clean sets *McAfee* takes away another VB100 award without difficulty.

McAfee VirusScan Enterprise 8.7.0i

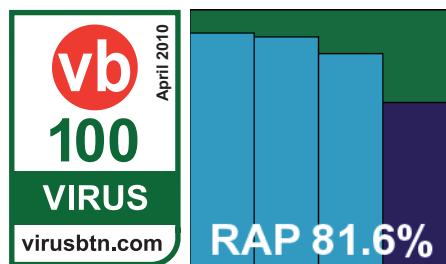
ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	93.35%
Worms & bots	99.11%	False positives	0

Total Protection's corporate big brother, *VirusScan*, is much more flexible, as befits a serious business environment,

and comes as a zip bundle of 84MB with an automated updater program of 120MB. The install process features numerous steps split into several stages, and is presented stolidly and chunkily throughout. On completion, a reboot is not demanded, but is recommended as it is required for the loading of one of the network drivers.

Like the previous product, the interface takes a grey and angular theme, but somehow it seems much more reassuring here. This is solid, respectable and unpretentious business software, providing what's needed without fuss, and it seems to do it well; configuration is provided in minute detail and everything seems sensible and logical – very much approved of by the lab team.

Scanning speeds were average, and on-access lag times fairly hefty, but with minimal RAM and CPU impact. Running through the main test sets proved no problem, with detection rates a trifle lower than the home-user scores, probably thanks to the several hours difference between grabbing the offline updater package and finally completing the online install for the other product. The WildList was covered in its entirety however, and with no issues in the clean sets either, *McAfee* adds further to its VB100 haul.



Microsoft Security Essentials 1.0.1611.0

ItW	99.99%	Polymorphic	100.00%
ItW (o/a)	99.99%	Trojans	95.41%
Worms & bots	99.42%	False positives	0

Microsoft's much lauded free-for-all desktop product seems to be doing good business and making some impression on the overall malware problem. A major update was recently made available, but didn't quite make the cut for this month's test. The product is usually installed online, but for our purposes an offline installer and updater were made available, measuring 60MB and 52MB respectively, which ran through swiftly in a handful of simple steps. No reboot was needed to finalize the process, and we were swiftly up and running.

The interface is simple and straightforward, neither overly fancy nor unsettlingly strait-laced; it provides some degree of configuration, but generally encourages users to stick to the (fairly sensible) pre-ordained defaults. Logging was a little strange for our purposes, but we eventually worked out how to process the details and got some usable results.

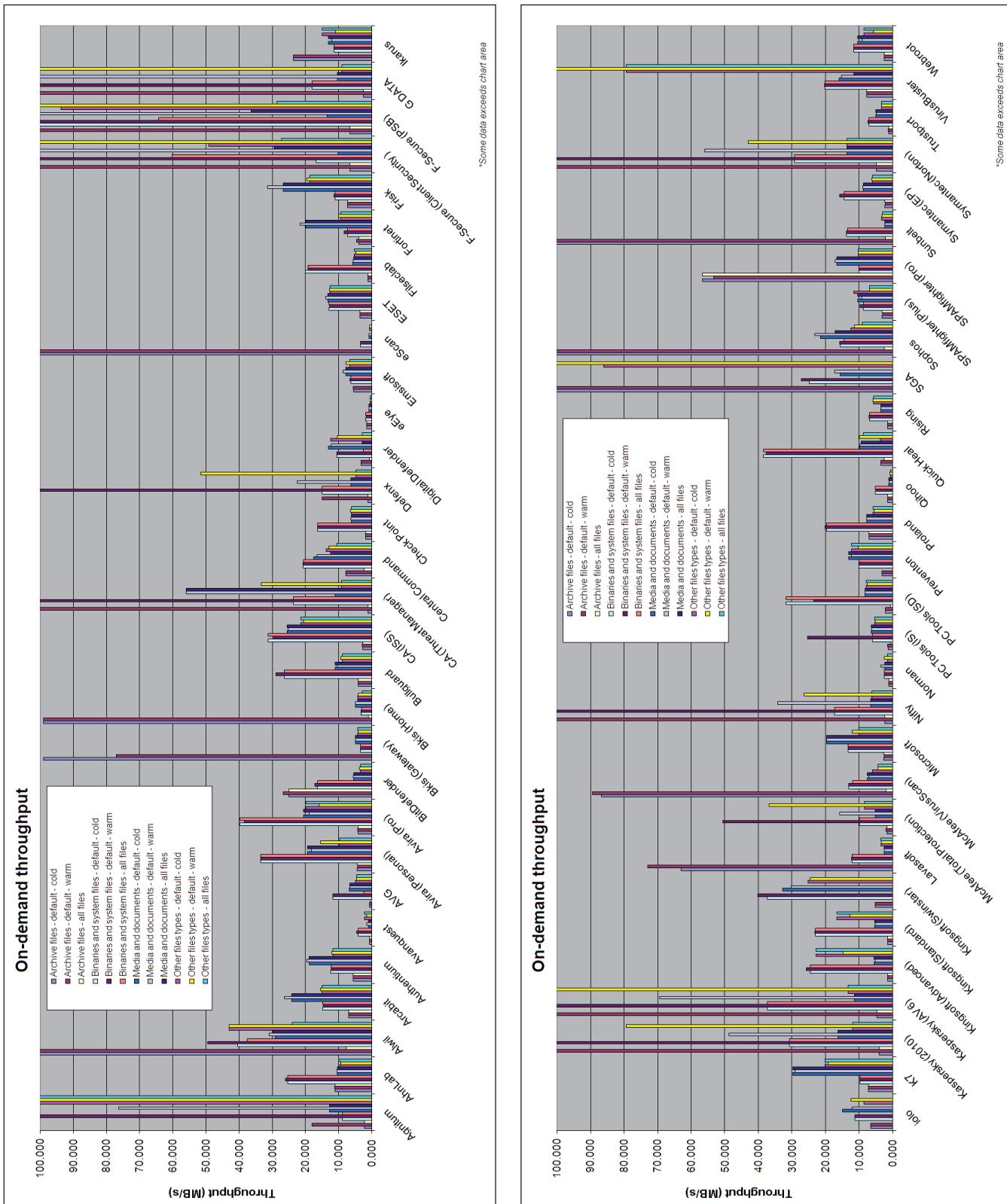
On-demand throughput was on the decent side, with file access lag times not bad to start with and barely perceptible once the product had settled into the system. The new performance measures showed a fair amount of RAM and CPU usage.

In the detection sets, coverage was generally excellent, with some very respectable scores in all sets. The clean sets caused no problems, but in the WildList set a single sample of the large batch of W32/Virut replications was not detected, showing a minor flaw in coverage of this strain – enough to deny *Microsoft* a VB100 award this month.

Nifty Corp. Security 24 5.6

ItW	99.99%	Polymorphic	99.99%
ItW (o/a)	99.99%	Trojans	94.31%
Worms & bots	98.62%	False positives	0

Nifty, the Japanese firm whose product is based on the *Kaspersky* detection engine, returns to our test bench this month to challenge us with its unusually designed, untranslated interface. Provided as a 163MB zip containing all components including updates, the install process runs through only a handful of steps, not all of them displaying properly even with basic Japanese character support.



included. Installation completes in under a minute before insisting on a reboot to finish things off.

Once installed, and guided by some instructions from the developers where characters were not properly displayed, we soon found our way around those bits of the GUI we needed access to, but detailed configuration was a little beyond the scope of our investigations. The defaults seemed fairly sensible though, and speed tests ran through nicely, with some good use of caching technology to speed things up over multiple runs. The memory usage also seemed fairly low.

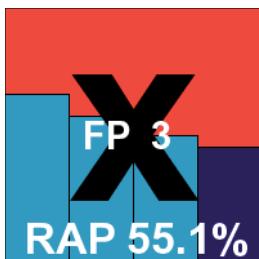
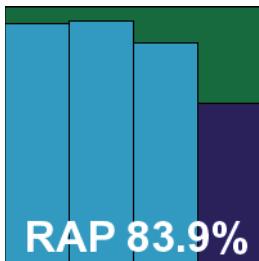
Detection rates were generally excellent, as expected of the *Kaspersky* engine, with a couple of perfectly justified suspicious alerts in the clean sets. In the WildList set, as feared, a single Virut sample was not detected, and thus *Nifty* is denied a VB100 award this month despite an otherwise strong performance.

Norman Security Suite 7.3

ItW	99.99%	Polymorphic	82.92%
ItW (o/a)	99.99%	Trojans	76.42%
Worms & bots	94.48%	False positives	3

Norman's flagship suite has been rejigged lately and received some approving glances from the lab team in the last *Windows* comparative. The current product comes as a 65MB installer, including all updates, and runs through in half a dozen steps which include firewall details and information on the experience level of the user. At the end, a message indicates that a reboot may be required shortly, and sure enough after another minute or so it does indeed ask the user to restart the system.

The interface is browser-based and looks competent and serious. It is fairly easy to navigate and provides a basic selection of configuration options, but in some areas it seemed a little baffling – having gone to the trouble of setting up some on-demand scan jobs using the task editor utility, there appeared to be no way to fire them off. We could have missed something of course, but being in something of a hurry we resorted to using the context-menu scanner instead. One other eccentricity about the product is the provision of a screensaver scanner, which runs when the computer is not in use.

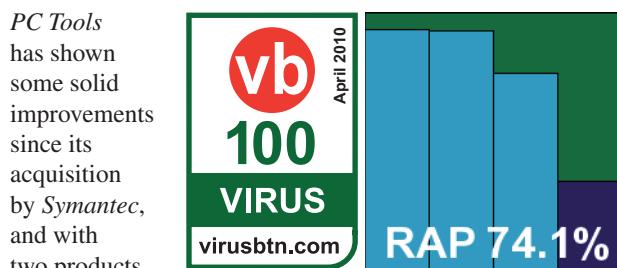


Ploughing through the speed tests took some time, in part thanks to the sandbox system which carefully checked out unknown files in the clean sets; this would have benefited from some caching of previous results to speed things up on re-runs. Both memory and CPU cycle usage seemed rather higher than most.

Detection rates were not bad though; there was a fair showing in the trojan and RAP sets, with a steady decline in the more recent weeks. In the WildList, a selection of Virut samples were missed – rather more on access than on demand thanks to the sandbox catching a few more – and a handful of false positives were raised in the clean sets, one of which was yet another version of the *Adobe Reader* installer. *Norman* thus does not reach the required grade for VB100 certification this month.

PC Tools Internet Security 7.0.0.514

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.95%
Worms & bots	99.51%	False positives	0



PC Tools has shown some solid improvements since its acquisition by *Symantec*, and with two products submitted as usual we looked forward to a continuation of this trend. The top-of-the-line *Internet Security* product comes as a chunky 117MB installer, which runs through quickly, with just five dialogs to respond to and a run time of under 30 seconds on a fast system.

Once up and running, the interface is slick and attractive, still not very instinctive to operate but providing a fair selection of configuration options after a little exploration. Running on-demand scans was a little frustrating thanks to a long delay opening the browse window each time, but we eventually got to the end and gathered some results.

These showed some slowish scan times but feather-light impact on file accesses. Memory use was a little on the high side but CPU use tended toward the lower end, making for what seems an overall well-balanced performance.

Detection rates again showed major improvements over previous months; the reactive parts of the RAP sets were covered superbly, although a significant drop was observed in the samples gathered after the product deadline. With no

issues in the clean or WildList sets, *PC Tools* comfortably earns another VB100 award.

PC Tools Spyware Doctor 7.0.0.538

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.93%
Worms & bots	99.51%	False positives	0

Spyware Doctor contains most of the same components as the *Internet Security* suite product, bar the firewall, and the set-up

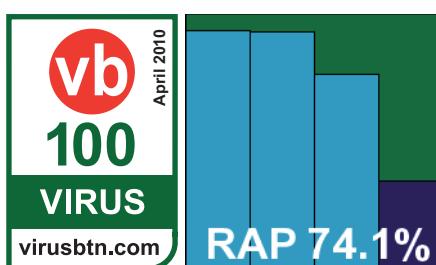
process, run from a 109MB install package with all updates preloaded, zips through in the same sort of time – one major difference being the offer of a *Google* toolbar. The navigation process was eased slightly by having already explored the suite solution and we stormed through the tests, finding some pretty similar results as expected, but a few minor differences too.

The on-demand scanning speeds were notably faster, while the access lags were considerably heavier; RAM usage balanced out as much the same, with slightly less used while idle but more when under heavy strain. Use of CPU cycles also seemed heavier. Detection rates were very similar to those of the previous product, and with matching results in the clean and WildList sets, another VB100 award is comfortably earned by *PC Tools*.

Preventon AntiVirus 4.1.67

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	88.69%
Worms & bots	97.37%	False positives	0

Preventon made a successful debut in the recent *Windows 7* test and looked likely to repeat its success again this month, given the results already obtained for other products



using the same technology. The 48MB installer took half a dozen clicks and under 30 seconds to get its business done, and didn't need a reboot to put the machine under its protective sway.

The interface is simple and unfussy but manages to provide a decent set of options. Running through the tests was something of a breeze therefore, and glancing through the results showed the expected fairly zippy scanning speeds, fairly light lag times and slightly higher use of CPU and RAM.

Detection results were also much as expected, with solid coverage in the standard sets and a decent level in the RAP sets, declining steadily across the weeks. The WildList and clean set posed no difficulties, and *Preventon* keeps up its record of VB100 passes to make it two out of two.

Proland Protector Plus Professional 9.1.003

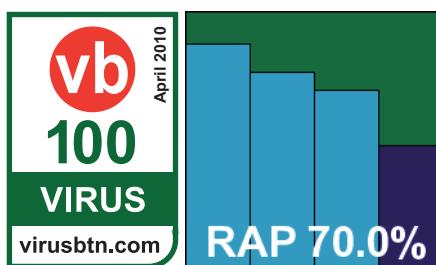
ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	88.94%
Worms & bots	97.84%	False positives	0

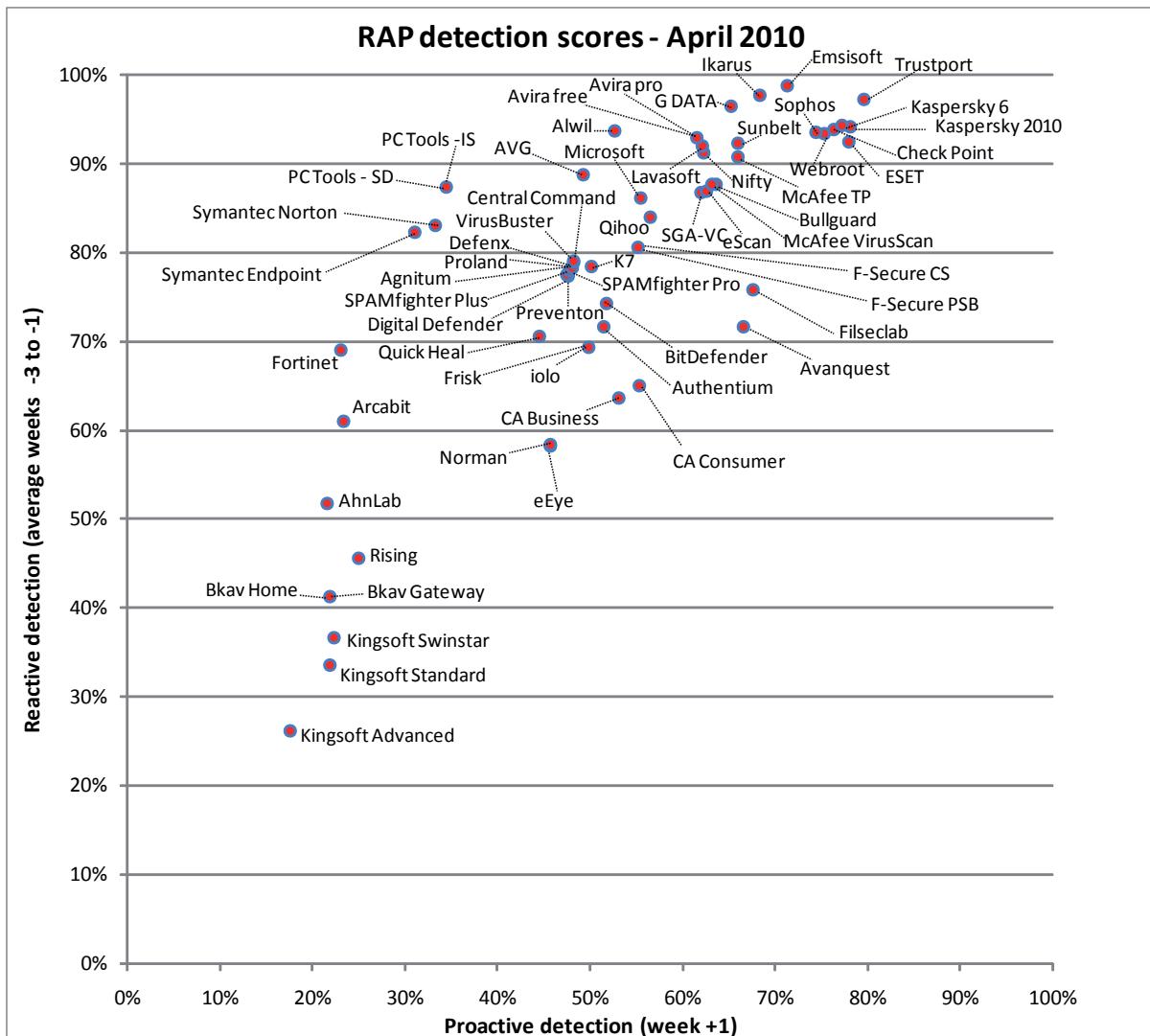
The *Proland* name is something of a blast from the past, the company having entered products in several tests in the late 1990s, and again in

a few scattered comparatives in more recent years – so far without much success. Its return took the form of a fairly normal 48MB installer, which ran through in six steps in under 30 seconds, with no reboot.

The interface is clear and lucid, with some attractive use of colour but no attempt to overdo the styling; it provides a decent level of basic configuration, with sensible defaults, and seems to respond well to the user even under pressure. Scanning speeds were fairly good, with a light touch in terms of file access lags but a fair amount of memory being used, while detection rates were generally solid with a decent starting level in the RAP sets.

For those experiencing *déjà vu* here, fear not; the merest glance at the scores quickly confirms that this is yet another implementation of a hugely popular engine for OEM retailers. The WildList and clean sets were handled ably, and *Proland* takes home a VB100 award.

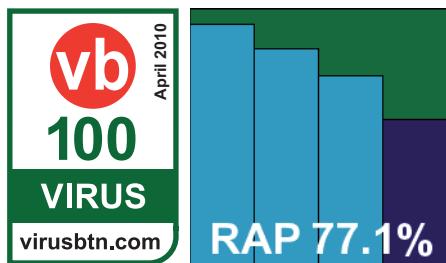




Qihoo 360 Security 1.1.0.1096

ItW	100.00%	Polymorphic	99.98%
ItW (o/a)	100.00%	Trojans	97.01%
Worms & bots	99.55%	False positives	0

Qihoo first appeared on the VB100 radar in the Windows 7 test late last year, with some success; the Chinese product uses the



BitDefender engine, and this month also offered full English translation, for our testing pleasure. The installer is no more than 77MB complete with updates, runs though in under 30 seconds with just a handful of clicks, proudly featuring a VB100 logo on one of the dialogs, and no reboot is needed.

The interface is pretty clear and simple, with the new translations helping us a lot; it seems nicely laid out, easy to navigate and responsive. On-access behaviour is a little eccentric, claiming in its configuration to block access to infected files on-read, whereas in fact access appears to be allowed, with warning pop-ups appearing shortly afterwards (or quite some time later if, like us, you bombard the solution with detections and the pop-ups have to queue up for the user's attention). Nevertheless, logs were kept of detections and results calculated from those.

The non-standard approach to on-access protection may have resulted in some less than accurate performance records, which seem to show an extremely light impact on the system; on-demand scans, by contrast, were rather slow. Detection rates were hard to fault however, with some splendid scores across the sets. With no problems in the WildList or clean sets *Qihoo* earns its second VB100 award in a row.

Quick Heal AntiVirus 2010 11.0.4.0.0.2

ItW	100.00%	Polymorphic	99.51%
ItW (o/a)	100.00%	Trojans	83.47%
Worms & bots	96.34%	False positives	0

Back among the VB100 veterans, it's a rare test that doesn't feature a *Quick Heal* product, and its appearance is usually welcomed

thanks to a strong reputation for straightforward, reliable and zippy behaviour. The current version came in at 88MB, and again installed very rapidly with just a few dialog prompts, completing with no reboot required in under a minute, including the brief 'pre-scan' run to check for dangerously infected systems.

The interface has been given a fresh lick of paint for the new decade but remains much the same in layout and design; simple, elegant and efficient, it manages to provide a solid level of configuration without over-cluttering itself.

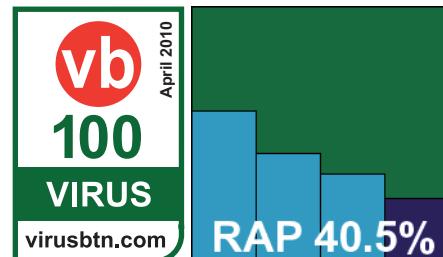
Scanning speeds were perhaps not quite as fast as we're used to, with impact on system resources slightly heavier than expected too; detection rates were decent though, with a respectable level achieved across the sets. The WildList and clean sets presented no difficulties, and *Quick Heal* earns yet another VB100 award.

Rising Internet Security 2010 22.00.02.96

ItW	100.00%	Polymorphic	70.02%
ItW (o/a)	100.00%	Trojans	54.05%
Worms & bots	87.94%	False positives	0

Despite being a long familiar name in the industry, *Rising* has a surprisingly short history in the VB100, with a good showing in 2008 followed by fewer entries and less luck in 2009. The company's 2010 product, provided as a 74MB

installer, started slowly with a rather lengthy set-up process, multiple dialogs to respond to and a reboot required.



Running through the tests was helped by a slick and attractive interface that also managed to pack in plenty of configuration without hampering easy navigation; the dancing lion in the corner of the screen was perhaps less useful. Speed tests seemed to pass without incident, recording some sluggish on-demand times and some hefty lags on access, although RAM usage was impressively low.

The detection tests were a rockier ride, with excitement aplenty; the heavy strain of the test sets did some odd things to the system, including some nasty mangling of the window manager which took some time to recover from. The on-access scanner appeared to shut down on occasion too; it was not clear whether this was caused by a particularly problematic file or by general exhaustion from the strain, but most of the main sets were managed without too much difficulty and the trojans set was eventually run to completion thanks to hard work, numerous small runs and removal of any files which seemed to be causing difficulties. On-demand scans ran a little more smoothly, although there was still a hefty impact on the system, and the logs produced at the end were pretty awkward for a human to interpret (a button is provided in the GUI to export them, but this seemed permanently greyed out).

Eventually we had all the information we needed in a usable form, and it showed some respectable figures in some sets, with the RAP scores perhaps a little disappointing and the trojan set scores hampered by the issues getting complete scans to run. The WildList was handled impeccably though, and without issue in the clean sets *Rising* scrapes its way to another VB100 award, tempered with hopes that these issues are resolved as soon as possible.

SGA Corp. SGA-VC 2

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.92%
Worms & bots	99.49%	False positives	0

While the name *SGA-VC* may not ring many bells with our readers, veteran followers of the VB100 will doubtless recall *VirusChaser*, which had a long and proud history in our comparatives until a few years ago. Returning after a lengthy absence, both the product and the company have

undergone something of a revamp, with the vendor now known as *SGA Corporation* and its product referred to generally as *VC*, although

the full '*VirusChaser*' title does crop up here and there. Internally, the core detection technology is now apparently provided by *BitDefender*.

The product was supplied to us as a 79MB installer with the updates rolled in, which took just half a dozen clicks and less than a minute to get up and running, with no reboot required. Translation seemed only partially complete, with much of the EULA presented in characters which couldn't be properly rendered by an English version of *Windows*. Another integration issue presented itself on the first run, when the *Windows Firewall* warned that it had blocked the scanner's activities – presumably an initial update attempt.

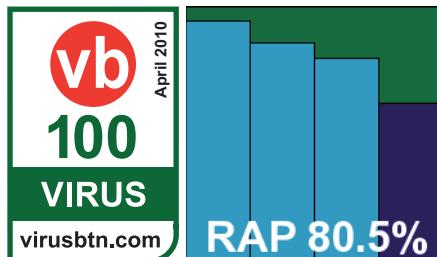
The main interface seemed straightforward enough though – a little cluttered and text-heavy but with the main components displayed clearly. Configuration proved a little minimal, with very little available that we needed; it was entirely impossible, for example, to persuade the product to scan anything other than its default extension list, while the archive option is present but seemed to have no effect. There was also some confusion over the whitelisting mode: a sample was accidentally marked 'always ignore' and there was no clear way of undoing this.

Nevertheless, we soon got through all our jobs, and found some usable results after untangling the product's logs. With the light default settings scanning speeds were pretty fast and lag times low, while resource usage was very low indeed. Detection rates, on the other hand, were very high, with great scores across the board – in many cases notably higher than those of *BitDefender* itself, presumably due to some adjustments to the engine's sensitive heuristics or some additional detection technology provided by *SGA*.

The WildList and clean sets caused no problems, and *SGA* comfortably returns *VirusChaser* to the ranks of VB100 certified products.

Sophos Endpoint Security and Control 9.0.3

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	95.32%
Worms & bots	99.14%	False positives	0



Sophos's latest product range has a rather ungainly title, but after a spell of leaning towards a scattered modularity seems now to

have gently absorbed the multiple additional components that have been thrown in, rather than having them bolted on top or hovering awkwardly alongside. The version provided for the test weighed in at a lightish 66MB, with an additional 13MB of updates, and the installer was fairly fast and simple after a brief pause at the beginning.

With things quickly up and running, and the interface still its same no-frills self – with easy access to the main components and some quite absurdly detailed configuration just a few clicks away – tests sped swiftly along. Scanning speeds were pretty good, while lag times were no more than medium, and resource usage leaned towards the better side of average.

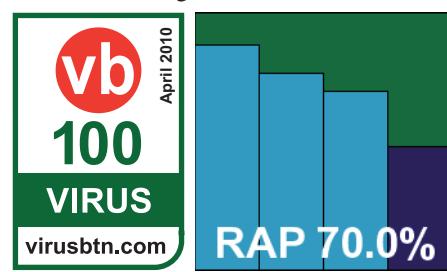
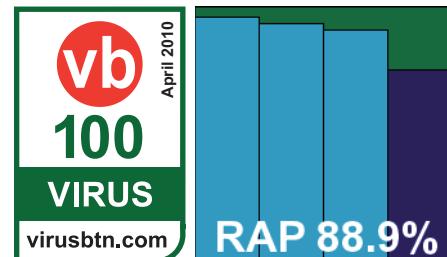
Detection figures were solid and assured, with some excellent scores in the RAP sets, and stability was generally solid. At one point – perhaps trusting too much in the product's reliable reputation – we took a shortcut and kicked off an overnight run of the main sets while an on-access test of the same sets was still running. On our return the next day we found an error message and a crash dump, but the incident did not seem to have affected either test, both of which had finished happily and produced excellent results. With the WildList and clean sets causing no problems, *Sophos* romps to another VB100 award.

SPAMfighter VIRUSfighter Plus 6.100.3

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	88.50%
Worms & bots	97.36%	False positives	0

Yet another new face, *SPAMfighter* first considered a VB100 entry some years ago, at which time the product was using *Norman*'s detection engine. Now a member of

our elite band of VBSpam certified vendors, the company joins the VB100 tests too, with a pair of entries.



The ‘Plus’ version was provided ready for action as a 46MB executable. There were few prompts to get through before the installation process kicked off, but it took a full five minutes, with no reboot, to complete. The design is simple and novice-friendly, colourful and full of encouraging language as well as details of the firm’s other products. A handful of the more vital configuration options are provided, but little else besides.

Performance measures showed some slow-ish scan times and heavy-ish lags, but RAM and CPU usage was fairly respectable; detection rates were quite solid with a steady downward curve in the RAP sets, and the figures revealed yet another entry for this month’s most popular engine by some considerable distance. The WildList and clean sets were, unsurprisingly, handled immaculately, and *SPAMfighter* also joins the growing ranks of VB100-certified vendors.

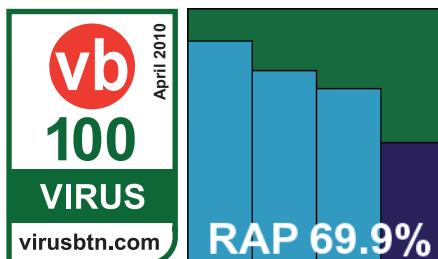
SPAMfighter VIRUSfighter Pro 6.2.68

ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	88.69%
Worms & bots	97.37%	False positives	0

SPAMfighter’s second product seems to be a slight step down in class from the first, although there is little obvious difference to the naked eye.

This one was not prepared in advance and required online installation and updating, but this was a fairly simple process, no more difficult or time-consuming than the offline experience of the *Plus* version. The interface looks identical, and we hoped for a similarly smooth run through the tests, but soon discovered there would be some impediment to this.

While the *Plus* version had been set simply to block access and log detections, this version insists on attempting to disinfect or quarantine every item it detects. As we have seen from other products in the past, this approach can make large tests rather slow and difficult. Eventually, as the test period drew to a close, we were able to allocate the product four of our test systems for a whole weekend, and with each of them running a section of the main tests we finally got some results in only four-and-a-bit days, or 16.5 machine/days (given our original estimate of one machine/day per product to complete the test on time, this



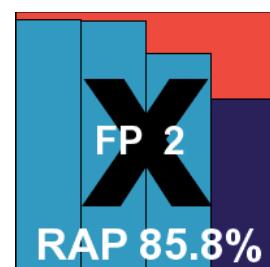
was rather generous of us, but we were keen to ensure the test reached a nice round number of participants).

With these issues aside (which are fairly minor, unlikely to affect the majority of users, and due to be fixed with an additional button in an upcoming build), all went pretty smoothly, with scanning speeds slightly faster and file access lag times slightly slower than the *Plus* edition. Resource usage was pretty identical, as were detection rates across the sets. Again no problems cropped up in the core sets, and *SPAMfighter* takes away a second VB100 award this month.

Sunbelt VIPRE AntiVirus Premium 4.0.3248

ItW	100.00%	Polymorphic	65.19%
ItW (o/a)	N/A	Trojans	98.98%
Worms & bots	99.71%	False positives	2

Another of those gaining their first VB100 award in the recent Windows 7 comparative and back hoping for more of the same, *Sunbelt* provided its latest product as a 16MB installer with a 55MB update package. The install itself was fast and easy with just a handful of prompts including a licence code request, and was done in around 30 seconds, at which point a reboot was required. From the installer title, it was clear that this product was in a late beta stage.



The design of the interface remains simple and fairly clear. Most options are not deeply configurable but some controls at least are provided; some areas seemed to have changed rather subtly from previous versions, and it was not entirely clear if it would be possible to disable the automatic quarantining of detected items, which had been necessary in the last test.

The performance tests ran through fairly smoothly but not super fast, with some slowish scan times and fairly hefty lag on access – much improved on repeat attempts it should be noted. Resource usage measures were about average for the group tested.

Detection scores on demand were splendid, with a particularly strong showing in the RAP sets. This was something of a surprise after a less-than-stellar performance here last time around. The WildList was handled with aplomb in this mode, but on access things did not go well: when faced with even the smallest handful of infected samples in a short period of time the product suffered serious errors, often rendering the whole system

barely responsive. Eventually, after several attempts on numerous systems with identical results, we were forced to abandon attempts to gather on-access scores completely. To add insult to injury, a couple of false positives were picked up in the clean sets, thus sealing *Sunbelt's* fate for this month.

Symantec Endpoint Protection

11.0.5002.333

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.26%
Worms & bots	99.26%	False positives	0

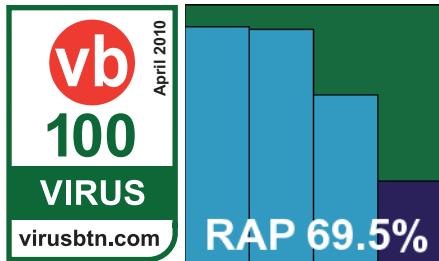
Once again we return to one of our regulars, with *Symantec's* corporate edition back in the test. The product is routinely

sent in the form of an archive containing a full set of contents from the install CD, so the submission measures over 500MB but includes numerous components not required here; the offline updater came in at 62MB. The set-up process is a little lengthy, mainly thanks to the other options available in the package, with some stately language to accompany the pace, but it's all done within a few minutes and rounds itself off with a reboot which, we are imperiously informed, we may delay one time only.

The *Symantec* product is pretty familiar to us by now, with a soft and curvy main GUI concealing the much more business-like configuration controls buried within. These provide for excellent depth of adjustment, and are generally logically designed and easily navigated.

Performance tests showed both scan times and file access lags on the less exciting side of medium, with resource consumption also tending more towards the heavy than the light, but stability was rock-solid throughout.

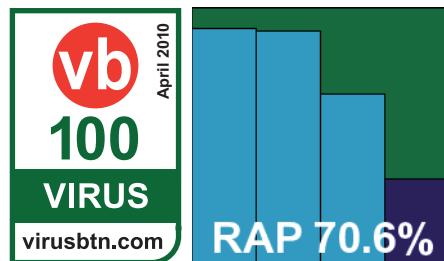
Detection rates were generally excellent in most of the sets, with a fairly steep drop in the RAP sets from lofty heights in the reactive portions to much lower figures in the proactive week, reflecting *Symantec's* focus on a dynamic and reputation-based protection system which we are not currently in a position to exercise properly. With the WildList covered without a blemish however, and no problems in the clean set either, *Symantec* has no problems achieving the required standard for yet another VB100 award.



Symantec Norton Antivirus 17.5.0.127

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.69%
Worms & bots	99.59%	False positives	0

Symantec's home-user brand *Norton* is pretty much ubiquitous around the world and one of the most widely used security



solutions. *Symantec* has in the past tended to focus on submitting its corporate products for VB100 testing, but has finally been persuaded to submit the retail editions as well. The 84MB main installer runs through in moments, and uses the same updater tool as the corporate product; we gave it a reboot just to make sure the updates had fully kicked in.

The interface took a few moments 'initializing', but when it appeared generally impressed with the slick and stylish design and a surprising depth of configuration and options. Running through the tests proved no problem, with the clear logging a special bonus for us. On-demand scanning speeds were pretty decent, and much improved on second and subsequent runs too, and while the product's lag times were a tad lighter than those of its corporate cousin, use of RAM and CPU cycles was perhaps a smidgen higher.

In detection results, the scores were slightly higher across the board – presumably with some heuristics set slightly higher by default, so again excellent numbers are seen in most sets, bar the proactive week of the RAPS. The core certification sets presented no problems, and *Norton* is also a worthy winner of a VB100 award.

Trustport Antivirus 2010 5.0.0.4092

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.81%
Worms & bots	99.94%	False positives	0

Trustport has been doing pretty well in our tests lately, having settled into a twin-engine approach which seems to suit it nicely. The latest build was sent in as a 151MB executable, and ran through in a fairly large number of stages but not taking too much time. On completion no true central GUI is provided, but rather a cluster of control and configuration screens, of which the central control module

is the closest to a main interface. After a few moments figuring out where everything is this proves a pretty usable method of control, with just about everything one could want within reasonably easy reach.

Performance figures were not the best, as one would expect from a dual-engine product, with some slow scanning times, heavy use of system resources and long lags accessing files, but this is made up for as usual by superb detection rates. All three reactive weeks of the RAP sets were treated with disdain, and even the proactive week presented few difficulties.

The WildList set was demolished just as easily, and with no false alarms in the clean sets *Trustport* walks away with another VB100 award.

VirusBuster Professional 6.2.51

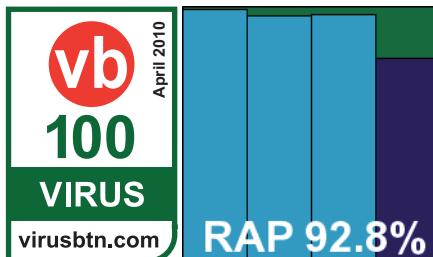
ItW	100.00%	Polymorphic	89.11%
ItW (o/a)	100.00%	Trojans	89.61%
Worms & bots	97.88%	False positives	0

At last we get round to the progenitor of the engine which seems to have been behind half the products in this month's test. Having

looked at both its detection and performance scores already this month, and even its interface in different colours, there seems little more to say, other than that it installed quickly and easily, has a slightly overcomplicated GUI, ran swift and light, got pretty decent scores across the sets, and had no problems achieving a VB100 award. Well done to *VirusBuster*, as well as to its many partners.

Webroot AntiVirus with SpySweeper 6.1.0143

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	95.92%
Worms & bots	99.30%	False positives	0



Finally we reach the last product on this month's list; *Webroot*'s latest incarnation comes as a 41MB installer and a 63MB updater

package, which installs pretty swiftly, with the offer of a toolbar and only two further prompts until a reboot is demanded.

The interface remains reasonably usable if a little cluttered in places, with some of the configuration seemingly deliberately concealed in the shrubbery. The performance tests showed rather slow scanning speeds, heavy file access lag times and sizeable resource consumption. These impressions were confirmed in the infected sets, where the product's greenish, yellowish hues and angular shapes make the user feel like they are pushing a boxcar full of angry cows through a custard lake.

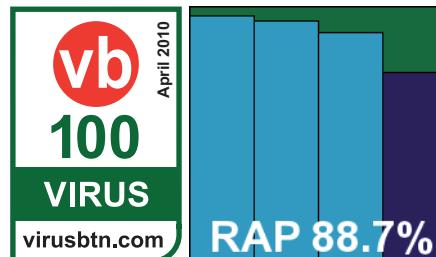
As scans progressed the system gradually wound itself into a pitiful state, with windows taking longer and longer to refresh. Eventually the first scan reached its end, and the button marked 'deselect all' was followed, through lack of any alternative, by that marked 'quarantine selected'; this confused matters even further and ended up hanging the system entirely, requiring a forced restart.

Of course, most users would be unlikely to find themselves in such a situation, and after nursing the product in a similar fashion through the rest of our tests, and finding no problems in the WildList or clean sets, and some excellent detection rates elsewhere, *Webroot* is deemed worthy of the last of this month's record crop of VB100 awards.

CONCLUSIONS

First, if you have made it this far, congratulations – it has been a long haul for us, and now you have joined us on our epic journey through the highs and lows of the current anti-malware market. With such a huge selection of products there are of course many notable trends and developments to comment on, but with so much already said I'll limit myself to the most vital and obvious.

The first thing that springs to mind looking over these results is the continuing trend for the relicensing of engines by OEM product makers, and the gradual climb to dominance of certain players in these markets. Of the 60 products in this month's test, nine were underpinned by the same engine, while another engine provided the



technology for four and another for three more. This trend presents some interesting points as we look to move our testing towards more labour- and time-intensive real-world methodologies, where the number of products that can be tested will be limited by the available resources. It seems vital that we continue to provide VB100 testing for this wealth of products, to ensure the public have a trustworthy source of information on their performance levels, but it also seems that the level of detail currently included could be trimmed somewhat, to allow us to carry out other duties.

A lot of the burden this month has been imposed by difficult and recalcitrant products. *Windows XP* is a mature and common platform, so we assume that products will support it solidly and without difficulty. However, this month's test has seen quite scandalous levels of instability, crashing, hanging, errors and shutdowns, failure to bear up under even the slightest strain and, in two separate cases, complete failure to provide any on-access protection at all. In this day and age users expect and deserve better; many of the companies here this month would do well to give their QA processes a thorough overhaul before doing anything else.

Of course, there have also been the usual problems with failure to detect WildList samples and with false positives in the clean set. This month's haul of FPs has included some fairly glaring examples, including several versions of *Adobe's Reader* – one of the most common pieces of non-*Microsoft* software on the planet – as well as samples from *Microsoft* itself and other major providers including *Google* and *Sun*. In the race to expand detection by ever more aggressive heuristics, vendors must strive to balance their detections with the false alarm rate, and in some cases this balance is not quite being maintained.

In the WildList, the deadly *Virut* once again took its casualties. These complex polymorphic viruses are proving challenging for labs to detect fully and accurately – which is exactly as their makers intended. Hopefully with our help and encouragement we can make a contribution to improving things on this score – all vendors with issues should already have been provided with samples and information, and we will continue to work with them to ensure any problems are fully rectified.

And now our work here is almost done. We look forward to a rather quieter comparative next time around.

Technical details:

All performance tests were run on identical systems with *AMD Athlon64 X2 Dual Core 5200+* processors, 2GB RAM, dual 80GB and 400GB hard drives, running *Microsoft Windows XP Professional, Service Pack 3*. Some additional tests were run on secondary systems with *AMD Phenom X2 Dual Core 550* processors, 4GB RAM, dual 40GB and 1TB hard drives, also running *Microsoft Windows XP Professional, Service Pack 3*.

APPENDIX – TESTING METHODOLOGY AND INTERPRETATION OF RESULTS

The testing methods of the VB100 are provided in some detail on our website (<http://www.virusbtn.com/vb100/about/100procedure.xml>), but as we have made a few additions to the data we provide in recent months it seems appropriate to provide an overview of how we go about testing products and gathering information on them, as well as how the figures and graphs we provide are intended to be used.

VB100: WildList and clean set

The VB100 certification scheme rests on two main areas of testing: the WildList set of malicious samples – verified as active malware commonly seen infecting the systems of real-world users – and our clean sets. The clean sets consist of our speed sets – compiled by harvesting all files from a selection of machines and organizing them by file type – plus a large set of known-good files from a broad selection of sources including magazine cover CDs, popular download sites, pre-installed OEM machines, hardware manufacturers' driver and update sites and others. We try to ensure that the test set is reasonably representative of the real world without penalizing products for what might be considered minor infractions, unlikely to inconvenience most users. We endeavour to select samples of files that are likely to have a significant user base, excluding more obscure and uncommon packages. We also try to exclude packages that make use of unsavoury activities such as harvesting user data without adequate permission, and also avoid most security-related software, in particular anti-malware software.

Currently, the process of assigning a significance value to non-malicious software is more of an art than a science. While the user-base of some types of software can be divined from download statistics on popular freeware sites, such data is not freely available for all types of file. Likewise, measuring the impact on the user of a false positive is not trivial. We have been investigating various methods of classifying files on both these scales for some time, and with some work being done by the AMTSO group on exactly these issues, we hope to be able to introduce a more clearly documented selection process for our clean sets in the near future.

The WildList test set is compiled on much more rigid grounds; each item on the monthly lists produced by the *WildList Organization* is represented by a single control sample, carefully vetted and confirmed by the list's operators, and each of these control samples is separately validated and replicated by our own lab staff. In most cases the malware replicates either on or off the local system, producing a file that is identical to the control sample. In such cases the

replicated file alone is used as our representative sample. However, in some cases, multiple file extensions may be used by a single item (for example, filling a shared folder with several copies of the same file, but using various different filenames intended to lure people into opening them, with different extensions used to conceal the files' purpose and potential). In such cases several copies of the sample are added to our test set, including each extension it is seen using. Additional files – such as dropped or downloaded files or loader files required to launch a control sample – are not included in the core set. In the case of file infectors, the original control sample is used to create replicants, infecting a range of 'goat' files; for polymorphic samples, this is done many times, with a limit of 2,500 representative samples of any given virus strain included in the official set; the original control sample is not used. When completed, the set should contain only samples which can cause an infection exactly as the control samples would cause.

The WildList is due for some updating to include a wider range of sample types very soon. When this expansion comes into play, we expect to adjust our replication process to focus simply on validation, as most samples in any such list will have no internal replication mechanisms; we also expect the list to provide an even tougher challenge to product developers than it already does.

The VB100 certification requirements demand that products detect the entire WildList set, both on demand and on access, without generating any false positives in the clean set. A certified product is simply one which has met these requirements; it does not imply that the product is superb if it has passed a single certification run, or that it is useless if it has failed to meet the requirements in a single run. On its own, a single VB100 pass can only show that a product is legitimate and competently put together; that its makers know what they are doing and have good access to the most common samples likely to affect their users. For a more complete picture of the quality of a product, our readers need to look at several reviews and monitor the performance of products over time to get an idea of the consistency and reliability of a solution. For this reason, we provide detailed archive data of all our tests on our website, along with summary information on each product's performance history (see <http://www.virusbtn.com/vb100/archive/>).

Additional data

To support this insight into quality as well as competence, each comparative review provides a range of information to complement the basics of the certification scheme. These extras include detection rates over our polymorphic, worms and bots, and trojans test sets and products' RAP scores. The RAP scores are based on detection rates for four sets of samples compiled over the three weeks prior to a test

deadline and one week after product submission, thus giving an idea of products' reactive and proactive detection abilities. The samples used in the RAP sets come from our daily feeds from various sources including malware labs from around the world and other independent collections, and exclude adware and 'potentially unwanted' items. They also currently exclude true viruses due to time constraints in performing proper replication of such samples. As part of the set-building process, we try to classify samples and select those with the greatest prevalence. This classification is currently based on our prevalence data, which is compiled from reports provided by a number of bodies including several major security firms as well as independent groups and government organizations.

Most of our main test sets are performed both on demand and on access. The on-demand tests for all our sets are run where possible as a standard scan from the product interface. Where the interface does not provide the option of scanning a single folder, a context-menu ('right-click') scan is substituted. This scan is performed with the default settings; the only adjustments made are to ensure that full and detailed logging is kept, and where possible to disable the automatic cleaning, deletion or quarantining of detected items. For on-access tests, an opener tool is run over the set performing simple file-open actions, and taking the MD5 checksum of the file if permitted to access it. For products which do not check files on-read, files are copied from one drive of the machine, or from a remote system, to the system partition to measure on-write detection. Again, default settings are used as far as possible, with logging and auto-cleaning the only areas adjusted. The RAP and main clean sets are generally only scanned on demand, under the assumption that, in general, on-demand scanners use more thorough defaults than on-access ones and any detection or false alarms made on access would also appear on demand. When products cannot be made to produce adequate logs on demand, or otherwise fail to satisfy our requirements in this way, on-access runs over these sets may be substituted.

The same methods are applied to the performance tests, most of which are run from DOS batch scripts which control the file-accessing tools and performance monitors used to gather information for our charts and graphs.

Of course, all of this only scratches the surface as far as modern security solutions are concerned, with a wide range of technologies remaining untouched by these methodologies. We continue to investigate ways of expanding our testing to include a full range of techniques including live online resources and dynamic monitoring. However, we have no doubt that simplified tests of core functionality such as provided here – covering a wide range of solutions and a broad depth of threats – will continue to be useful to ensure the legitimate can be discerned from the devious, the rogues from those of good pedigree.

END NOTES & NEWS

The New York Computer Forensics Show will be held 19–20 April 2010 in New York, NY, USA. For more information see <http://www.computerforensicshow.com/>.

Infosecurity Europe 2010 will take place 27–29 April 2010 in London, UK. For more details see <http://www.infosec.co.uk/>.

The 19th EICAR conference will be held 10–11 May 2010 in Paris, France with the theme 'ICT security: quo vadis?'. For more information see <http://www.eicar.org/conference/>.

The fourth annual Counter-eCrime Operations Summit (CeCOS IV) will take place 11–13 May 2010 in São Paulo, Brazil. For details see http://www.apwg.org/events/2010_opSummit.html.

NISC11 will be held 19–21 May 2010 in St Andrews, Scotland. Interest in attending can be registered at <http://nisc.org.uk/>.

The International Secure Systems Development Conference (ISSD) takes place 20–21 May 2010 in London, UK. For details see <http://issdconference.com/>.

CARO 2010, the 4th International CARO workshop will take place 26–27 May 2010 in Helsinki, Finland. The workshop will focus on the topic of 'Big Numbers'. For more information see <http://www.caro2010.org/>.

CSI SX – Security for Business Agility takes place 26–27 May 2010 in San Francisco, CA, USA. The event will address the challenges of managing security in an increasingly mobile business environment. For details see <http://www.csixs.com/>.

Security Summit Rome takes place 9–10 June 2010 in Rome, Italy (in Italian). For details see <https://www.securitysummit.it/>.

The 22nd Annual FIRST Conference on Computer Security Incident Handling takes place 13–18 June 2010 in Miami, FL, USA. For more details see <http://conference.first.org/>.

The Seventh International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) will take place 8–9 July 2010 in Bonn, Germany. For more information see <http://www.dimva.org/dimva2010/>.

CEAS 2010 – the 7th annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference – will be held 13–14 July 2010 in Redmond, WA, USA. For details see <http://ceas.cc/>.

Black Hat USA 2010 takes place 24–29 July 2010 in Las Vegas, NV, USA. DEFCON 18 follows the Black Hat event, taking place 29 July to 1 August, also in Las Vegas. For more information see <http://www.blackhat.com/> and <http://www.defcon.org/>.

The 19th USENIX Security Symposium will take place 11–13 August 2010 in Washington, DC, USA. For more details see <http://usenix.org/>.

RSA Conference Japan will be held 9–10 September 2010 in Akasaka, Japan. For details see <http://www.smj.co.jp/rsaconference2010/english/index.html>.

VB2010 will take place 29 September to 1 October 2010 in Vancouver, Canada. For the full conference programme including abstracts for all papers and online registration, see <http://www.virusbtn.com/conference/vb2010>.

Hacker Halted USA takes place 9–15 October 2010 in Miami, FL, USA. A call for papers is now open. For more information see <http://www.hackerhalted.com/>.

RSA Conference Europe will take 12–14 October 2010 in London, UK. Registration opens in May. For details see <http://www.rsaconference.com/2010/europe/index.htm>.

The fifth annual APWG eCrime Researchers Summit will take place 18–20 October 2010 in Dallas, TX, USA. eCRS 2010 will bring together academic researchers, security practitioners, and law enforcement to discuss all aspects of electronic crime and ways to combat it. For more information see <http://www.ecrimeresearch.org/>.

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 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.