

virus

BULLETIN

Fighting malware and spam

CONTENTS

- 2 **COMMENT**
PWN2KILL, EICAR and AV: scientific and pragmatic research
- 3 **NEWS**
SonicWALL in latest acquisition
VB2010 early birds
Erratum: VBSpam comparative review May 2010
- 3 **VIRUS PREVALENCE TABLE**
- 4 **TECHNICAL FEATURE**
Anti-unpacker tricks – part nine
- 7 **FEATURE**
What's the deal with sender authentication? Part one
- 12 **CONFERENCE REPORT**
EICAR 2010: rainy days in Paris
- 14 **COMPARATIVE REVIEW**
VB100 – Windows Server 2008 R2
- 37 **END NOTES & NEWS**

IN THIS ISSUE

THE DARK SIDE

'Crossing over to the Dark Side of the customer/vendor divide has made me increasingly aware of just how bad "bad" can be.' David Harley comments on the recent 'PWN2KILL' challenge and the place of scientific and pragmatic research in AV.

page 2

EVALUATING AUTHENTICATION

Sender authentication is a hot topic in the world of email. It has a number of uses and a number of suggested uses. Which ones work in real life? Which ones don't quite measure up? Can we use authentication to mitigate spoofing? Can we use it to guarantee authenticity? And how do we authenticate email, anyway? Terry Zink provides the answers to these questions and more.

page 7

VB100 CERTIFICATION ON WINDOWS SERVER 2008

VB's lab team battled with inconsistencies and unreliable behaviours in this month's VB100 test, but managed eventually to pull some meaningful results together. John Hawes names and shames the badly behaved products and reveals this month's VB100 winners.

page 14





‘Crossing over to the Dark Side of the customer/vendor divide has made me increasingly aware of just how bad “bad” can be.’

David Harley, ESET

PWN2KILL, EICAR AND AV: SCIENTIFIC AND PRAGMATIC RESEARCH

I guess no one joins the anti-malware industry for a peaceful working environment, a celebrity lifestyle, or a need to be loved by the world in general and other security professionals in particular. (If they do, they probably move quickly on to a role with a more congenial working environment, such as traffic warden, flak jacket model, or leader of the Labour Party.) And while I’ve visited the topic of AV’s bad reputation before (see *VB*, November 2006, p.6), crossing over to the Dark Side of the customer/vendor divide (my name is David, but you can call me Darth) has made me increasingly aware of just how bad ‘bad’ can be.

At the first International Alternative Workshop on Aggressive Computing and Security (iAWACS), held in 2009 by the École Supérieure d’Informatique, Electronique, Automatique (ESIEA), a ‘PWN2RM’ challenge was held, in which a number of anti-malware products were installed on a machine and attempts were made (while logged in as administrator) to disable them. The attempts were successful in most cases (see <http://www.esiea-recherche.eu/data/pwn2rm.pdf>.) An interesting idea, and though a compromise with physical access and administrator privileges doesn’t necessarily

translate easily into an automated malware attack, and still less into a meaningful metric for ranking products, the disabling of security processes is a very common feature of malware attacks.

At the second workshop, held last month, the ‘PWN2KILL’ challenge took the idea several steps further. The rules of the contest stated that its aim was to perform a ‘comparative evaluation of commercial anti-virus software’, using a variety of attacks. The slides relating to the 2010 challenge are available at ESIEA’s website, and the number of vendor fails recorded is pretty worrying. The technical briefings for some of the attacks are very sparse on detail, so I guess the vendor community will have to wait until the attack code becomes available before we can fully evaluate and learn from the challenge.

Until then, it would be premature to sound the death knell of anti-malware on the basis of this challenge. Scientific method is a Good Thing, but it doesn’t matter whether the methodology is reproducible if it isn’t right. A paper presented by Dechau *et al.* at last month’s EICAR conference focused on one of the attacks used in PWN2KILL and inspired heated discussion among delegates. Defensibly enough, the students were restricted to attack code that was based on attempting to bypass anti-virus in order to execute the EICAR test file. However, that particular combination of methodology and sample created problems, since some of the paper’s conclusions were based on non-detection of modified versions of the EICAR test file – in violation of the test file’s specifications (see *VB*, June 2003, p.13 and EICAR’s own description). Vendors were understandably disturbed at being penalized for conforming strictly to the specifications. Nonetheless, it would be a pity to focus on that hiccup rather than on the message behind the presentation, as voiced with passion by EISEA’s Eric Filiol and EICAR chairman Rainer Fahs.

They’re not alone in their disappointment that anti-malware products cannot provide anything like 100% detection and resistance to attacks. As researchers, we can argue that we have never claimed that anti-virus kills 100% of malware, let alone other attacks; that we (largely) abandoned signature detection for algorithmic methods years ago; that we’ve long advocated multi-layered defence; and that a business cannot survive on R&D without marketing. But we need to understand the insights and needs of academics and customers with critical systems, just as they need to understand our need to deliver pragmatic, market-driven solutions.

In the meantime, I’m considering changing my name from Darth to Aunt Sally.

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Consulting Editors:

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, USA*

NEWS

SONICWALL IN LATEST ACQUISITION

The last five weeks have seen a flurry of activity in acquisitions and mergers in the security field. In the most recent announcement, network security systems provider *SonicWALL, Inc.* has agreed to be acquired by an investor group led by private equity firm *Thoma Bravo* in a deal worth around \$717 million. *SonicWALL's* shareholders will receive \$11.50 in cash for each share of common stock they hold, with the purchase expected to complete in late September.

Other recent activity has seen a major share of *Sophos* sold to private equity firm *APAX Partners*, Slovakian anti-spam firm *COMDOM Software* acquired by fellow Slovakian security vendor *ESET* and a trio of encryption-related purchases by *Symantec*, which has acquired *PGP*, *GuardianEdge* and *VeriSign's* authentication services business.

VB2010 EARLY BIRDS

Register for VB2010 before 15 June to receive an early bird discount. The programme – which covers subjects including: botnets, cyberterrorism, blackhat SEO, targeted attacks, Mac threats, anti-spam testing, anti-malware testing, in-the-cloud scanning and more – can be viewed at <http://www.virusbtn.com/conference/vb2010/programme/>. VB2010 takes place 29 September to 1 October 2010 in Vancouver, Canada.

ERRATUM: VBSPAM COMPARATIVE REVIEW MAY 2010

Careful scrutiny of the results of the May 2010 VBSpam comparative review (see *VB*, May 2010, p.24) has revealed a minor bug in the scripts used to calculate the products' performance. As a result of this bug, the spam catch rates of six products were under-reported. False positive rates were not affected, and the ranking of the products by their final score remains the same. The correct results can be found in the table below:

	FP rate	False negatives	True positives	SC rate	Final score
BitDefender	0.14%	943	246372	99.62%	99.21
FortiMail	0.23%	4730	242585	98.09%	97.40
McAfee EWS	0.18%	2856	244459	98.85%	98.30
McAfee Email Gateway	0.50%	1481	245834	99.40%	97.90
Sophos	0.23%	762	246553	99.69%	99.01
SpamTitan	0.14%	3609	243706	98.54%	98.13

VB offers its apologies to the vendors for these errors.

Prevalence Table – April 2010^[1]

Malware	Type	%
Autorun	Worm	10.73%
VB	Worm	7.78%
Conficker/Downadup	Worm	6.52%
Adware-misc	Adware	4.59%
FakeAlert/Renos	Rogue AV	4.37%
OnlineGames	Trojan	4.20%
Injector	Trojan	4.04%
Agent	Trojan	3.94%
Heuristic/generic	Virus/worm	3.47%
Delf	Trojan	3.38%
Wintrim	Trojan	2.44%
Zbot	Trojan	2.36%
Heuristic/generic	Trojan	2.14%
Small	Trojan	1.97%
Virtumonde/Vundo	Trojan	1.73%
Downloader-misc	Trojan	1.69%
Heuristic/generic	Misc	1.63%
Virut	Virus	1.61%
Autolt	Trojan	1.58%
Hupigon	Trojan	1.56%
Alureon	Trojan	1.45%
Encrypted/Obfuscated	Misc	1.30%
Kryptik	Trojan	1.30%
Peerfrag/Palevo	Worm	1.14%
Bancos	Trojan	1.07%
Crypt	Trojan	1.05%
Tanatos	Worm	0.98%
Istbar/Swizzor/C2lop	Trojan	0.97%
Exploit-misc	Exploit	0.97%
Sality	Virus	0.95%
Armadillo	Packer	0.94%
Bifrose/Pakes	Trojan	0.91%
Others ^[2]		15.28%
Total		100.00%

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

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

TECHNICAL FEATURE

ANTI-UNPACKER TRICKS – PART NINE

Peter Ferrie
Microsoft, USA

New anti-unpacking tricks continue to be developed as older ones are constantly being defeated. Last year, a series of articles described some tricks that might become common in the future, along with some countermeasures [1–9]. Now, the series continues with a look at tricks that are specific to debuggers and emulators.

In this article we look at anti-debugging tricks including self-modifying code, selectors, RDTSC and *Syser* plug-ins.

Unless stated otherwise, all of the techniques described here were discovered and developed by the author.

1. SELF-MODIFYING CODE

If a debugger uses the common ‘CC’ opcode (short-form ‘INT 3’ instruction) to place breakpoints during step-over, then it is vulnerable to self-modifying code that removes the breakpoint. As a result, the debugger’s control of the process will be lost. Example code looks like this:

```
mov al, 90h
xor ecx, ecx
inc ecx
mov edi, offset l1
rep stosb
l1: nop
```

Of course, there are a couple of variations, such as using ‘rep movs’ instead of ‘rep stos’. The direction flag can be involved, too, in such a way that at a glance, the overwrite might be overlooked. Example code looks like this:

```
mov al, 90h
push 2
pop ecx
mov edi, offset l1
std
rep stosb
nop
l1: nop
```

As noted in a previous paper [1], single-stepping is also vulnerable to a variation of this technique, if the overwrite includes the string instruction itself.

The solution to this problem is to use hardware breakpoints instead, though this workaround has its own set of problems. What is not immediately obvious in this example is that the debugger has no way of knowing if the breakpoint that it places at a location is the one that is executed. If the application removes the breakpoint, it can restore it afterwards, and then jump to the address to execute that

breakpoint. The debugger will see the breakpoint exception that it was expecting, and behave as normal. Example code looks like this:

```
mov al, 90h
11: xor ecx, ecx
inc ecx
mov edi, offset l3
12: rep stosb
13: nop
cmp al, 0cch
14: mov al, 0cch
jne l1
15: ...
```

In this example, stepping over the instruction at l2 will allow the code to reach l4. This will cause the breakpoint to be replaced by l2 and executed by l3. The debugger will then regain control. At that time, the only obvious difference will be that the AL register will hold the value 0xCC instead of 0x90, which will allow l5 to be reached in what appears to be one pass instead of two. Of course, much more subtle variations are possible, including the execution of entirely different code-paths.

A variation of the technique can be used as a simple method to detect the presence of a debugger. Example code looks like this:

```
xor ecx, ecx
inc ecx
mov esi, offset l1
lea edi, [esi + 1]
rep movsb
11: mov al, 90h
cmp al, 0cch
je being_debugged
```

2. SELECTORS

Selector values look stable, but they are actually volatile. Specifically, a selector value can be set within a thread, but it might not hold its value for very long. Certain events will cause the value to be changed back. One such event is an exception. In the context of a debugger, the single-step exception can cause some unexpected behaviour. Example code looks like this:

```
xor eax, eax
push fs
pop ds
11: xchg [eax], c1
xchg [eax], c1
```

Single-stepping through this code will cause an access violation exception at l1 because the DS selector will be restored to its default value even before l1 is reached.

A variation of this technique detects the single-step event in a less obvious fashion, simply by checking if the assignment was successful. Example code looks like this:

```

push 3
pop gs
mov ax, gs
cmp al, 3
jne being_debugged

```

This technique is used by Zlob. However, this code is vulnerable to a race condition caused by a thread-switch event, because a thread-switch event also results in the selectors being restored to their default values.

A variation of this technique waits intentionally for a thread-switch event to occur, in order to trigger the effect. Example code looks like this:

```

push 3
pop gs
11: mov ax, gs
shr ax, 1
jb 11

```

This technique is used by Zlob. The code expects the GS selector to become zero again when a thread-switch occurs. This technique works only on the 32-bit versions of *Windows*. It is invalid for 64-bit versions of *Windows* because the GS value on those platforms has bit 0 set, so the loop never exits.

This technique is actually a variation of an anti-emulation trick first seen in 2000, which has been rediscovered. At that time, selectors were not well-supported, so assignments often misbehaved or were ignored completely. Example code looks like this:

```

mov eax, ds
xor ebx, ebx
mov ds, bx
mov ecx, ds
cmp ecx, eax
;detect selector not updated
je being_debugged

```

This technique was first used by Moridin, but Moridin simply checked if the selector held its value when assigned the same value. Example code looks like this:

```

mov edi, ds
push edi
pop ds
mov eax, ds
cmp edi, eax
jnz being_debugged

```

3. RDTSC

When the system is powered-on, a timer starts to run, whose value can be queried by the RDTSC instruction. Given how long a typical system takes to boot, and how long it takes for an arbitrary application to be launched, the value that is returned by the RDTSC instruction should be at least *x*, where *x* is a quite large value. Unfortunately, it is common for some hiding tools to intercept the RDTSC instruction,

and to return a small incrementing value instead, which reveals their presence. It might be better to begin with the real value, but there is a problem with that, too. The problem is that if code knows that it is running at start-up, then too large a value reveals that it was not executed in the usual way. This technique could be used to determine the execution state, instead of checking from which directory the application was launched, for example.

4. DATA-EXECUTION PREVENTION (DEP)

Data-Execution Prevention is intended to disallow the execution of code from pages that are not marked explicitly as executable. However, for compatibility reasons, the protection is not as secure as it sounds. If code begins in an executable section, and jumps into a non-executable section with DEP enabled, then an exception will occur as expected. However, if execution begins in a non-executable section, then the file will run with DEP silently disabled. This is true even if the code jumps into an executable section, and then back into a non-executable section.

Turbo Debug32 (and possibly other debuggers) allows breakpoints to be executed in non-executable pages, even in cases where the execution of any other instructions would cause a DEP exception.

5. SYSER PLUG-INS

Some packers have been written to detect *Syser*, so a plug-in (only one so far) has been written to attempt to hide *Syser* from those packers. The following is a description of that plug-in, along with its very serious bug.

5.1 HideSyser

HideSyser hooks the *ntoskrnl* *NtCreateFile()* function by overwriting the first five bytes of the handler to point to the driver code, and patching one byte at a fixed offset within the routine. The plug-in works only on *Windows XP*. When run on any other platform, *HideSyser* will cause a kernel-mode crash (blue screen).

The crash is caused by the one-byte patch, which is intended to disable the popping of a frame pointer. This disassembly shows more:

```

mov edi, edi
push ebp
mov ebp, esp
mov edx, [ebp+10]
...
push ebx
push esi
push edi
...
push d [ebp+30]
push d [ebp+2c]

```

```

push d [ebp+28]
push d [ebp+24]
push d [ebp+20]
push d [ebp+1c]
push d [ebp+18]
push d [ebp+14]
push edx
push d [ebp+C]
push d [ebp+8]
call ntcreatefileplus5
pop edi
pop esi
pop ebx
pop ebp
ret 2Ch

```

As we can see, the call to the original `ntoskrnl NtCreateFile()` function intends to use the stack frame that *HideSyser* creates, and if the frame were popped, then the stack would be unbalanced.

However, the patch can be made completely unnecessary by changing the way in which the original `ntoskrnl NtCreateFile()` function is called. Example code looks like this:

```

mov edi, edi
push ebp
mov ebp, esp
...
xor eax, eax
jmp ntcreatefileplus5

```

This allows the API to use the original caller's parameters, thus avoiding the need to push them again. The `'xor eax, eax'` line is required to support *Windows NT4* and *Windows 2000*. As a result, this code would work on all versions of *Windows*.

When running on *Windows XP*, the driver code checks for the names `'\Device\Syser'`, `'\Device\SyserBoot'`, `'\Device\SyserDbgMsg'`, `'\.\syser'` and `'\??\syser'`, and returns failure if any of them are matched.

The author of *HideSyser* did not respond to the report.

6. OLLYDBG-SPECIFIC

OllyDbg was described in a previous paper [6]. The following is a description of a bug that had been discovered since that paper was published.

6.1 Step-over

When *OllyDbg* is asked to step over an instruction, it checks if stepping over the instruction is a meaningful request. *OllyDbg* allows stepping over only the `CALL, REP[[N]E] <string>`, and `LOOP[[N]E]` instructions. However, there is a problem if an address-size override is used. Example code looks like this:

```

xor ebx, ebx
push 40h
mov eax, esp
push 3000h
push esp
push ebx
push eax
push -1 ;GetCurrentProcess()
call NtAllocateVirtualMemory
mov b [ebx], 0c3h
call d [bx+1]

```

11: ...

OllyDbg knows that the instruction can be stepped over, but it is confused by the prefix and so does not place any breakpoint at all. As a result, execution resumes freely from 11. This bug was fixed in *OllyDbg* v2.00.

The next part of this series will concentrate on *OllyDbg* plug-ins.

The text of this paper was produced without reference to any Microsoft source code or personnel.

REFERENCES

- [1] Ferrie, P. Anti-unpacker tricks. <http://pferrie.tripod.com/papers/unpackers.pdf>.
- [2] Ferrie, P. Anti-unpacker tricks – part one. *Virus Bulletin*, December 2008, p.4. <http://www.virusbtn.com/pdf/magazine/2008/200812.pdf>.
- [3] Ferrie, P. Anti-unpacker tricks – part two. *Virus Bulletin*, January 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200901.pdf>.
- [4] Ferrie, P. Anti-unpacker tricks – part three. *Virus Bulletin*, February 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200902.pdf>.
- [5] Ferrie, P. Anti-unpacker tricks – part four. *Virus Bulletin*, March 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200903.pdf>.
- [6] Ferrie, P. Anti-unpacker tricks – part five. *Virus Bulletin*, April 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200904.pdf>.
- [7] Ferrie, P. Anti-unpacker tricks – part six. *Virus Bulletin*, May 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200905.pdf>.
- [8] Ferrie, P. Anti-unpacker tricks – part seven. *Virus Bulletin*, June 2009, p.4. <http://www.virusbtn.com/pdf/magazine/2009/200906.pdf>.
- [9] Ferrie, P. Anti-unpacker tricks – part eight. *Virus Bulletin*, May 2010, p.4. <http://www.virusbtn.com/pdf/magazine/2010/201005.pdf>.

FEATURE

WHAT'S THE DEAL WITH SENDER AUTHENTICATION? PART 1

Terry Zink
Microsoft, USA

Sender authentication is a hot topic in the world of email. It has a number of uses and a number of suggested uses. Which ones work in real life? Which ones don't quite measure up? Can we use authentication to mitigate spoofing? Can we use it to guarantee authenticity? And how do we authenticate email, anyway?

The email system is modelled on the real-life postal mail system – which has both strengths and weaknesses. Let's suppose for the sake of argument that I have a best friend whose name is Tony. Let's also suppose that I live in the Seattle area in Washington in the US, and that Tony has recently moved to Sacramento, California. The only way we can communicate is via postal mail (neither of us knows how to use the Internet, we both refuse to pay for telephone services and we don't know how to use smoke signals). One day, I receive what appears to be a handwritten letter. I don't recognize the handwriting as Tony's because I never paid attention to his writing, but the envelope is addressed to me and the return address in the top left corner shows Tony's name and an address in Sacramento, California. If I had no other information to go on, I would assume that this letter really was from Tony.

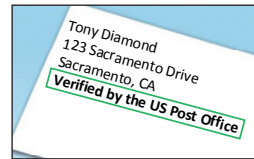
On opening the envelope, however, I find that it is not a personal letter at all but an advertisement for a diploma from an online university. They're offering a good deal – only \$99 for a degree – but I am annoyed because someone has falsely sent me a letter in my friend's name.

What would be useful would be if some authority traced the letter from Tony's home in California to my place in Washington. What if the Post Office placed a 'verified' stamp against the return address in the top-left side of the envelope?

In other words, what if the Post Office guaranteed that the message came from where it claimed to come from by going to Tony's place directly, verifying that the return address was correct, and then indicating with a stamp of authenticity that this was the originating address of the letter? If that were the case, then all I would have to do would be to look for that US Post Office stamp to be sure of who my mail was from.

EMAIL

Email, in its simplest form, is like postal mail. Anyone can send mail to anyone else, and can send mail *as* anyone else. My somewhat good friend Frank can send me an email,



pretending to be Tony, and the email will reach me. I will initially think that the email is from Tony, but in reality it is not.

I remember back in my university days when we learned how to send 'fake' email. The basic idea behind this was that we could send email to whomever we wanted and specify any return address we wanted, even from a domain that didn't exist. So, I sent a few fake messages to family and friends of mine. Oh, what great fun I had! It didn't occur to me that ethically challenged people would exploit this for nefarious purposes.

Unfortunately, the type of postal authority I described above, which guarantees the authenticity of the originating point of a letter, doesn't exist in real life. Fortunately, in email we can do better.

To begin with, we need to understand how email gets from point A to point B. Email travels through connections called ports. To keep track of all the different connections, the ports are numbered. Port 25 is the one that is used to transmit and receive email. When a computer attempts to transmit email, it opens a connection to port 25 and attempts to transmit using the Simple Mail Transfer Protocol, or SMTP.

This whole transaction depends on five commands which constitute the core of SMTP: HELO, MAIL FROM, RCPT TO, DATA and QUIT.

1. HELO identifies the sending machine. 'HELO mail.tzink.com' should be read as 'Hello, I'm mail.tzink.com'. However, the sender does not necessarily have to tell the truth; in fact, nothing prevents the sender from saying 'Hello, I'm bonjour. hola.guten-tag' or 'Hello, I'm wozzle.wozzle.gov', or even 'Hello, i.am.not.configured.properly'.
2. MAIL FROM is the command that initiates the mail processing. It means 'I have mail to deliver from so-and-so'. The address that is specified becomes the Envelope From or Envelope Sender (or the P1 From) and it does not need to be the same as the sender's own address.
3. RCPT TO is the flip-side of MAIL FROM; it specifies the intended recipient of the message. One piece of mail can be sent to multiple recipients by including multiple RCPT TO commands. The specified address becomes the Envelope To, which is also referred to as the Envelope Recipient (or P1 To). It is this that determines who the mail will be delivered to, regardless of what is in the To: line.
4. DATA starts the actual mail entry. Everything entered after a DATA command is considered to be part

of the message and there are no restrictions on its form. Lines at the beginning of the message (before the first blank line) that start with a single word and a colon are considered to be headers by most mail programs. A line consisting only of a period terminates the message.

5. QUIT terminates the connection.

Below is an example mail conversation between the sending domain tony.net (Tony runs his own mail server) and the recipient domain tzink-is-awesome.com (I run one, too)¹. The commands in bold are the transmitting machine while the ones in plain text are the recipient machine.

```
HELO mail.tony.net
250 mailhost.tzink-is-awesome.com Hello
mail.tony.net, pleased to meet you
MAIL FROM: tony@diamond.net
250 tony@diamond.net... Sender ok
RCPT TO: tzink@tzink-is-awesome.com
250 tzink@tzink-is-awesome.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: Tony Diamond <tony@diamond.net>
To: Terry Zink <tzink@tzink-is-awesome.com>
Date: Tue, Apr 7 2010 14:36:14 PST
Subject: How's it going?

So this is pretty cool, I'm sending an email message.
-- Tony
.
250 FAA214578 Message accepted for delivery
QUIT
221 mailhost.tzink-is-awesome.com closing connection
```

Note the five important commands: HELO, MAIL FROM, RCPT TO, DATA and QUIT. These are the basics of what it takes to send an email. Sending email is very simple and that is its strength; Tony can log on and, using his mail server, send me an email.

Tony can send the email shown above. But so can Frank. In SMTP, there's nothing to say that the MAIL FROM has to be Tony or Frank. Both Tony and Frank can put whatever they want into the MAIL FROM and send it to me, and I'll get the message. And as it turns out, email's simplicity is also its weakness.

AN AUDIT TRAIL

While the postal mail service doesn't indicate exactly where a letter was picked up from, email does (in a way) have that feature. When the receiving mail transfer agent (MTA) receives the message, it inserts additional headers which allow us to trace the message to its source. For the example

¹ My examples are simplified and the actual SMTP transaction would be more complicated in real life. The email addresses are fictional, although the domains might be real.

above, these would be the headers from the message when the receiver got them:

```
From tony@diamond.net
Received: from mail.tony.net (mail.diamond-mail.net
[292.13.130.22]) by mail.tzink.net (MyMailer 1.0) for
tzink@tzink-is-awesome.com with EMSTP id 123456789
From: Tony Diamond <tony@diamond.net>
To: Terry Zink <tzink@tzink-is-awesome.com>
Date: Tue, Apr 7, 2010 14:36:14 PST
Subject: How's it going?
```

Let's step through these one by one. The first line is the From address, which is the Envelope Sender. The Envelope Sender is generated by the receiving machine from the MAIL FROM command which comes from the transmitting machine. Note the lack of a colon in the From header – this distinguishes it from the other From: header later on. The convention is not universal, but it is common. The envelope headers are generated by the receiving machine, while the message headers are created by the transmitting machine.

The next line is a Received header. This is also an envelope header because it is generated (stamped) by the receiving machine. This Received header is important because it is the email equivalent of the US Post Office putting its stamp of authority against the originating address. If you want to see where an email came from, look for a Received header:

```
Received: from mail.tony.net
```

This piece of mail was received from a machine that calls itself (HELOs as) mail.tony.net. Next comes:

```
(mail.diamond-mail.net [292.13.130.22])
```

The IP address of the sending machine is 292.13.130.22 – Received headers will always log the sending IP address. The name of the sending machine is mail.diamond-mail.net. This name is found by performing a reverse DNS lookup of the IP address. In other words, here's what happened:

1. The message was received from a machine that said its name was mail.tony.net.
2. The IP address of the transmitting machine was 292.13.130.22.
3. A reverse DNS lookup of that IP address shows its name to be mail.diamond-mail.net.

Not all IP addresses have reverse DNS lookups, but when they exist it is easier to implement a weak form of sender authentication. If it didn't exist, the name part would be blank.

The next part of the header is the following:

```
by mail.tzink.net (MyMailer 1.0)
```

This indicates that the machine that received the message is mail.tzink.net using the (fictional) mail-receiving software MyMailer (version 1.0). This is followed by:

```
for <tzink@tzink-is-awesome.net>
```


This indicates that the message was addressed to tzink@tzink-is-awesome.net. This is the Envelope To, the address that is specified in RCPT TO by the sending machine. It is this address that the message is routed to. Note that this address does not have to be the same as the one in the To: header later on. The Envelope Sender is not always in a Received header, sometimes it is in a header elsewhere in the message. Finally, the Received header ends with:

```
with EMSTP id 123456789
```

The receiving machine assigned the ID number 123456789 to the message. This is used by mail administrators for checking logs.

The next few headers are message headers:

```
From: Tony Diamond <tony@diamond.net>
To: Terry Zink <tzink@tzink-is-awesome.com>
Date: Tue, Apr 7, 2010 14:36:14 PST
Subject: How's it going
```

These are created by the transmitting machine (Tony's). Note that there are four important routing headers: the Envelope To, the Envelope From, the message To: and the message From:. The envelope headers are generated by the receiving machine based on the SMTP commands used by the transmitting machine, while the To: and From: headers are extra headers inserted into the body of the message (which often show up in email clients such as *Thunderbird*, *Apple Mail* or *Outlook*). The message is routed based on the envelope headers, not the message headers. Also note the absence of a colon in the envelope headers.

Envelope headers appear differently in different mail servers. Sometimes the envelope sender is specified in the Return-Path header.

It is important to note that my example above is simple. Often, a message will go through more routing and will have a few more Received headers. However, the Received headers outlined here are key to determining where a message came from – from Tony legitimately, or from Frank.

SPAMMER TECHNIQUES

The system described above works well if everyone plays by the rules. But not everyone does; in fact, spammers quite often 'cheat' and do all sorts of malicious things to try to get their messages into users' inboxes. From the example earlier:

```
Received: from mail.tony.net (mail.diamond-mail.net
[292.13.130.22]) by mail.tzink.net (MyMailer 1.0) for
tzink@tzink-is-awesome.com with EMSTP id 123456789
```

In this example, the IP (292.13.130.22) that sent the message has a reverse DNS of mail.diamond-mail.net. However, what would happen if a spammer decided to forge

the HELO? What if they said 'Hello, my name is mail.fake.net'?

```
Received: from mail.fake.net (mail.diamond-mail.net
[292.13.130.22]) by mail.tzink.net (MyMailer 1.0) for
tzink@tzink-is-awesome.com with EMSTP id 123456789
```

In this example, the machine claimed to be mail.fake.net, but was sending from mail.diamond-mail.net. Straight away, we can see that there is a mismatch. When we look up the IP address mail.fake.net, it turns out that it resolves to 264.33.78.90. In other words, it is completely different from mail.diamond-mail.net. Thus, we have uncovered an example of a transmitting machine claiming to be sending from one mail host, but in fact sending from another.

A smarter spammer will use a trick to bypass this. Rather than sending from an IP address that has a reverse DNS lookup (i.e. converting an IP to a domain name), they will send mail from an IP that has no reverse DNS. In that case, the received line would look like the this:

```
Received: from mail.fake.net (unknown [282.31.32.33])
by mail.tzink.net (MyMailer 1.0) for tzink@tzink-is-
awesome.com with EMSTP id 123456789
```

I've inserted the 'unknown' because the above IP address does not resolve in DNS. Since the transmitting IP has no reverse DNS there's no way to verify whether 282.31.32.33 resolves to it. Performing a DNS lookup on mail.fake.net reveals an address that doesn't match the IP address; this is suspicious but not definitive.

A smarter spammer still would obfuscate even more:

```
Received: from hofgado (unknown [272.31.32.33]) by
mail.tzink.net (MyMailer 1.0) for tzink@tzink-is-
awesome.com with EMSTP id 123456789
```

The transmitting machine called itself 'hofgado' and sent from an IP with no reverse DNS. There's definitely no way to resolve this because the HELO won't resolve via a DNS lookup ('hofgado' is not in the proper format) and there is no reverse DNS for the IP 272.31.32.33. Nothing can be verified and we can make no assertions as to the authenticity of the message. While this certainly looks suspicious, one of the great problems of filtering spam is that misconfiguration of legitimate mail servers is incredibly common, and so looking for mail with misconfiguration as one of its features is not enough to flag a message as spam.

THE PLOT THICKENS

Each time mail goes through a relay, the receiving MTA stamps a Received header telling you where it came from and where it's going. The analogy in the postal world would be the post office writing down on the envelope that Tony's letter to me was picked up in Sacramento, processed in San Francisco, relayed through Boise, Idaho and then delivered to me in Seattle.

Suppose that Tony's mail to me went through multiple hops. We can see whenever that occurs:

```
From tony@diamond.net
Received: from mail.jason.net (jd.net
[284.33.167.99]); Tue, Apr 7, 2010 14:35:35 PST
Received: from bergie.net (mail.rypod.com
[267.99.33.167]); Tue, Apr 7, 2010 14:34:01 PST
Received: from mail.tony.net (mail.diamond-mail.net
[292.13.130.22]) by mail.tzink.net (MyMailer 1.0);
Tue, Apr 7, 2010 14:33:15 PST
From: Tony Diamond <tony@diamond.net>
To: Terry Zink <tzink@tzink-is-awesome.com>
Date: Tue, Apr 7, 2010 14:36:14 PST
Subject: How's it going?
```

I've highlighted the Received headers in different colours. In general, Received headers are read from bottom to top (that is, mail originated from the bottom Received header and took the path outlined in each Received header above it), with the most recent one being stamped at the top and being the most reliable. In the above example, the message started from the IP 292.13.130.22 at Tony's mail host. It was routed through my other friend bergie.net (IP = 267.99.33.167), then went through jd.net before finally arriving at its end destination in my inbox. It's a complicated process but from the above, we can see that the message originated at 292.13.130.22, the first IP address. It's a nice, handy way to trace the path an email followed.

Unfortunately, spammers will often insert fake routing information into the headers. Suppose that the email headers said the following:

```
From tony@diamond.net
Received: from mail.tony.net (mail.diamond-mail.net
[292.13.130.22]) by mail.tzink.net (MyMailer 1.0);
Tue, Apr 7, 2010 14:36:15 PST
Received: from frank (franksmail.net
[284.33.167.99]); Tue, Apr 7, 2010 14:35:35 PST
Received: from mail.tony.net (mail.diamond-mail.net
[262.13.130.22]) by mail.tzink.net (MyMailer 1.0);
Tue, Apr 7, 2010 14:31:15 PST
From: Tony Diamond <tony@diamond.net>
To: Terry Zink <tzink@tzink-is-awesome.com>
Date: Tue, Apr 7, 2010 14:36:14 PST
Subject: How's it going?
```

From here, we can see that the mail started out from Tony's mail server, was relayed through Frank's mail server and then routed through Tony's (again?) before it came to me. While it's odd that this double routing occurred, it is possible (though not probable).

The fact is that this message could have taken that path, or it could have originated at Frank's machine. Frank could have inserted a fake Received header to make it look as if it started at Tony's machine in order to trick the receiver into thinking it came from a trusted source. Without doing some manual inspection, it's difficult to know programmatically where the message actually originated. Usually in the

message headers there are some clues, but the fact is that the only Received header you can trust is the topmost one². That's the one your receiving MTA stamps, and you can trust it to tell you where the message has come from.

WEAK AUTHENTICATION

Looking at parts of headers that are fake is one thing. However, it's not enough simply to be able to distinguish between fake headers and real ones; we still need to be able to authenticate who the mail came from. In other words, while we certainly want to be able to tell when something is fake, we also want to know when something is real. If Tony sends me a letter, I might be able to tell from the handwriting that it doesn't belong to him and therefore that the message is fake. But how would I be able to know if the message is real? Is there anything that we have in email that allows us to make that validation?

One of the simplest forms of authentication is Forward-Confirmed Reverse DNS – something that I call a weak form of authentication.

Now that we have seen how email headers are inserted by the receiving machine upon receipt of an email, we need to go into a little bit of detail about how mail servers convert IP addresses to host names and vice versa.

DNS stands for Domain Name System. It converts a host name to its IP address. Reverse DNS is the opposite: it converts an IP address to its host name. It does this by examining the IP's PTR record:

A PTR record, or pointer record, maps an IPv4 address to the canonical name for that host. Setting up a PTR record for a hostname in the in-addr.arpa domain that corresponds to an IP address implements a reverse DNS lookup for that address. For example, at the time of writing, www.icann.net has the IP address 192.0.34.164, but a PTR record maps 164.34.0.192.in-addr.arpa to its canonical name, referrals.icann.org.

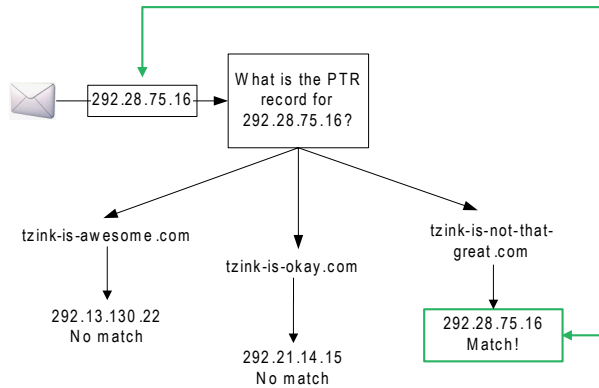
The converse of a PTR record is the A record, which maps a hostname to its 32-bit IP address. So, A-records are used for DNS lookups (example.com to xx.yy.zz.ww) and PTR records are used for reverse DNS lookups (xx.yy.zz.ww to example.com).

This brings us to Forward Confirmed Reverse DNS, or FCrDNS, which is when an IP has a forward DNS (name -> IP) and reverse DNS (IP -> name) that match³. The process works as follows:

²There are scenarios where you can trust lower Received headers, but those are outside the scope of this discussion.

³See <http://www.answers.com/topic/forward-confirmed-reverse-dns>.

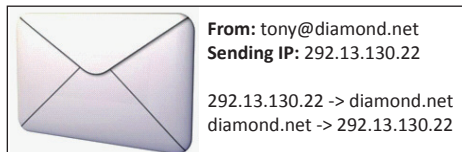
1. A reverse DNS lookup is performed on an IP. This returns a list of hostnames associated with that IP (the list could have 0, 1 or more entries).
2. For each entry in that list, a regular DNS lookup is performed to see if the IP matchup matches the original IP address. So, for example:



Since we matched the IP address in one of the domain's A-records that was found in the PTR, we are said to have FCrDNS for the IP.

This is important in spam filtering because if an IP has FCrDNS then we can be sure that the mail originated at the domain. Spammers cannot normally forge this if they are sending from zombie computers.

So, for the following email that Tony has sent me:



The sending IP and the domain name match when we check them out in DNS. We have now confirmed that the IP and domain agree with each other in DNS. Because the owner of the IP and the domain are the only ones that can maintain the public records in DNS, we can be sure that the mail is coming from the owner of that IP and domain. Since Tony owns them I can be sure that the message came from Tony.

I call this a weak form of authentication for two reasons:

1. Authentication by FCrDNS is implicit, not explicit. Yes, it's nice if the A-record of the sending domain matches the PTR record of the sending IP. If the two of them match, then the chances are very high that the owner of the IP and domain are one and the same. We assume that is the way it is supposed to be, by design, but there's no public documentation from the domain and IP owner saying that they set it up that way.

This works for small users that don't control a lot of IP addresses, but not for big ones.

2. It doesn't scale.

Often in legitimate circumstances, we just can't get FCrDNS.

Let's say I am a very large (fictitious) webmail provider, woohoo.com. If I send mail from tzink@woohoo.com, the sending IP of the MTA may not be in woohoo.com's A-record. In fact, this is quite common. In order to scale to support millions of users, Woohoo has deliberately separated the hosting of its main page <http://www.woohoo.com/> from its email servers. This is needed for redundancy; if the main page goes down it shouldn't affect the mail servers, and vice versa.

Woohoo.com → A-record	Woohoo.com → IPs that send mail
257.16.0.0/16	257.17.0.0/16

If you receive an email from tzink@woohoo.com, it will always come from an IP in the range 257.17.0.0 – 257.17.255.255. If you get the A-record for woohoo.com, it will always fall in the range 257.16.0.0 – 257.16.255.255. They will never match.

What constitutes a match, anyhow? If tzink@woohoo.com sends from IP 257.17.11.162:

- A-record for woohoo.com – 257.16.18.48
- PTR-record 257.17.11.162 – mail22.woohoo.com

Is this a match? It looks like it. But maybe not. Maybe woohoo.com doesn't want anyone doing partial matches, it has to be a complete match. But part of woohoo.com is there – maybe we should use it? Should we authenticate implicitly? What sorts of risks do we open ourselves up to if we do? (A lot.)

Unfortunately, the idea of implicit authentication is a risk.

Forward-Reverse Confirmed DNS is simply too narrow a case to be used for authentication. For small senders who have narrow lists of IPs to maintain, it works. As an organization gets larger, it needs to find a solution that scales much better and authentication must be more explicit. We still want to authenticate an email, but we have to move onto something other than FCrDNS. To do that, we need to look at stronger authentication technologies – SPF, SenderID and DKIM. The discussion of those, however, will have to wait until next month.

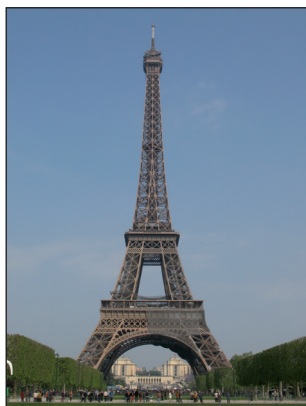
CONFERENCE REPORT

EICAR 2010: RAINY DAYS IN PARIS

Eddy Willems

G Data Software and EICAR, Belgium

The 19th EICAR conference took place last month in the heart of the beautiful city of Paris at the École Supérieure d'Informatique, Electronique, Automatique (ESIEA).



Paris in the sunshine.

The second International Alternative Workshop on Aggressive Computing and Security (iAWACS'10) was held immediately before the conference at the same venue, and EICAR delegates were also able to attend this event. iAWACS'10 included workshops on smart cards and crash courses on securing PLC networks, but the most noteworthy item on the agenda was the anti-virus evaluation challenge 'PWN2KILL', the aim of which was to attempt to bypass anti-virus software and evaluate its effectiveness in practical terms. A technical summary is available on the iAWACS website. [David Harley shares his views on the challenge on p.2 – Ed.]

GETTING STARTED

After an official EICAR members meeting and welcome party on the Sunday evening, the real meat of the conference began on Monday morning with an opening address from the chairman of EICAR, Rainer Fahs, continuing with a keynote from Christophe Devine – better known as the father of 'Aircrack' – about problems related to AV testing. He described a series of tests and rated their usefulness. Devine believes that, in most cases, careful inspection reveals no real winners, and several tests are not even relevant to the real world. He proposed an initiative called AVerify, an open-source anti-virus test suite which would facilitate the creation of reproducible, more reliable tests. AVerify would be inspired by the EICAR test file, maintained independently of EICAR but following the same code of conduct.

'Parasitics, the next generation' was a joint paper from Vitaly Zaytsev (*McAfee*) and Josh Philips (*Kaspersky Lab*), in which an in-depth analysis of two of the most recent advanced and sophisticated viruses (W32/Xpaj and

W32/Winemem) was presented along with the new techniques they use to transform their code to avoid detection. Zaytsev and Philips discussed ways in which VM-based obfuscators can be defeated.

Zdenek Breitenbacher used 'Lego building blocks' to demonstrate that although each copy of polymorphic malware is totally different in a simple binary view, we can still find some characteristics that always remain more or less the same. He discussed a characteristic the malware analyst can use: entropy. But instead of calculating the entropy as a single number describing the whole file, we need a very detailed map which plots entropy throughout the file. He showed that by inspecting the entropy map, a malware analyst can easily isolate the innocent and the suspicious parts of the file. The entropy map of one polymorphic family often remains the same for all of its copies. In fact, such an entropy map can act as a special kind of signature, which could be used in the same way as a traditional signature. The entropy map offers a new and unexpected view of malicious files and may help malware analysts in many different tasks.

Igor Muttik revealed 'a single metric for evaluating a security product'. He analysed the factors contributing to the probability of successful protection, presented a mathematical approach to calculating this probability and discussed how this can be implemented in practice. He showed some examples of how the growing frequency of attacks dictates a statistical approach to measuring the quality of security software. Lysa Myers from *West Coast Labs* gave us an insight into their new testing techniques, and Alexey Tkachenko from *Dr. Web* presented a detailed analysis of the nasty Backdoor.Tdss rootkit (aka TDL3).

That evening the conference gala dinner provided an opportunity to relax and enjoy good French food and champagne during a pleasant boat trip on the river Seine. While heavy rain disrupted a short walk by the river, the beautiful sparkling lights of the Eiffel tower in the background created a truly magical atmosphere.

BEST PAPER

For the first time in the history of the EICAR conference, the best paper prize was awarded this year to an industry paper which combined elegant theory with practical applications. In her paper 'Symbian worm Yxes: towards mobile botnets?', Axelle Apvrille described how this mobile malware connects to the Internet, installs new malware or spreads to other victims. She explained how malicious remote servers participate in the configuration and propagation of the malware, noting Yxes's similarities to a botnet. The paper shows the importance and lack of



Paris (and delegates) in the rain.

security on mobile phones. It also indicates several areas on which future work should focus, such as communication decryption and tools to analyse mobile-embedded malware.

Jan Vrabec and David Harley shared their views on the methodology and categories used in performance testing of anti-malware products. This seems to remain a contentious area. While there is plenty of information on detection testing, very little is available on performance testing. The paper aims to objectively evaluate the most common performance evaluation metrics used in anti-malware testing, such as scanning speed, memory consumption and boot speed, and to highlight the main potential pitfalls of such testing procedures. Vrabec and Harley made some recommendations on how to test objectively and how to spot potential bias. A nice paper, and a must-read!

‘Crowdsourcing’ is best defined as ‘a neologism for the act of taking tasks traditionally performed by an employee or a contractor, and outsourcing them to a group (crowd) of people or community in the form of an open call’. In her paper, Methusala Cebrian Ferrer posed the question of whether there could be a future for crowdsourcing security. As web-based technologies move towards interactive social media, real-time web, and capturing geo-specific content, it is important to understand whether crowdsourcing could be a viable strategy for the security industry. In other words, collective security intelligence is becoming a necessity if we want to deal with the amount of data which besets us: the problem is that this is easier said than done.

In ‘Perception, security and worms in the Apple’, David Harley, Pierre-Marc Bureau and Andrew Lee compared the view from *Apple* and its user community as a whole with the view from the anti-virus labs of the actual threat landscape. They examined the ways in which the *Apple*-using community is receiving increasing attention as a potential source of illegitimate profit, reviewing the directions likely to be taken by malware over the next year

or two, and assessing the likely impact of attacks against *Apple* users and the implications for business and for the security industry. As the Mac user community still sees the Mac as a safe haven, it is indisputable that this platform will see many more problems arise in the future.

Vlasti Broucek from the University of Tasmania discussed ‘the cost of university Internet access’ and highlighted the need for continued vigilance on the part of users, network administrators, service providers and policy makers. Using examples from two different areas of the university, he demonstrated, that if we are not to create an Internet of ‘Big Brother surveillance’, or even worse one of ‘self-censoring behaviours’ – or force mass adoption of encryption to ensure privacy and the security of users from prying eyes – then user education, change management and communication from the very top right to the bottom of the organization will play a vital role.

AND FINALLY

The final paper on the programme was a very interesting theoretical and academic paper presented by four ESIEA students (Jonathan Dechau *et al.*), who attempted to evaluate the ability of anti-virus to detect malware spreading through *Office* documents. The paper used the EICAR test file to demonstrate that macro-based attacks are very easy to put into action, and prompted some heated discussions about problems related to signature-based detection. Some of the paper’s conclusions were potentially flawed, having been based on non-detection of modified versions of the EICAR test file (see p.2). However, the theory behind this research seems to be perfectly correct and will inspire more discussion about the detection methodologies currently used and the consequent problems in all security products these days: this was, of course, the real message behind the presentation.

LOOKING BACK AND LOOKING AHEAD

By the time you read this, or soon after, most of the presentations from this year’s conference, including those I’ve been unable to include in this summary, will be available at <http://www.eicar.org/>. Once again this year saw a significant increase in the quality and quantity of papers submitted for the conference and the event itself was a great success. As one of the founding members of EICAR, I remember the first constitutional conference in Brussels in 1991. A lot has happened and improved during those 19 years and I fully expect this to continue. The location of the 20th EICAR conference has yet to be decided, although rumours are spreading quickly. A call for papers and announcement of dates and venue will be published soon.

COMPARATIVE REVIEW

VB100 – WINDOWS SERVER 2008 R2

John Hawes

Following our usual pattern of alternating between desktop and server platforms, we come this month to *Microsoft's* latest upgrade to its server solution. This is presented as a simple refresh of the 2008 version, but in fact is a much bigger deal, essentially being *Windows 7 Server*. The new platform is considerably revised and updated, and is available only for 64-bit hardware. We expected that this combination of a new platform and the use of full x64 would deter some vendors from entering products for what could be a rather tricky test, but in fact we were inundated with far more entries than we had anticipated. With the working month shortened by some urgent lab maintenance and a cluster of conferences, it looked like the lab team would once again be getting little rest as we hurried along, hoping as usual for well-behaved and reliable products to deal with.

PLATFORM AND TEST SETS

Installation of the test systems was a fairly simple process, with the set-up process for the new platform closely mirroring that of *Windows 7* and running smoothly on our shiny new batch of test systems. These were all fully supported from the off with no need for additional drivers etc. Having made a few standard adjustments, installed some useful software such as PDF viewers in case any help files might need perusal, and configured networking to fit in with our lab set-up, we were ready to take snapshots and move on to preparing the test sets. The most interesting aspect of the platform preparation process was the requirement for a small additional partition on the hard drive. Small adjustments to our reimaging set-up were required to ensure both partitions were reset to their original status for each test run.

Test set preparation was a rather more arduous task, with much work required to bring the lab systems back up to full functionality after having been neglected during the hectic period of the last comparative. With space running out and more processing power required, a few hasty temporary fixes were required to enable us make a start on this month's test.

The core WildList test set saw a sprinkling of new additions, with an early test deadline meaning we just missed the release of the March list; the sets were instead aligned with the February list, which included the same W32/Virut strain that caused some upsets last time around, as well as the

venerable W32/Polip which was generally handled more solidly. New additions followed the trend of recent months, dominated by W32/Koobface worms with little else of particular novelty or interest.

The other core part of the certification set, the clean sample set, saw some considerable expansion, with the usual addition of the most popular items from various freeware sites supplemented with swathes of more serious software packages from *Microsoft, Sun* and others as a nod to the server setting of this month's test.

The remaining sets followed the usual pattern. A small adjustment to the polymorphic set was made to increase the representation of some of the more recent and prevalent items, while some older and less interesting families were retired from the set. The trojans and worms & bots sets were built with samples gathered in the period between the last test and the start of this month's RAP period. The RAP samples were sorted into their weekly sets, which were somewhat larger than previous ones thanks to increased sample-gathering efforts. Due to the tight time frame of the test, only minimal processing was possible prior to compiling the sets and putting them into use on the test systems, so the sets scanned by each product contained well over 100,000 samples. We expected a great deal of these to be ruled out of the final count – whether because they failed our validation process or because they didn't even get as far as the checking process – but the large raw sets promised a significant amount of scanning time and the likelihood of problems for the products. In the final reckoning, the weekly batches averaged just over 12,000 samples per week.

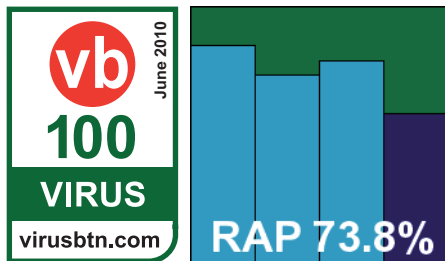
The speed sets, used for our various performance measures, were tidied a little but remained much the same as usual. Some minor adjustments were made to the CPU and RAM usage measurement tools introduced recently (for a full explanation of these see *VB*, April 2010, p.23). With everything in place, testing proceeded without delay.

Agnitum Outpost Security Suite Pro 2009 6.7.3

ItW	100.00%	Polymorphic	89.10%
ItW (o/a)	100.00%	Trojans	90.35%
Worms & bots	95.88%	False positives	0

Agnitum's Outpost has put in a string of solid performances of late; it has a straightforward and unflashy approach providing several protective layers in a well-ordered, solid-feeling interface. Set-up and configuration is clear and problem free, with a reboot required to complete installation. Chugging through the test sets proved equally

smooth and reliable. Scanning speeds were not lightning fast, but some good optimization improved the speed of scanning of previously checked items considerably. This made for a good profile on our speed graphs, while RAM consumption was a little above the average for this month's field, but CPU cycle drain was fairly low, even under heavy pressure.

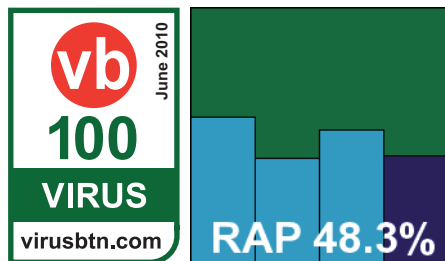


Detection scores in the main sets were very solid, and RAP scores fairly decent. With no problems handling the WildList and no false alarms in the clean sets, *Agnitum* scoops up another VB100 award and gets this month's test off to a good start.

AhnLab V3Net for Windows Server 7.7.6.4 build 1152

ItW	100.00%	Polymorphic	99.58%
ItW (o/a)	100.00%	Trojans	67.43%
Worms & bots	69.43%	False positives	0

The set-up process for the server version of *AhnLab's* product is fast and simple, with few decisions to make and no need



for a reboot to complete. The product interface closely resembles the desktop edition, with a fairly minimal set of configuration options which might be a little short on flexibility for more demanding administrators. However, navigation is clear and tidy and carrying out simple tasks is easy, with the available options well laid out. The separation of scans into virus and spyware checks was a little confusing however – most products offer a separate spyware system which looks at registry entries and other configuration issues rather than scanning files; it seems more rational to keep it simple and check for any bad stuff with a single scan, rather than requiring multiple checks. Running through the tests, the on-access scan of the main set brought up our first blue screen on the new platform

– this came after a rather longer period of stability than on our first visit to *Windows 7*, but was still rather disappointing. The machine rebooted happily though, with nothing vital lost by way of logging etc., and retries proved more successful with no repeat of the glitch. Scanning speeds were mid-range on demand, with a small amount of optimization evident in the ‘warm’ scans, and pretty impressive on access. RAM usage was fairly low and CPU consumption around the middle of the field.

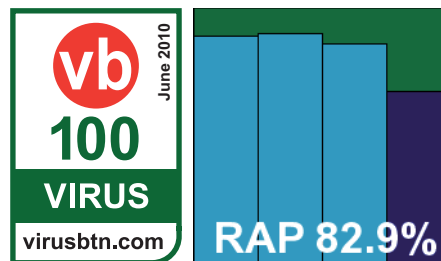
Detection rates in the main test sets were unspectacular, and the RAP sets were not handled especially impressively either. It has been suggested that our sample-gathering techniques may put vendors from certain geographic regions at a disadvantage, but we have been making every effort to ensure global coverage and some of our largest and most regular sample sources are based in the Far East – we will continue to work on this issue to improve the representativeness of our test sets.

The WildList and clean sets proved no problem for *AhnLab*, however. There were a large number of alerts stating that *Office* documents containing macros contained, well, macros, but the warnings were couched in language that was close enough to a detection alert to merit recording them in the ‘suspicious’ column on our tables. Nevertheless, *AhnLab* comfortably earns a VB100 award.

avast! Server 4.8.1113

ItW	100.00%	Polymorphic	99.33%
ItW (o/a)	100.00%	Trojans	93.56%
Worms & bots	96.93%	False positives	0

avast! (formerly *Alwil*) announced the change of its company name as testing got under way – this seemed like a sensible move given the product's brand recognition value.



Disappointingly, the company name was the only new thing here – the developers informed us that the new version 5 server edition of the product was not quite ready for release, and we had to make do with version 4.

This was no great problem, however, as the older edition has been around long enough to acquire a rugged stability which shrugs off the need for flashy good looks. The

On-demand detection	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	697	95.88%	195	89.10%	4688	90.35%	0	0
AhnLab V3Net	0	100.00%	5166	69.43%	12	99.58%	15821	67.43%	0	15
avast! Server	0	100.00%	518	96.93%	26	99.33%	3126	93.56%	0	0
AVG I.S. Network Edition	0	100.00%	337	98.01%	52	97.57%	1583	96.74%	0	0
Avira AntiVir Windows Server	0	100.00%	319	98.11%	0	100.00%	1479	96.96%	0	0
BitDefender Security	0	100.00%	1205	92.87%	0	100.00%	3319	93.17%	0	0
Bkis BKAV Gateway Scan	0	100.00%	5223	69.09%	1598	63.21%	24288	50.00%	4	0
Bkis BKAV Gateway Scan Plus	0	100.00%	5224	69.09%	1598	63.21%	24288	50.00%	4	0
Bkis BKAV Home Edition	0	100.00%	5223	69.09%	3349	54.25%	24288	50.00%	4	0
Bkis BKAV Home Edition Plus	0	100.00%	5223	69.09%	3333	58.17%	24289	50.00%	4	583
Central Command Vexira	0	100.00%	684	95.95%	195	89.10%	4740	90.24%	0	0
Coranti Multicore	0	100.00%	217	98.72%	0	100.00%	1709	96.48%	0	0
Defenx Security Suite	0	100.00%	719	95.75%	196	88.85%	4941	89.83%	0	2
Digital Defender	0	100.00%	930	94.50%	195	89.10%	6241	87.15%	1	0
eEye Blink Server	3	99.9998%	4603	72.76%	338	82.01%	12095	75.10%	0	0
eScan I.S. Suite	0	100.00%	591	96.50%	4	99.995%	3373	93.06%	0	0
ESET NOD32 Antivirus	0	100.00%	143	99.15%	6	99.99%	1587	96.73%	0	2
Fortinet FortiClient	0	100.00%	1750	89.64%	33	99.08%	14278	70.61%	0	0
Frisk F-PROT	0	100.00%	1282	92.41%	0	100.00%	10001	79.41%	0	0
F-Secure AntiVirus	0	100.00%	1111	93.43%	0	100.00%	3387	93.03%	0	0
G DATA AntiVirus	0	100.00%	1044	93.82%	0	100.00%	327	99.33%	0	0
Kaspersky Anti-Virus 6	0	100.00%	282	98.33%	2	99.998%	2432	94.99%	0	0
Kaspersky Anti-Virus 8	0	100.00%	276	98.37%	266	99.69%	2574	94.70%	0	0
Kingsoft 2011 Advanced	0	100.00%	10827	35.93%	4832	57.11%	41275	15.03%	0	0
Kingsoft 2011 Standard	0	100.00%	11554	31.63%	4832	57.11%	43495	10.46%	0	0
McAfee VirusScan	0	100.00%	1066	93.69%	1	99.999%	6880	85.84%	0	0
Norman Endpoint Protection	3	99.9998%	4635	72.57%	288	83.09%	12208	74.87%	3	0
Quick Heal AntiVirus	0	100.00%	1776	89.49%	11	99.50%	11194	76.95%	0	0
Rising I.S.	0	100.00%	7029	58.41%	3577	70.27%	24880	48.78%	0	0
Sophos Endpoint	0	100.00%	295	98.25%	0	100.00%	4266	91.22%	0	1
SPAMfighter VIRUSfighter	0	100.00%	1889	88.82%	1426	71.61%	6269	87.09%	1	0
Trustport AntiVirus 2010	0	100.00%	177	98.95%	0	100.00%	1190	97.55%	0	0
VirusBuster	0	100.00%	684	95.95%	195	89.10%	4740	90.24%	0	0

installation process is lucid and logical, and after a reboot the slightly unusual control system provides an admirable level of configuration – enough to satisfy the most demanding of administrators.

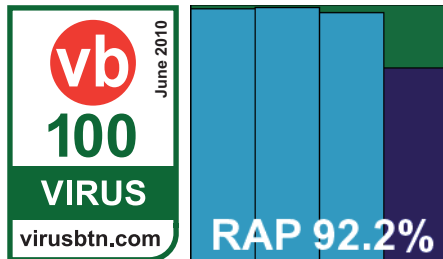
Running through the tests was a smooth process, with excellent scores in the main sets and RAP scores perhaps a fraction below what we have seen in recent months – clearly version 5 includes some significant improvements in more than just the GUI design.

Scanning speeds were pretty zippy though, and both file access lag times and RAM consumption very light indeed. The core WildList and clean sets presented no difficulties, and *avast!* earns its first VB100 award under its new company name.

AVG Internet Security Network Edition 9.0.814

ItW	100.00%	Polymorphic	97.57%
ItW (o/a)	100.00%	Trojans	96.74%
Worms & bots	98.01%	False positives	0

AVG's developers chose to submit a standard desktop product for this test, rather than the specialist server versions many of their fellow vendors provided.



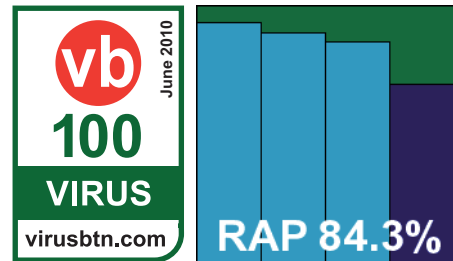
The flagship product installs quickly and easily, with no need for a reboot despite the multiple layers of protection included (many of which are not covered by our testing but should provide additional defence against attacks). As we have noted previously, the presentation of the many modules has some redundancy and makes the GUI a little cluttered and on occasion confusing to navigate, but there is a solid and respectable look and feel to it, and a good level of fine-tuning is provided for most purposes.

Scanning speeds were fairly average, on-access lags low in some areas but heavier in others. RAM usage was low, but CPU consumption fairly high, making for a mixed set of performance results overall. Detection rates in the main test sets were exemplary and RAP scores were pretty impressive. With no problems handling the WildList or clean sets, AVG continues this month's run of successes by earning a VB100 award.

Avira AntiVir Windows Server 8.02.01.211

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.96%
Worms & bots	98.11%	False positives	0

Avira's AntiVir provided the first of what we expected to see many of this month: fully fledged server protection systems based



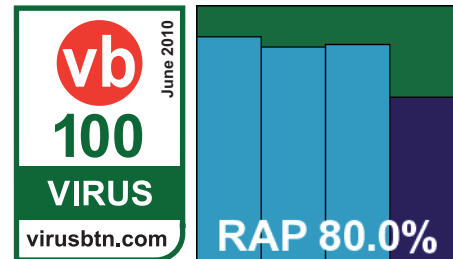
on the MMC system. Installation was delayed a little thanks to the requirement for C++ libraries to be put in place, but no reboot was needed to finalize the install. The interface is, of course, considerably more demanding than the average cartoony home-user GUI, but provides a complete range of controls and fine-tuning options. These are fairly easy to locate and configure once the layout and operation technique have been divined.

Scanning speeds were consistently fast, with some good, light on-access times, low CPU drain but surprisingly high RAM usage. Once again some excellent scores were recorded across the standard sets and also in the RAP sets. Full coverage extended to the WildList set, and with no false alarms in any of the clean sets Avira picks up another VB100 award.

BitDefender Security for Windows Servers 3.4.11.141

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.17%
Worms & bots	92.87%	False positives	0

Another full-blown server solution, and again using the MMC for its main control interface, BitDefender's product



installed simply and proved equally straightforward to operate – with rather more colour and panache to the GUI than expected from this kind of approach. Navigation

On-access detection	WildList		Worms & Bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	858	94.92%	195	89.10%	5588	88.50%
AhnLab V3Net	0	100.00%	5166	69.43%	12	99.58%	15993	67.07%
avast! Server	0	100.00%	297	98.24%	26	99.33%	2655	94.53%
AVG I.S. Network Edition	0	100.00%	388	97.70%	52	97.57%	2289	95.29%
Avira AntiVir Windows Server	0	100.00%	330	98.05%	0	100.00%	1657	96.59%
BitDefender Security	0	100.00%	1320	92.19%	0	100.00%	3600	92.59%
Bkis BKAV Gateway Scan	0	100.00%	5223	69.09%	1598	63.21%	24283	50.01%
Bkis BKAV Gateway Scan Plus	0	100.00%	5224	69.09%	1598	63.21%	24285	50.00%
Bkis BKAV Home Edition	0	100.00%	5223	69.09%	3366	58.13%	24284	50.01%
Bkis BKAV Home Edition Plus	0	100.00%	5223	69.09%	3366	58.13%	24284	50.01%
Central Command Vexira	0	100.00%	810	95.21%	195	89.10%	5231	89.23%
Coranti Multicore	0	100.00%	195	98.85%	0	100.00%	1631	96.64%
Defenx Security Suite	0	100.00%	858	94.92%	195	89.10%	5588	88.50%
Digital Defender	0	100.00%	930	94.50%	195	89.10%	6241	87.15%
eEye Blink Server	3	99.9998%	4869	71.19%	85	83.63%	12693	73.87%
eScan I.S. Suite	0	100.00%	698	95.87%	0	100.00%	4165	91.43%
ESET NOD32 Antivirus	0	100.00%	466	97.24%	8	99.96%	2320	95.22%
Fortinet FortiClient	0	100.00%	1751	89.64%	1338	71.34%	12392	74.49%
Frisk F-PROT	9	98.26%	1439	91.49%	0	100.00%	11527	76.27%
F-Secure AntiVirus	0	100.00%	1575	90.68%	0	100.00%	3396	93.01%
G DATA AntiVirus	0	100.00%	496	97.07%	0	100.00%	564	98.84%
Kaspersky Anti-Virus 6	0	100.00%	431	97.45%	2	99.998%	2990	93.84%
Kaspersky Anti-Virus 8	0	100.00%	819	95.15%	266	99.69%	3342	93.12%
Kingsoft 2011 Advanced	0	100.00%	10837	35.88%	4832	57.11%	41431	14.71%
Kingsoft 2011 Standard	0	100.00%	11554	31.63%	4832	57.11%	43506	10.43%
McAfee VirusScan	0	100.00%	1230	92.72%	1	99.999%	6167	87.30%
Norman Endpoint Protection	3	99.9998%	5184	69.33%	782	76.42%	12788	73.67%
Quick Heal AntiVirus	0	100.00%	4379	74.09%	46	96.49%	29177	39.93%
Rising I.S.	0	100.00%	5959	64.74%	7768	65.28%	29852	38.54%
Sophos Endpoint	0	100.00%	296	98.25%	0	100.00%	2723	94.39%
SPAMfighter VIRUSfighter	0	100.00%	1889	88.82%	1426	71.61%	6269	87.09%
Trustport AntiVirus 2010	0	100.00%	157	99.07%	0	100.00%	1135	97.66%
VirusBuster	0	100.00%	684	95.95%	195	89.10%	4740	90.24%

was logical and the scheduling system in particular drew approving nods from the lab team, with a quick and simple set-up process for jobs using a proper calendar for improved efficiency. A few oddities were noted in some jobs, with a number of subfolders of the selected areas apparently skipped over in some scans, but after careful checking and a few re-runs, a complete set of results were safely in the bag.

Scanning speeds were pretty good on demand and not bad on access once the product had familiarized itself with the files; the resource usage graph also shows a pretty light memory and processor footprint. Some highly respectable detection figures were obtained in the main sets, with decent coverage across the RAP sets too. The WildList was handled effortlessly, and with no false alarms either *BitDefender* adds another VB100 award to its solid testing history.

Bkis BKAV Gateway Scan 2829

ItW	100.00%	Polymorphic	63.21%
ItW (o/a)	100.00%	Trojans	50.00%
Worms & bots	69.09%	False positives	4

Bkis BKAV Gateway Scan Plus 2829

ItW	100.00%	Polymorphic	63.21%
ItW (o/a)	100.00%	Trojans	50.00%
Worms & bots	69.09%	False positives	4

Bkis BKAV Home Edition 2829

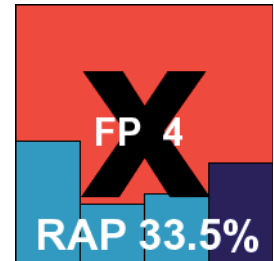
ItW	100.00%	Polymorphic	54.25%
ItW (o/a)	100.00%	Trojans	50.00%
Worms & bots	69.09%	False positives	4

Bkis BKAV Home Edition Plus 2829

ItW	100.00%	Polymorphic	58.17%
ItW (o/a)	100.00%	Trojans	50.00%
Worms & bots	69.09%	False positives	4

Bkis made its VB100 debut in the last comparative (see *VB*, April 2010, p.23), and put in a good showing but didn't quite make the grade for certification. Clearly encouraged by the experience, the company has returned in force this month with no fewer than four products submitted. Despite our warnings that it might not be possible to include so many in what looked likely to be a well-subscribed test, as well as the recent imposition of entry fees for three or

more submissions from a single vendor, the Vietnamese firm insisted they all be included, and in the end – thanks to generally good behaviour – we managed to squeeze them all in. As all are fairly similar both in design and in performance, it seems sensible to cover them all with a single write-up, pointing out any differences as necessary.



The installation process is remarkably simple, with only a couple of clicks and a few moments' wait before everything is done – a reboot is needed at the end. The interface is clear and well laid out, providing a basic level of configuration. This is unlikely to satisfy the demands of a corporate server administrator, but ample for the average inexpert home user. The only evident difference between the home and gateway versions – on the surface at least – is the colour of the interface, which is a slightly pastel orange for the home products and a rather sickly green for the gateway ones.

Running through the tests proved fairly straightforward thanks to the simple and responsive design, and the absence of any serious problems. Detection rates for all products were fairly similar, with some evidence of improved coverage of polymorphic viruses in the gateway solutions. Scores in the main sets were somewhat below par, and in the RAP sets showed a severe dip in the week -2 set, recovering slowly to show a surprising jump in the proactive week – we can only assume that some oddity in the sources of our sets caused the latter two weeks of the reactive portion to contain a large number of items not accessible to *Bkis*.

In the performance tests, all four products were closely matched in terms of scanning speed (somewhat mediocre) and lag times (rather hefty). In the resource consumption measures, the *Gateway Scan* product showed some pretty high use of RAM throughout, while all the others were much lower on the same measure, performing quite favourably compared to the field. However, all were fairly high on CPU cycle consumption.

After a handful of misses in the WildList last time around, things were looking good when all four product versions managed a clean sweep of the latest list in both modes. An unlucky snag arrived in the clean sets however, when all four identified a tool provided by *Microsoft* as a trojan (several versions for different platforms were included in the clean set), and also misidentified another item from a prominent developer, thus denying *Bkis* its first VB100 award for a second month running.

Archive scanning		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Agnitum Outpost	OD	2	√	√	√	X	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
AhnLab V3Net	OD	9	9	9	9	9	9	X	9	√
	OA	X	X	X	X	X	X	X	X	X
avast! Server	OD	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
AVG I.S. Network Edition	OD	√	√	√	√	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Avira AntiVir Windows Server	OD	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Security	OD	X/√	X/√	X/8	X/√	X/√	X/√	X/8	X/√	√
	OA	X/√	X/√	X/√	8/√	X/√	X/√	X/√	1/√	√
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 Gateway Scan Plus	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	√
Bkis BKAV Home Edition Plus	OD	X	X	X/1	X/1	X	X/1	X	X/1	√
	OA	X	X	X	X	X	X	X	X	√
Central Command Vexira	OD	X	√	√	X/√	X	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Coranti Multicore	OD	√	√	8/√	√	√	√	8/√	√	√
	OA	X	X	X/1	X	X	X	X	X	X
Defenx Security Suite	OD	2	√	√	√	X	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Digital Defender	OD	1	1	1	1	X	1	X	1	√
	OA	1	1	X	X	X	1	X	1	X/√
eEye Blink Server	OD	X	√	1	√	√	√	√	√	√
	OA	X	X/√	X	X/√	X/√	X/√	X/√	X/√	√
eScan I.S. Suite	OD	9	5	3	5	5	5	4	5	√
	OA	X/√	X/√	X	X/√	X	X/√	X/8	X/√	√
ESET NOD32 Antivirus	OD	√	√	√	√	√	√	5	√	√
	OA	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	√	4	√
	OA	X	√	√	√	√	√	√	4	√
Frisk F-PROT	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	2	2	X	X	X	2	√

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*
F-Secure AntiVirus	OD	X/√	√	√	√	√	√	8	√	X/√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/8	X/√	X/√
G DATA AntiVirus	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	4	√	√	√	8	8	√
Kaspersky Anti-Virus 6	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky Anti-Virus 8	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
Kingsoft 2011 Advanced	OD	X	√	X	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Kingsoft 2011 Standard	OD	X	√	X	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X/2	X/√	√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	√	X/√	X/√	X/√	X/√	X/√	√
Norman Endpoint Protection	OD	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	√
Quick Heal AntiVirus	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	√
Rising I.S.	OD	X	X	√	√	√	√	√	√	√
	OA	X	X	√	X/√	X/√	X/√	X/√	X/√	√
Sophos Endpoint	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
SPAMfighter VIRUSfighter	OD	1	1	1	1	X	1	X	1	√
	OA	X/1	X/1	X	X/1	X	X	X	X/1	1/√
Trustport AntiVirus 2010	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	√	X/√	1/√	X/√	1/√	√
VirusBuster	OD	2	√	√	X/√	X	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√

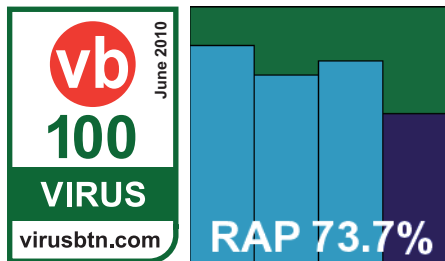
Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels.

In a final unexpected difference between the four products, one of them labelled a large swathe of samples included with the core operating system as suspicious adware. Despite these glitches *Bkis's* product range impressed with its stability and good behaviour, and the company remains a strong contender to join the ranks of VB100 certified vendors soon.

Central Command Vexira Anti-Virus for Windows Servers 6.2.53

ItW	100.00%	Polymorphic	89.10%
ItW (o/a)	100.00%	Trojans	90.24%
Worms & bots	95.95%	False positives	0

Vexira entered our mammoth XP test (see *VB*, April 2010, p.23) after a lengthy absence from the comparative reviews, and returns this month for more of the same. The product set-up is reasonably undemanding, and on completion we were not surprised to see the familiar interface of *VirusBuster's* server solution, veteran of many server-level comparatives, with a change in colour scheme apparently the main difference.



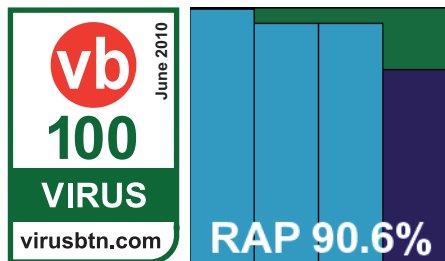
The GUI itself – once again using the MMC system – is a little clunky and awkward in places, lacking a little in completeness of vision with some options looking the same, but operated in different ways. In general, a good level of control is provided once the control system has been wrestled into submission, but in some places it is less than fully effective – notably, the options to enable on-access checking of archives appeared to have no effect at all.

Scanning speeds were fairly middling, with no sign of any optimization on repeat scanning and a fairly low resource footprint, but detection rates were respectable in the main test sets and pretty decent in the RAP sets too. There were no problems in the core certification sets, and *Central Command* earns a second VB100 award in a row.

Coranti Multicore 2010 1.000.00022

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.48%
Worms & bots	98.72%	False positives	0

A newcomer to the VB100 test bench, *Coranti* is the new face of a project which, under a different name, has been on the verge of joining the tests for some time. Still in beta, the product uses a multi-engine approach combining the detection capabilities of four separate solutions. First impressions were good, with a clean and smooth installation process which zipped through, although the initial update of all four engines did take quite



some time, with something close to 250MB of data to download. This could present difficulties in some situations, and it might be preferable for the developers to provide their installer to customers with more recent detection data included, rather than making them install the product and then leave their machine less than fully protected for such a long time. Perhaps this will be implemented as the development process draws to completion.

The product interface is attractive and nicely laid out, with a decent level of configuration easily accessible. While running a scan, an animation shows a magnifying glass moving over an orange symbol – although at first glance this looked like someone polishing a goldfish.

A few quirks were noted, most frustratingly the apparent inability to return to the scan progress screen if navigated away from mid-scan. These were minor issues though; scanning speeds were rather more of an issue, with the multi-engine approach apparently running each engine in turn over the selected area, making for multiple progress bars and some rather lengthy scanning times. File access lags were rather hefty too, and as might be expected, use of CPU and RAM was among the highest in this month's field.

The flip side of this, of course, is the power of multiple engines, and unsurprisingly some splendid scores were achieved across the test sets, with very solid numbers in all the RAP batches. This information was a little hard to come by, with logs having to be stripped from a rather gnarly database format, and hopefully future builds will include the option to keep all detection data and export to file – an especially important option for anyone using the product in a proper server environment.

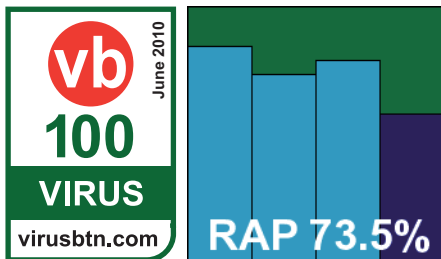
The WildList set was handled without problems, and in the clean sets, where there was some danger of the multi-engine approach causing further problems, only a handful of suspicious warnings were raised, meaning *Coranti* can proudly join the ranks of VB100-certified products.

Defenx Security Suite 2010 3063.452.0728

ItW	100.00%	Polymorphic	88.85%
ItW (o/a)	100.00%	Trojans	89.83%
Worms & bots	95.75%	False positives	0

Another relative newcomer returning after a successful debut last time around, *Defenx* is closely modelled on *Agnitum's* *Outpost* product, with a change of colour scheme the main adjustment made for the company's regional users. The set-up and usage experience are thus identical to that of *Outpost*, and speeds, performance ratings and detection scores also show little difference.

Good detection levels in the main sets and decent RAP scores combine with an absence of false alarms in the clean sets and fine coverage of the WildList to earn *Defenx* its second VB100 award.



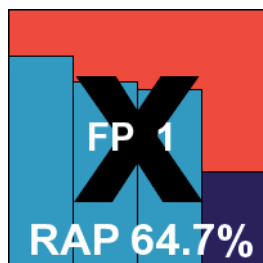
of logs after a fixed level of entries, but this issue was circumvented and results eventually obtained.

Scanning speeds and overheads were fairly good and performance drains pretty light, with some decent scores in the main sets. A solid start in the RAP sets was followed by a fairly sharp drop in the proactive week – notably more so than others based on similar technology, hinting at an entry made somewhat earlier than others and missing some last-minute updates. Also differing from others based on the same technology, a single false alarm in the clean sets – a guide to *Windows 7* produced by *Microsoft* flagged as an exploited document – meant that, despite a clean run through the WildList set, *Digital Defender* narrowly misses out on a VB100 award this month.

Digital Defender 2.0.27

ItW	100.00%	Polymorphic	89.10%
ItW (o/a)	100.00%	Trojans	87.15%
Worms & bots	94.50%	False positives	1

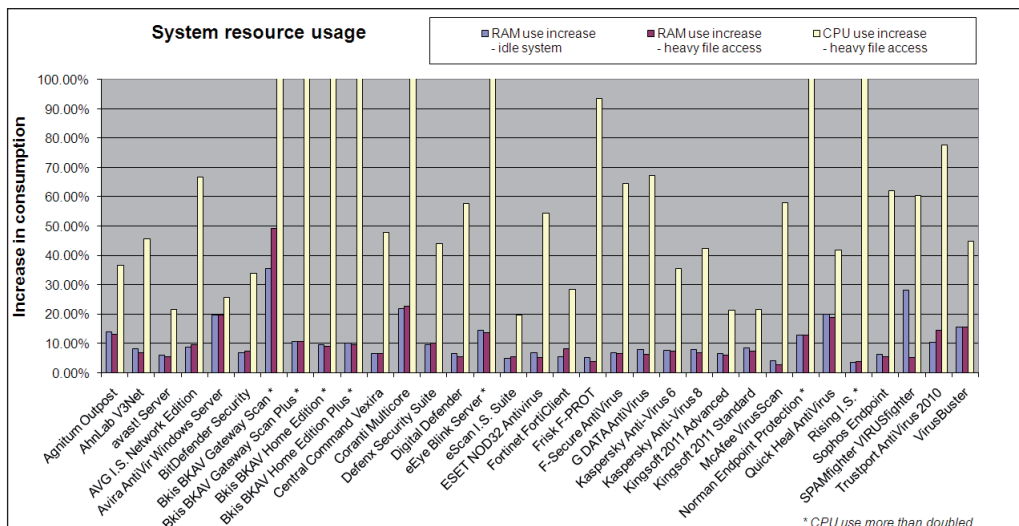
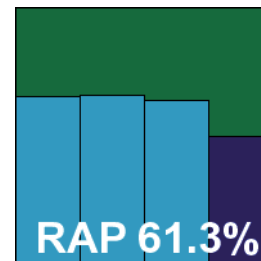
Digital Defender is another of the newbies from the last test, returning after a glorious debut. Its solution is an implementation of the *VirusBuster* detection engine in a pleasantly simplified GUI – unlikely to appeal to most server admins but more than ample for the home market (which seems to be the company’s main target). Installation and set-up is fairly straightforward, but testing was impeded initially by the requirement for an activation key to access some of the configuration. With this in place, things moved on reasonably well – hampered for a time by the overwriting



eEye Blink Server 4.6.2

ItW	99.99%	Polymorphic	82.01%
ItW (o/a)	99.99%	Trojans	75.10%
Worms & bots	72.76%	False positives	0

Blink has become a regular entrant in our tests lately, but this is the first appearance of the server edition. In terms of user experience there is not a great deal of difference however; the install process is fairly simple and speedy, and the interface looks much the same – fairly serious and unflashy with an air of solid efficiency. A decent level of configuration is provided, and the product seems to run smoothly and respond to adjustment rapidly. There



System resource usage	RAM use increase – idle system	RAM use increase – heavy file access	CPU use increase – heavy file access
Agnitum Outpost	13.96%	13.17%	36.75%
AhnLab V3Net	8.30%	6.95%	45.69%
avast! Server	6.06%	5.58%	21.52%
AVG I.S. Network Edition	8.75%	9.44%	66.80%
Avira AntiVir Windows Server	19.54%	19.56%	25.71%
BitDefender Security	6.82%	7.46%	34.01%
Bkis BKAV Gateway Scan*	35.64%	49.13%	111.49%
Bkis BKAV Gateway Scan Plus*	10.78%	10.69%	114.05%
Bkis BKAV Home Edition*	9.50%	9.07%	113.11%
Bkis BKAV Home Edition Plus*	10.10%	9.65%	111.55%
Central Command Vexira	6.59%	6.43%	48.03%
Coranti Multicore	21.86%	22.67%	136.77%
Defenx Security Suite	9.61%	10.00%	44.01%
Digital Defender	6.62%	5.60%	57.96%
eEye Blink Server*	14.52%	13.66%	108.08%
eScan I.S. Suite	4.84%	5.34%	19.61%
ESET NOD32 Antivirus	6.74%	5.19%	54.56%
Fortinet FortiClient	5.54%	8.21%	28.58%
Frisk F-PROT	5.15%	3.73%	93.83%
F-Secure AntiVirus	6.96%	6.53%	64.68%
G DATA AntiVirus	7.86%	6.28%	67.47%
Kaspersky Anti-Virus 6	7.70%	7.35%	35.63%
Kaspersky Anti-Virus 8	8.05%	6.90%	42.47%
Kingsoft 2011 Advanced	6.67%	6.10%	21.36%
Kingsoft 2011 Standard	8.56%	7.27%	21.68%
McAfee VirusScan	3.97%	2.87%	58.14%
Norman Endpoint Protection*	12.72%	12.72%	113.84%
Quick Heal AntiVirus	19.85%	18.80%	42.07%
Rising I.S.*	3.62%	3.87%	117.67%
Sophos Endpoint	6.39%	5.48%	62.14%
SPAMfighter VIRUSfighter	28.27%	5.11%	60.50%
Trustport AntiVirus 2010	10.46%	14.50%	77.89%
VirusBuster	15.70%	15.56%	44.89%

*CPU use more than doubled

are a number of additional protective layers, including the vulnerability management which is the firm's forte.

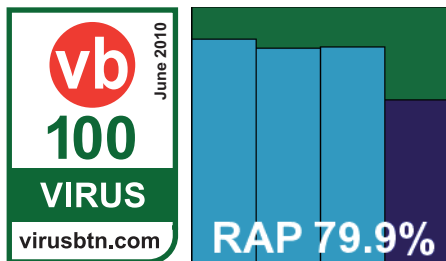
One oddity was noted when a large scan job, which ran for over 36 hours, came to an end without quite covering the full area requested, skipping over the last few folders. There was not enough time to retry the whole job, so just those sections of the test set that had clearly been missed out were re-scanned separately.

On-demand scanning speeds were rather languorous, thanks to the implementation of *Norman's Sandbox* to thoroughly investigate unknown items, and lag times and RAM usage were also fairly high, with CPU cycle usage in high activity periods considerably higher than most products. Detection rates were reasonable in most sets, with the clean set handled without problems, but in the WildList set a tiny number of examples of the W32/Virut strain which also caused the product problems last time went undetected. Although only falling short of the required 100% by a whisker, *Blink* misses out on a VB100 award once again.

eScan Internet Security Suite for Windows 10.0.1058.690

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	93.06%
Worms & bots	96.50%	False positives	0

The latest version of *eScan's* suite provides a number of additional protective layers not covered by our testing, but installs easily and is fairly simple to operate. The logically designed



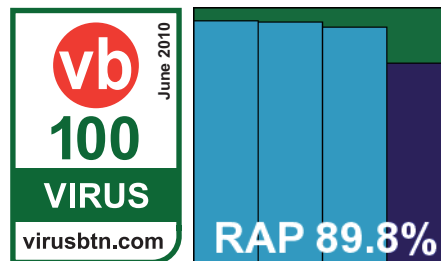
interface provides a decent range of fine-tuning options in an easily accessible way. Scanning speeds were sluggish in the extreme on demand, with some optimization apparent on rescans in some areas but not in others. On-access overheads were fairly low however, and resource consumption not too intrusive.

Detection rates were pretty solid, with high scores in the main sets and a decent showing in the RAP sets. The WildList caused no problems, and with no nasty surprises in the clean sets, *eScan* earns a VB100 award.

ESET NOD32 Antivirus 4.2.40.0

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	96.73%
Worms & bots	99.15%	False positives	0

Little has changed about *ESET's* *NOD32* for some time, only a few adjustments having been made since a major redesign



a few years ago. It remains attractive to look at as well as easy to use. The installation process is fairly standard – enlivened only by the unusual feature of requiring the user to make a choice as to whether or not to detect greyware items – and does not require a reboot to complete. The interface is clear and detailed, with an excellent selection of configuration options, some of which are a little repetitive in places but generally logically and clearly laid out. During testing the interface appeared to freeze up a few times when asked to do more work while under heavy stress, but it soon recovered its composure and continued to get on with the job under the hood.

Scanning speeds were medium, with on-access lags and CPU usage also in the middle of the field; memory usage was fairly low, however. Detections rates were excellent, showing a continuation of the upward trend seen in the last few tests. A couple of items in the clean set were alerted on as potentially unwanted – a fairly accurate description of toolbars and other functions bundled with popular freeware packages – but no false alarms were noted and the WildList was handled flawlessly, earning *ESET* yet another VB100 award.

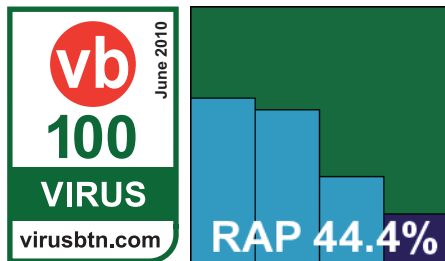
Fortinet FortiClient 4.1.3.143

ItW	100.00%	Polymorphic	99.08%
ItW (o/a)	100.00%	Trojans	70.61%
Worms & bots	89.64%	False positives	0

Fortinet's endpoint client seems fairly unchanged from several recent tests, although during the simple and speedy install an option to select a free or premium version of the product was something of a surprise. The interface is nice and clear and provides a fair degree of configuration, but a few problems were noted during testing; on-access scanning appeared initially to be inactive, but after a reboot (not

On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	1.67	27.45	1.67	17.37	223.39	17.37	9.14	31.85	9.14	10.75	93.81	10.75
AhnLab V3Net	5.17	5.18	5.17	13.76	20.76	13.76	18.49	21.84	18.49	14.53	21.06	14.53
avast! Server	277.23	308.03	7.35	37.53	37.83	30.27	36.99	40.95	29.40	49.14	51.59	24.00
AVG I.S. Network Edition	0.69	346.53	0.69	15.80	32.13	15.80	7.45	7.59	7.45	5.49	5.61	5.49
Avira AntiVir Windows Server	7.13	7.15	7.13	49.91	49.38	49.91	31.41	26.66	31.41	31.27	21.50	31.27
BitDefender Security	184.82	198.02	184.82	20.85	20.76	20.85	16.04	16.62	16.04	13.76	14.33	13.76
Bkis BKAV Gateway Scan	99.01	99.01	NA	4.13	4.26	4.13	4.82	5.00	4.25	4.19	4.11	3.85
Bkis BKAV Gateway Scan Plus	99.01	99.01	NA	4.39	4.32	4.32	4.90	5.45	5.45	4.16	4.09	4.09
Bkis BKAV Home Edition	99.01	99.01	NA	4.38	4.25	4.25	5.97	4.90	4.90	4.19	4.13	4.13
Bkis BKAV Home Edition Plus	99.01	99.01	NA	4.38	4.29	4.29	4.90	5.21	5.21	4.09	4.16	4.16
Central Command Vexira	10.15	10.19	3.21	24.43	24.31	3.02	22.26	18.34	4.25	19.84	16.38	2.90
Coranti Multicore	2.47	2.48	2.39	6.64	6.67	5.13	2.92	2.88	2.89	2.49	2.37	2.26
Defenx Security Suite	1.69	27.45	1.69	17.31	234.56	17.31	9.10	32.30	9.10	10.64	93.81	10.64
Digital Defender	4.44	4.62	NA	13.88	15.08	13.88	20.66	16.38	20.66	19.47	14.33	19.47
eEye Blink Server	1.97	1.95	1.82	3.35	3.34	3.33	4.09	4.09	4.09	3.05	3.04	3.05
eScan I.S. Suite	0.45	1.05	0.45	0.08	0.62	0.08	0.47	0.50	0.47	0.63	0.55	0.63
ESET NOD32 Antivirus	3.54	3.53	3.54	10.20	10.24	10.20	15.49	16.15	15.49	14.14	14.53	14.14
Fortinet FortiClient	6.15	7.24	6.15	4.47	11.41	4.47	29.78	32.76	29.78	13.06	19.11	13.06
Frisk F-PROT	11.09	11.13	11.09	17.97	17.77	17.77	36.40	40.23	36.40	29.48	29.48	29.48
F-Secure AntiVirus	924.09	462.05	2.81	23.22	27.27	21.42	19.43	21.84	14.51	79.38	103.19	12.28
G DATA AntiVirus	4.41	2772.27	4.41	24.06	4691.22	24.06	14.42	458.62	14.42	11.47	343.96	11.47
Kaspersky Anti-Virus 6	5.38	2772.27	5.38	17.97	1563.74	17.97	7.91	286.64	7.91	5.90	257.97	5.90
Kaspersky Anti-Virus 8	2.92	924.09	2.92	13.88	234.56	13.88	7.77	38.22	7.77	6.45	29.48	6.45
Kingsoft 2011 Advanced	2.29	2.30	2.29	27.12	26.96	26.96	8.92	8.92	8.92	17.79	20.23	20.23
Kingsoft 2011 Standard	2.31	2.29	2.31	27.76	28.09	27.76	9.10	9.10	9.10	18.43	19.84	18.43
McAfee VirusScan	115.51	120.53	2.97	18.11	18.18	16.75	11.82	11.24	11.02	8.60	7.88	7.70
Norman Endpoint Protection	1.40	1.40	NA	3.34	3.34	3.34	4.12	3.95	4.12	3.10	2.97	3.10
Quick Heal AntiVirus	3.95	3.97	2.66	47.39	47.87	47.39	11.13	11.52	11.13	12.14	13.40	12.14
Rising I.S.	2.10	2.09	2.10	10.99	10.76	10.99	5.96	5.96	5.96	9.92	10.02	9.92
Sophos Endpoint	396.04	138.61	396.04	15.08	15.13	15.08	23.16	24.14	23.16	13.76	14.33	13.76
SPAMfighter VIRUSfighter	4.46	4.56	NA	13.25	13.52	13.25	15.92	16.04	15.92	13.76	13.76	13.76
Trustport AntiVirus 2010	2.13	2.14	2.13	11.73	13.37	13.37	13.37	10.57	7.01	4.30	4.76	4.30
VirusBuster	10.27	10.15	10.27	24.56	24.56	24.56	24.56	18.80	19.11	16.38	17.20	16.38

demanded by the installer) this was rectified. Also, an attempt to run some jobs on the scheduler failed to produce any scanning.



Further upsets were to follow, with both on-demand and on-access tests freezing and hanging frequently throughout scanning of the trojans and RAP sets. Some samples in the test sets appeared to trip up the engine, meaning that during the on-access tests the machine would occasionally start moving extremely slowly, while it was clear that all on-access detection had ceased. Oddly, after several forced reboots and continuations with the offending portions of the sets removed, we eventually found that protection could be restored simply by switching the on-access protection off and back on again (no easy task given the state of the machine, with every click taking an age to have any effect and the whole experience feeling like pushing a bus with no wheels up a steep slope). As the on-access tests would continue while this process was performed, it may have caused some samples to go undetected which would have been spotted had the product been fully functional, but given the time already taken up there seemed to be no other option.

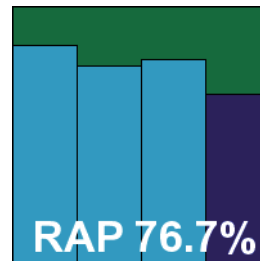
The RAP tests were even more problematic, with numerous attempts to get through the sets failing, including one overnight attempt which stuck after about 500 samples and sat there all night insisting it was still scanning but making no further progress – the task had to be forcibly killed to allow further interaction with the product. Blocks of samples had to be removed to obtain complete results.

Scanning speeds were obtained, which were fairly decent, with mid-range overheads and resource consumption. Detection results for the main sets also proved reasonable, given the somewhat anomalous figures for the trojans set; the low RAP scores may suffer from the same effect. With the WildList and clean sets handled without problems, the product just about scrapes through to earn a VB100 award, but admins will be well advised to keep a close eye on the product to ensure it doesn't get itself snarled up.

Frisk F-PROT 6.0.9.3

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	98.26%	Trojans	79.41%
Worms & bots	92.41%	False positives	0

Frisk's product remains simple in the extreme, with an installation process which completes quickly in only a handful of stages; a reboot is required to complete. The pared-down interface provides a basic set of controls, and its simplicity makes it hard to get lost in, but does have a few odd little quirks which may confuse users who are not used to the design.

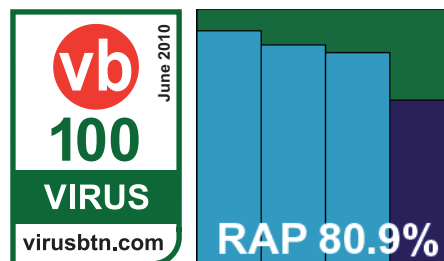


Testing proceeded smoothly, with some good scanning speeds recorded and no complaints about the on-access overheads either; memory use was fairly low while quite heavy use was made of CPU cycles. Scanning the main sets produced some decent scores, but in the RAP sets the product reported errors several times, on occasion requiring a reboot to return the scanner to a usable state. On-access protection remained stable throughout despite these problems. RAP scores, once fully obtained, proved pretty decent, and all was well in the clean sets. The WildList was handled well on demand, but despite all looking good, one more fly appeared in the ointment on checking the on-access results – a handful of samples, detected without problems on demand, were ignored by the on-access scanner. The fact that these samples were all detected on demand with the same detection ID hints at some error in the set-up of the on-access component. A VB100 award remains just out of Frisk's grasp this month.

F-Secure AntiVirus for Windows Servers 9.00 build 333

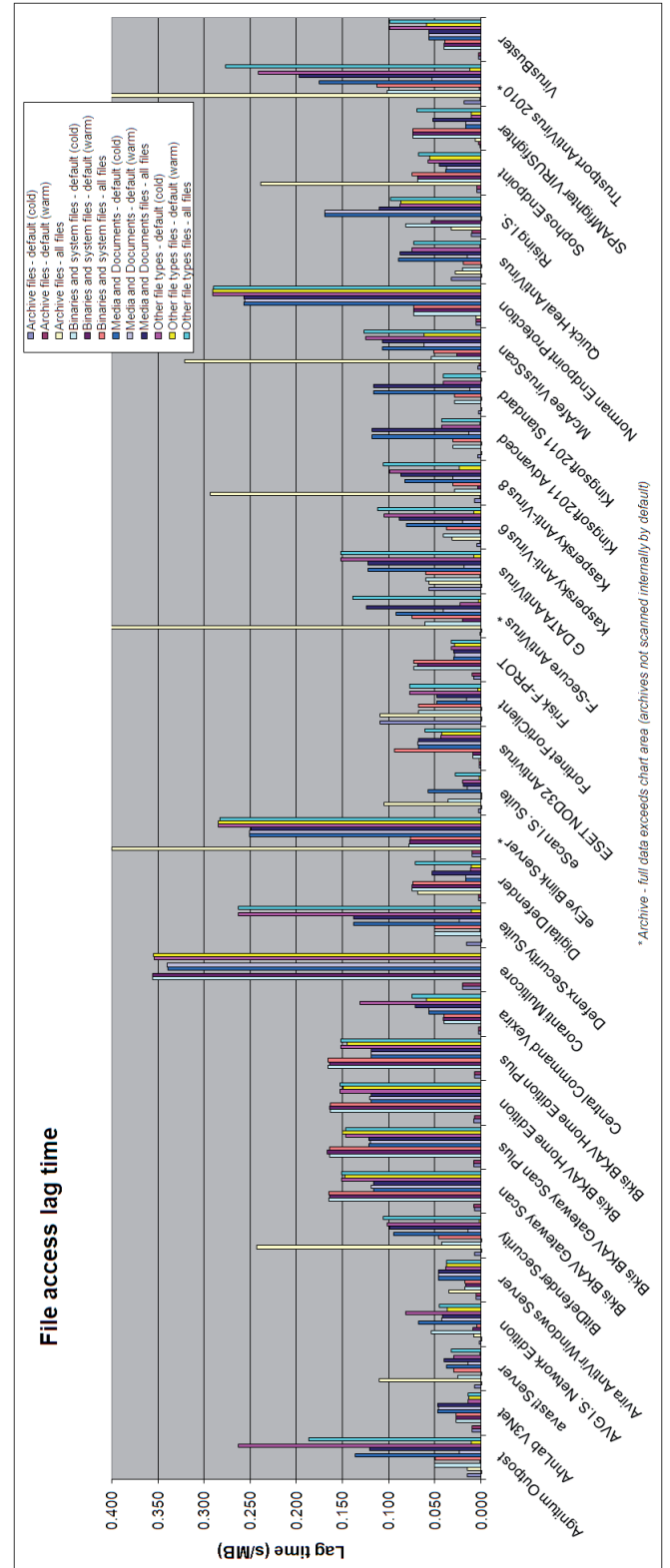
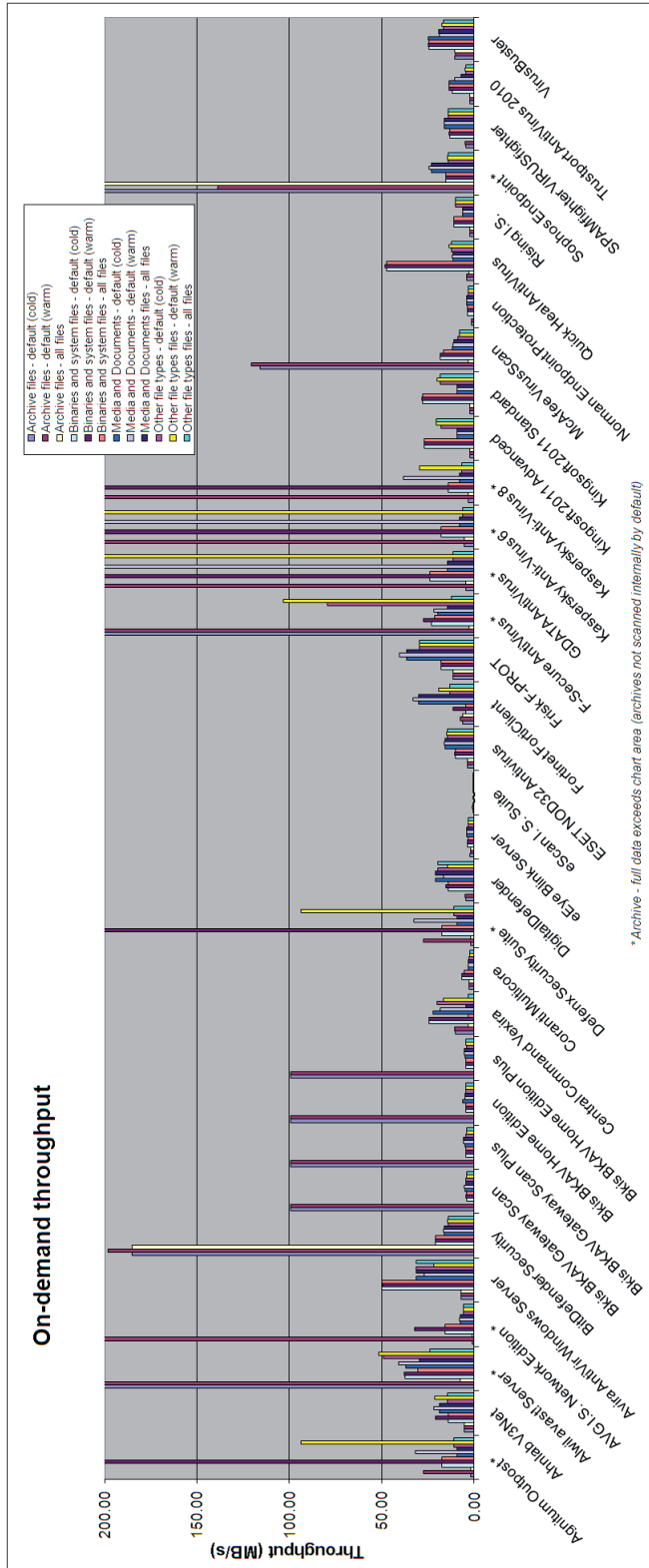
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.03%
Worms & bots	93.43%	False positives	0

F-Secure's server-level product installs fairly simply, with no reboot requested, although we chose to restart



the machine as a precaution after manually applying updates. The interface is web-based, which caused some rather disconcerting alerts from the locked-down browser warning of untrusted sites and defunct certificates; doubtless these problems would be mitigated on a

File access lag time (s/MB)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	0.015	0.000	0.015	0.051	0.001	0.050	0.136	0.024	0.121	0.263	0.010	0.187
AhnLab V3Net	0.010	0.010	NA	0.027	0.027	0.027	0.046	0.046	0.046	0.014	0.013	0.014
avast! Server	0.007	0.000	0.110	0.025	0.000	0.030	0.037	0.014	0.040	0.029	0.001	0.032
AVG I.S. Network Edition	0.001	0.000	0.007	0.053	0.008	0.004	0.067	0.043	0.042	0.082	0.036	0.045
Avira AntiVir Windows Server	0.006	0.005	0.034	0.017	0.016	0.017	0.046	0.046	0.046	0.038	0.037	0.037
BitDefender Security	0.007	0.000	0.243	0.042	0.000	0.046	0.095	0.014	0.099	0.102	0.001	0.106
Bkis BKAV Gateway Scan	0.007	0.007	NA	0.165	0.164	0.165	0.116	0.119	0.116	0.151	0.147	0.151
Bkis BKAV Gateway Scan Plus	0.007	0.007	NA	0.164	0.166	0.164	0.122	0.120	0.122	0.146	0.150	0.146
Bkis BKAV Home Edition	0.007	0.007	NA	0.163	0.164	0.163	0.118	0.121	0.118	0.152	0.149	0.152
Bkis BKAV Home Edition Plus	0.007	0.007	NA	0.166	0.164	0.166	0.119	0.119	0.119	0.151	0.145	0.151
Central Command Vexira	0.002	0.002	NA	0.040	0.041	0.040	0.056	0.056	0.071	0.131	0.059	0.074
Coranti Multicore	0.020	0.020	NA	0.356	0.356	NA	0.340	0.340	NA	0.354	0.355	NA
Defenx Security Suite	0.015	0.000	NA	0.050	0.001	0.050	0.138	0.024	0.138	0.263	0.010	0.263
Digital Defender	0.003	0.003	0.068	0.074	0.074	0.074	0.017	0.016	0.053	0.011	0.010	0.071
eEye Blink Server	0.009	0.009	0.400	0.078	0.078	0.077	0.251	0.250	0.249	0.284	0.285	0.283
eScan I.S. Suite	0.003	0.000	0.105	0.036	0.000	0.000	0.057	0.014	0.019	0.020	0.002	0.028
ESET NOD32 Antivirus	0.002	0.002	0.002	0.008	0.008	0.094	0.068	0.068	0.068	0.043	0.043	0.060
Fortinet FortiClient	0.109	0.000	0.109	0.068	0.000	0.068	0.048	0.016	0.048	0.077	0.003	0.077
Frisk F-PROT	0.008	0.010	NA	0.073	0.069	0.073	0.030	0.029	0.030	0.032	0.029	0.032
F-Secure AntiVirus	0.001	0.000	0.421	0.061	0.020	0.074	0.092	0.041	0.124	0.023	0.003	0.139
G DATA AntiVirus	0.057	0.000	0.057	0.060	0.001	0.060	0.122	0.018	0.122	0.151	0.007	0.151
Kaspersky Anti-Virus 6	0.005	0.001	0.031	0.041	0.001	0.037	0.081	0.020	0.088	0.105	0.008	0.112
Kaspersky Anti-Virus 8	0.007	0.001	0.294	0.029	0.003	0.030	0.082	0.031	0.087	0.099	0.023	0.105
Kingsoft 2011 Advanced	0.003	0.000	NA	0.030	0.000	0.030	0.118	0.013	0.118	0.042	0.000	0.042
Kingsoft 2011 Standard	0.003	0.000	NA	0.029	0.000	0.029	0.116	0.012	0.116	0.040	0.000	0.040
McAfee VirusScan	0.003	0.001	0.321	0.054	0.026	0.052	0.107	0.062	0.106	0.125	0.062	0.127
Norman Endpoint Protection	0.005	0.005	0.005	0.073	0.073	0.073	0.257	0.256	0.257	0.291	0.290	0.290
Quick Heal AntiVirus	0.032	0.000	0.028	0.020	0.000	0.019	0.089	0.014	0.088	0.075	0.001	0.073
Rising I.S.	0.010	0.010	0.032	0.081	0.054	0.000	0.169	0.169	0.111	0.088	0.087	0.098
Sophos Endpoint	0.004	0.004	0.238	0.069	0.069	0.075	0.039	0.038	0.045	0.057	0.056	0.068
SPAMfighter VIRUSfighter	0.001	0.002	0.006	0.074	0.074	0.074	0.016	0.016	0.052	0.011	0.010	0.070
Trustport AntiVirus 2010	0.018	0.001	0.729	0.101	0.002	0.113	0.175	0.053	0.197	0.241	0.012	0.277
VirusBuster	0.002	0.003	NA	0.040	0.040	0.040	0.056	0.056	0.056	0.099	0.059	0.099



system with a web connection (which not all servers will necessarily have). The design of the interface is clear and it looks attractive, but the scan design is somewhat clunky and the scheduler system is fairly basic. Only a single job can be set up with the standard settings of the manual scanner – more demanding admins may want considerably more flexibility to run various scheduled jobs – and even selecting more than a single folder is not at all simple. We also noticed on a few occasions the manual scanner settings reverting to previous options despite changes having apparently been applied successfully.

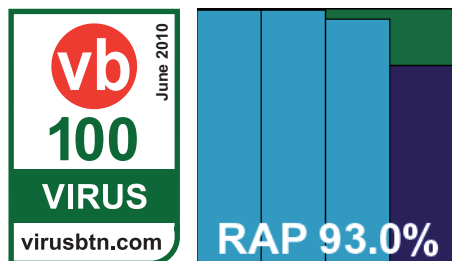
With these quirks observed and noted, scanning proceeded fairly well, with some excellent speed measures, fairly light resource usage and decent scores in the main sets on access. On demand, however, we found logging something of a problem – an issue we have noted before with *F-Secure* products. Twice we ran the standard large job scanning the usual selection of test sets, but on both occasions although the results screen showed large numbers of detections, clicking the ‘show log’ button brought up details of the previous scan – a clean job with nothing to report. In the end, a command-line version of the scanner bundled with the product was used to get results, and the issue seemed only to affect scans with large numbers of detections. This may be an unlikely scenario in the real world, but is not inconceivable in a large file server environment – most server administrators will want considerably more detailed, trackable, and most of all reliable logging from a serious server-grade product. The developers have made some urgent investigations into the problems we encountered and have promised a rapid fix.

Despite our logging issues, detection rates across the sets proved very solid, and with no problems in the WildList or clean sets *F-Secure* earns a VB100 award.

G DATA AntiVirus 10.5.132.28

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	99.33%
Worms & bots	93.82%	False positives	0

G DATA's server product has appeared in a previous comparative with only German-language interfaces, but this time a full translation was provided, allowing



much more thorough investigation of its capabilities. The set-up process is slightly complex, with an administration element installed first and the client protection deployed from there. This seemed a very proper approach to corporate usage, and worked fairly well. Some error messages were shown during the installation of the management tool, related to the .NET and SQL Server components bundled with it, but these seemed to present no serious problem. Everything was soon up and running, and deployment of the client protection ran very smoothly and simply.

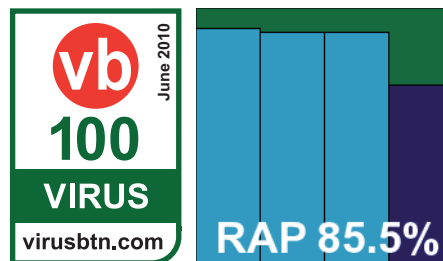
Running through scans was fairly easy too, with some excellent optimization of scanning of previously checked files and a surprisingly light imprint on memory and processor cycles. Occasionally the connection to the admin tool was lost and had to be re-initialized, and on completion of large scan jobs we had some problems exporting logs to file, with the export function failing silently on several occasions. Eventually we gave up on it and resorted to ripping the data from some temporary cache files uncovered by digging through the registry.

The data obtained showed the product's usual superb detection levels across all sets, with no issues in the clean or WildList sets, and *G DATA* earns a VB100 award despite a few frustrations in the product.

Kaspersky Anti-Virus 6 for Windows Servers 6.0.4.1424

























ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	94.99%
Worms & bots	98.33%	False positives	0

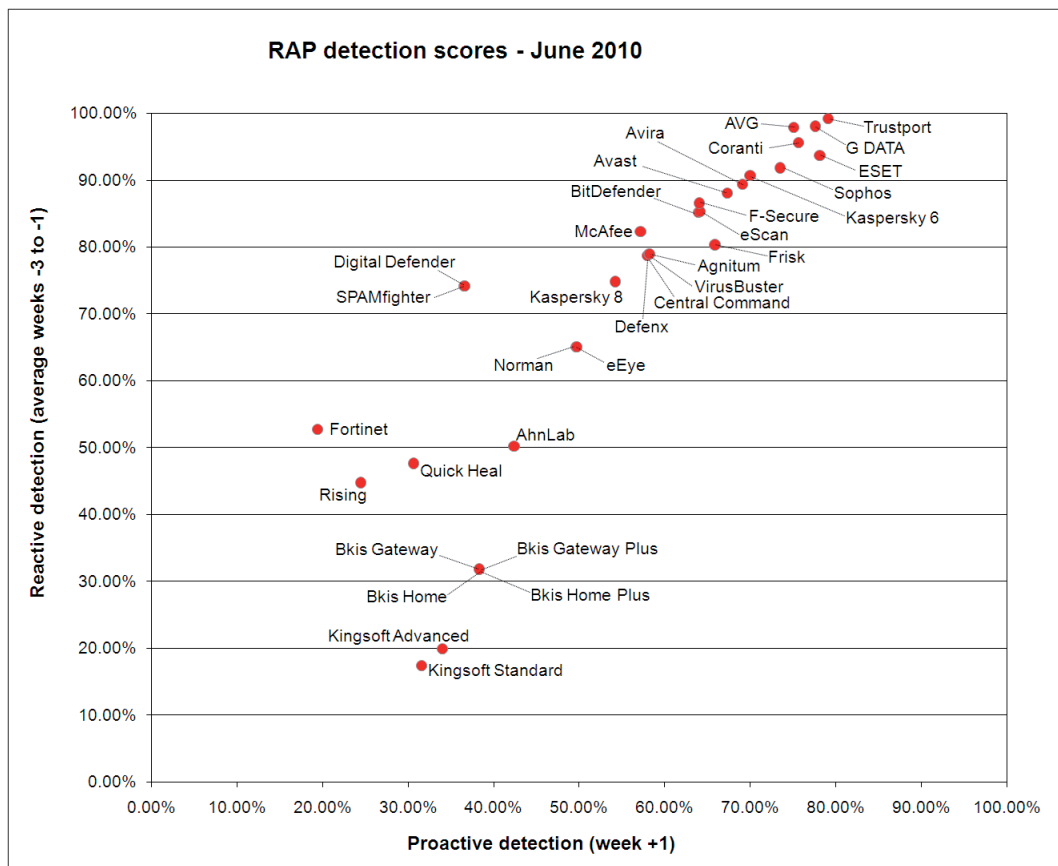
Kaspersky Lab entered two products this month, the first apparently being the current standard product.



The install and set-up is a fairly simple and painless process, and the interface is another based on the MMC, with some nice use of colour to give it a little clarity. It proved fairly easy to use if somewhat complex, and provided an excellent level of configuration for the server administrator.

Scanning speeds were good, with previously scanned files effortlessly ignored, resource usage on the low side

Reactive and Proactive (RAP) detection scores	Reactive			Reactive average	Proactive week +1	Overall average
	week -3	week -2	week-1			
Agnitum Outpost 	84.65%	73.41%	78.90%	78.99%	58.27%	73.81%
AhnLab V3Net 	57.37%	41.27%	52.15%	50.26%	42.38%	48.29%
avast! Server 	88.63%	89.67%	85.84%	88.05%	67.32%	82.87%
AVG I.S. Network Edition 	98.28%	98.73%	96.56%	97.86%	75.07%	92.16%
Avira AntiVir Windows Server 	93.39%	89.01%	85.83%	89.41%	69.11%	84.33%
BitDefender Security 	87.59%	83.66%	84.62%	85.29%	64.16%	80.01%
Bkis BKAV Gateway Scan	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Gateway Scan Plus	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Home Edition	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Bkis BKAV Home Edition Plus	46.69%	22.42%	26.49%	31.86%	38.28%	33.47%
Central Command Vexira 	84.52%	73.39%	78.88%	78.93%	58.17%	73.74%
Coranti Multicore 	99.18%	93.69%	93.94%	95.60%	75.64%	90.61%
Defenx Security Suite 	84.37%	73.16%	78.58%	78.70%	57.96%	73.52%
Digital Defender	81.68%	71.88%	68.88%	74.15%	36.53%	64.74%
eEye Blink Server	65.46%	65.87%	63.97%	65.10%	49.72%	61.25%
eScan I.S. Suite 	87.49%	83.65%	84.40%	85.18%	63.94%	79.87%
ESET NOD32 Antivirus 	94.51%	94.42%	92.02%	93.65%	78.14%	89.77%
Fortinet FortiClient 	64.39%	59.97%	34.00%	52.78%	19.41%	44.44%
Frisk F-PROT	84.77%	76.78%	79.50%	80.35%	65.87%	76.73%
F-Secure AntiVirus 	91.21%	85.83%	82.62%	86.55%	64.07%	80.93%
G DATA AntiVirus 	99.31%	99.28%	95.63%	98.07%	77.62%	92.96%
Kaspersky Anti-Virus 6 	91.93%	90.06%	90.06%	90.68%	69.99%	85.51%
Kaspersky Anti-Virus 8 	85.59%	65.42%	73.47%	74.83%	54.24%	69.68%
Kingsoft 2011 Advanced 	25.42%	12.46%	22.10%	19.99%	34.03%	23.50%
Kingsoft 2011 Standard 	22.01%	10.36%	20.03%	17.46%	31.53%	20.98%
McAfee VirusScan 	87.83%	81.72%	77.48%	82.34%	57.15%	76.05%
Norman Endpoint Protection	65.52%	65.79%	63.91%	65.07%	49.64%	61.21%
Quick Heal AntiVirus 	56.03%	43.07%	43.93%	47.67%	30.61%	43.41%
Rising I.S. 	52.90%	45.67%	35.77%	44.78%	24.45%	39.70%
Sophos Endpoint 	93.94%	91.47%	90.14%	91.85%	73.53%	87.27%
SPAMfighter VIRUSfighter	81.72%	71.90%	68.84%	74.15%	36.61%	64.77%
Trustport AntiVirus 2010 	99.64%	99.58%	98.30%	99.17%	79.10%	94.16%
VirusBuster 	84.52%	73.39%	78.88%	78.93%	58.17%	73.74%



and detection rates excellent. The only oddity noted was an apparent rescan of infected sets after the job had completed together with a prompt which asked for an action, but this did not affect the gathering of results once the scan was aborted.

The WildList and clean sets were handled well, and a VB100 award is comfortably earned.

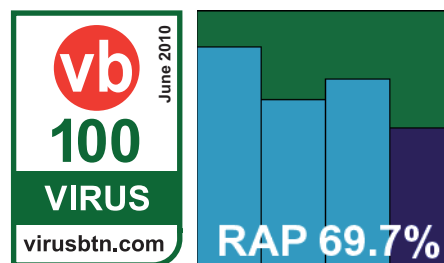
Kaspersky Anti-Virus 8 for Windows Servers Enterprise Edition 8.0.0.354

ItW	100.00%	Polymorphic	99.69%
ItW (o/a)	100.00%	Trojans	94.70%
Worms & bots	98.37%	False positives	0

The second offering from *Kaspersky* this month is a new version, which appears to be in a late stage of beta testing. The install and set-up was a little more complex than the older version, with both a protection client and an administration tool required, but once up and running the MMC interface met with approval from the lab team, who considered its design one of the best approaches to the

format seen this month. The only slight annoyance was the fiddliness of setting scan options, with actions stored in a separate area from the main set-up component, but this was soon dealt with.

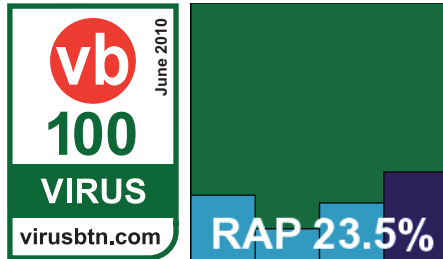
Scanning speeds were once again excellent and benefited hugely from smart optimization with both memory and CPU usage slightly higher than version 6, but barely noticeably. Detection rates were also splendid, although RAP scores were a little down on the other product – presumably due to some heuristic approaches not being included with this version. The WildList set caused no problems though, and the few alerts in the clean set accurately labelled VNC clients as VNC clients – useful information for a corporate admin. *Kaspersky* earns a second VB100 award this month.



Kingsoft Internet Security 2011 Advanced Edition 2008.11.6.63

ItW	100.00%	Polymorphic	57.11%
ItW (o/a)	100.00%	Trojans	15.03%
Worms & bots	35.93%	False positives	0

Kingsoft's latest product installs very simply in just a few clicks, with no need for a reboot. The design is glossy and attractive, but only provides basic configuration and is a little clunky in translation at some points.

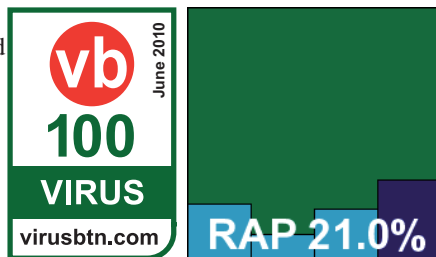


Scanning speeds were reasonable, with a fairly light impact on system performance, but detection rates over recent items were fairly disappointing – although, bizarrely, the proactive week of the RAP sets was handled better than the older samples. No problems were spotted in the WildList or clean sets however, and a VB100 award is duly earned.

Kingsoft Internet Security 2011 Standard Edition 2008.11.6.63

ItW	100.00%	Polymorphic	57.11%
ItW (o/a)	100.00%	Trojans	10.46%
Worms & bots	31.63%	False positives	0

Once again *Kingsoft* provided two products that are almost indistinguishable on the surface, with nothing to indicate which is the standard and which the advanced, other than the name of the installer.

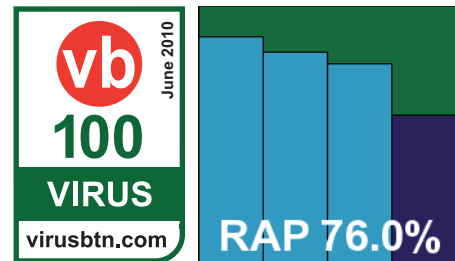


The installation and user experience were identical, with even more lamentable detection rates in many of the sets, but the certification requirements were met comfortably and *Kingsoft* earns a second VB100 award this month despite a rather poor RAP showing.

McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	Polymorphic	99.99%
ItW (o/a)	100.00%	Trojans	85.84%
Worms & bots	93.69%	False positives	0

McAfee's corporate product is an old faithful, remaining pretty unchanged for many years now, but there seems



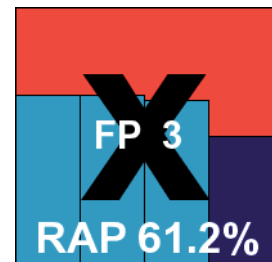
no need to mess with such a solid and business-like tool. Installation is fast and simple, requesting a reboot to engage some of the network protection but not requiring it to get the core malware protection enabled. Running through the tests was as smooth and efficient a process as ever, with decent scanning speeds, on-access overheads and CPU use somewhat above average, but memory consumption the lowest of all products tested this month.

Detection rates were similarly reliable across all sets, with no problems in the WildList or clean sets, thus *McAfee* earns a VB100 award and extra commendation for solidity and problem-free testing.

Norman Endpoint Protection 7.20

ItW	99.99%	Polymorphic	83.09%
ItW (o/a)	99.99%	Trojans	74.87%
Worms & bots	72.57%	False positives	3

Norman's server product installs in a few standard steps and needs no reboot to get down to business. The interface is closely modelled on the desktop versions seen in previous comparatives, with a fairly simple design and a fair level of options for the server admin, laid out in a rational and intuitive manner.



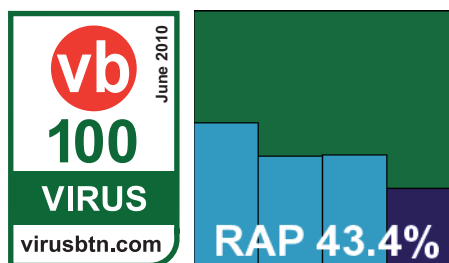
With the heavy use of the firm's renowned sandbox for additional protection against new threats, scanning speeds were fairly sluggish, particularly over executables, and on-access overheads and resource usage similarly high.

Detection rates were reasonable in the main sets and the RAP batches, but in the WildList set – as feared having already seen the results of other products using the *Norman* engine – a tiny number of W32/Virut samples went undetected. In the clean set, a batch of files included in the *Sun Java SDK* were detected as, of all things, *JAVA/SMSsend.B* trojans, making doubly sure that no VB100 award can be earned by *Norman* this month.

Quick Heal AntiVirus 2010 Server Edition 11.00/4.0.0.3

ItW	100.00%	Polymorphic	99.50%
ItW (o/a)	100.00%	Trojans	76.95%
Worms & bots	89.49%	False positives	0

Quick Heal's server edition seems little different from its desktop versions, with the usual fast and simple install process with no reboot needed.



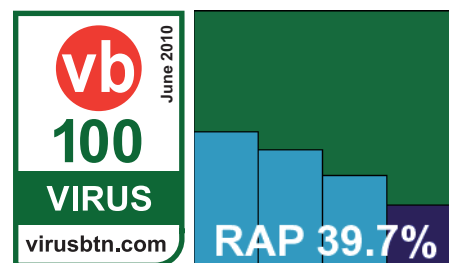
The interface is similarly simple to use, and ran stably throughout the test. Scanning speeds were pretty good, and on-access overheads fairly decent too, with a surprisingly high amount of RAM used but CPU use lower than many in this month's field.

Detection rates were reasonable in the main sets, a little below par in the RAP sets, but the core requirements of the clean sets and WildList samples were handled flawlessly, and a well-behaved product earns *Quick Heal* another VB100 award.

Rising Internet Security 2010 22.00.02.96

ItW	100.00%	Polymorphic	70.27%
ItW (o/a)	100.00%	Trojans	48.78%
Worms & bots	58.41%	False positives	0

Rising's 2010 edition is colourful and cartoony, with an installation process of average length and complexity.



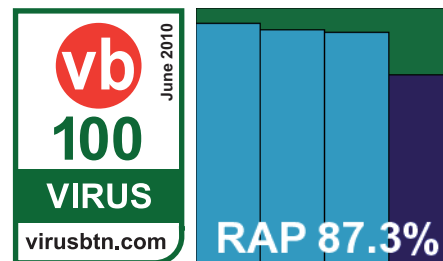
The GUI provides a decent level of configuration, which is mostly fairly accessible but in places it can be a little laborious to implement certain changes. Some nice graphs and other statistical data are provided alongside the standard logging subsection.

On-demand scanning speeds were unspectacular, and on-access overheads fairly high, with impressively low memory consumption and CPU usage remarkably high. Detection rates across the sets were fairly mediocre, with RAP scores tumbling as the samples grew more recent, but the WildList was handled without difficulty and no problems emerged in the clean sets either, thus earning *Rising* another VB100 award.

Sophos Endpoint Security and Control 9.0.5/4.52G

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	91.22%
Worms & bots	98.25%	False positives	0

Sophos's latest offering remains little changed from previous versions, with numerous new features stealthily merged in



without any major redesign of the interface. The interface itself is fairly simple to navigate and provides a truly remarkable degree of fine-tuning, much of it located in a super-advanced area which we refrained from meddling with. Installation is simple and clear, and completed rapidly with no requirement for a reboot.

Performance tests showed some fairly average scanning speeds and on-access overheads, and pretty low resource consumption. Running the main detection tests was a little more problematic however, after an initial attempt to run a scheduled scan overnight failed with cryptic error messages hinting at a lack of space. Attempting to open the product's log file drew the same error, although the system partition had at least 20GB free – surely plenty to allow a log to be loaded.

A reboot quickly put a stop to this silliness and tests proceeded without further interruption, although not as quickly as the progress bar would have us believe (as in many previous tests, it quickly leapt to 99% and remained there for well over 99% of the scanning time). In the

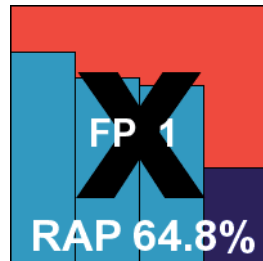
main sets detection rates were excellent, but a first stab at the RAP sets showed some bizarrely low and irregular figures. A retry showed the scanner getting stuck on a file on at least a couple of attempts, and in the end results were obtained with the offending item removed from the set, and using the command line scanner provided with the product for speed (considerably more than the allotted time having already been taken up). Results proved well worth the wait however, with excellent scores across all four weeks, the proactive week particularly impressive.

The WildList and clean sets caused no difficulties though, and *Sophos* also earns another VB100 award.

SPAMfighter VIRUSfighter 6.101.6

ItW	100.00%	Polymorphic	71.61%
ItW (o/a)	100.00%	Trojans	87.09%
Worms & bots	88.82%	False positives	1

Yet another repeat appearance from one of last month's newcomers, *VIRUSfighter* is one of many implementations of the popular *VirusBuster* engine. A simple and rapid installation process requires no reboot and results in a fairly attractive interface which is reasonably simple to operate.



A pretty limited set of controls is provided – suitable for the home user but unlikely to appeal to the server administrator. On-demand scans from the GUI can only target whole disk partitions, so most tests were run using the context-menu option.

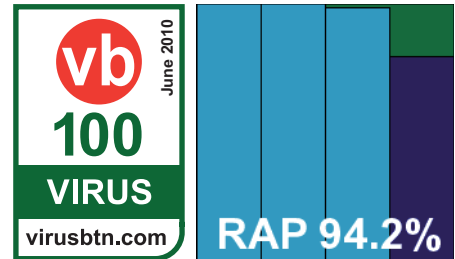
Running some of the larger detection tests proved a little problematic, with scans failing, hanging or crashing a number of times. On some occasions the product reported that scanning was still ongoing long after the logs showed having reached the end of the sets – which made it a little tricky to guess when something was, in fact, finished.

Detection results in the main sets and RAP batches were reasonable, more closely mirroring *Digital Defender* (with which the product shares some ancestry) than the core *VirusBuster* product on which it is ultimately based. While the WildList was handled adequately, as expected, a single item in the clean sets – that pesky *Microsoft* howto document – was labelled as exploited, and as a result *SPAMfighter* narrowly misses out on a VB100 award this month.

Trustport AntiVirus 2010 5.0.0.4118

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.55%
Worms & bots	98.95%	False positives	0

Trusty *Trustport* is put in place with a fairly fast set-up process, and provides a sturdy, business-like interface.



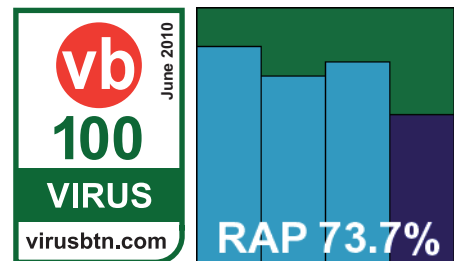
A very good amount of configuration and fine-tuning is offered, which is arrayed sensibly to allow easy access to all the required options. Running through the tests was smooth and simple, although the product's dual-engine approach caused the scans to be somewhat slower than most, with on-access overheads and resource consumption somewhat higher.

However, detection rates were pretty stratospheric, with an awesome display in the RAP sets which could well be our highest ever score. The WildList presented no difficulties, and with no false alarms either *Trustport* romps home to another easy VB100 award.

VirusBuster for Windows Servers 6.2.51

ItW	100.00%	Polymorphic	89.10%
ItW (o/a)	100.00%	Trojans	90.24%
Worms & bots	95.95%	False positives	0

We have already seen the *VirusBuster* engine in use several times this month, and even the interface for this server edition



made an appearance earlier in the *Vexira* product. The MMC-based system provides a reasonable degree of control, although many of the controls are somewhat fiddly to operate and there is a lack of consistency in the implementation. Monitoring the progress of jobs is also somewhat problematic.

Nevertheless, testing progressed without any major obstacles, and results were much as expected, with a decent showing in the main sets, reasonable scores in the RAP sets and mid-range performance figures. No problems were encountered in the WildList or clean sets, and *VirusBuster* proves worthy of a VB100 award this month.

CONCLUSIONS

It proved to be another somewhat exhausting test this month, with pressure on the lab team not helped by some illness during the course of the month, and the attendance of technical meetings and conferences abroad. This would have been less of a problem had the products played nicely and behaved as well as we had hoped. With a tight schedule and limited testing resources, we allocated an ideal 24 machine/hours per product – we felt that this was not an unreasonable estimate of the time it should take to complete all the required tests, and many products easily got through all the sets and the various iterations of the performance measures within this time period.

However, several other products were less than cooperative. Many an evening we left the lab fully expecting to find several sets of completed results by morning, only to be disappointed on our return with products stuck on odd files, claiming completion but actually having skipped chunks of the sets, or completed but having failed to record accurate results of what they had been up to. A further handful of products submitted to the test took up their share of testing time – and in some cases more than their fair share – but in the end were excluded from the test due to various problems: incompatibility with the test platform, problems applying updates, or difficulties obtaining enough usable results for it to be worthwhile including them.

These inconsistencies and unreliable behaviours are particularly significant on a server platform, where administrators require absolute trustworthiness and total trackability of all activities, especially regarding detections and attempts at disinfection. In many products this month – even those claiming to be aimed at the server sphere – we noted shortcomings in configuration as well, with some vital tools and options required by many admins either missing or not fully functioning.

Of course, a number of the products included in this test provide a range of additional capabilities not covered by our tests, but in the server environment much of the purpose of implementing a security solution is to protect things other than the server operating system itself – scanning

and monitoring fileshares and other inter-node connections is vital to prevent cross-contamination, the passing of malicious code from one zone to another – and for such purposes the behavioural layers added to many of the products will be unsuitable. Even some of the cloud-based data provided by some solutions may be inaccessible on a server, depending on the strictness of corporate network set-up. This, then, is one area where ‘traditional’ detection technology remains at the forefront of the protective arsenal. We hope the data provided this month will be a useful resource to assist admins in selecting a suitable product for their purposes.

Among those products which did perform adequately in this test, we saw a fairly wide spread of results. Our performance measures highlighted a range of different approaches, with some using more or less memory than others, some more or less processor cycles; some used more of one than the other, while some were notably high or low on both counts. These performance figures should not, of course, be extrapolated to guess at the exact resource footprint in other circumstances or on other systems (where results could vary considerably), but they should provide a reasonable comparison between the products included in the test.

As far as detection rates are concerned, we have seen some really excellent figures in this test, with several products surpassing expectations while a few have done somewhat less well than expected. Our RAP data and charts also continue to provide plenty of interest.

We will continue to monitor the ever-changing abilities of labs to keep up with the growing glut of malicious code, returning to a desktop platform next time around and doubtless seeing another large haul of competitors on the test bench. We can only hope, for our sanity’s sake, to see some rather better behaviour than that encountered in many solutions this month.

Technical details

All tests were performed on identical systems with AMD Phenom II x2 550 processors at 3.11 GHz, 4 GB RAM, and dual 80 and 500 GB SATA hard drives, running *Microsoft Windows 2008 Server R2 Standard Edition*.

Any developers interested in submitting products for Virus Bulletin’s VB100 comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at <http://www.virusbtn.com/vb100/about/schedule.xml>.

END NOTES & NEWS

MAAWG 19th General Meeting takes place 8–10 June 2010 in Barcelona, Spain. See <http://www.maaawg.org/>.

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>.

The 8th German Anti Spam Summit takes place 15–16 September 2010 in Wiesbaden, Germany. The event – covering a number of spam and other Internet-related topics – will be held mainly in English. Participation is free of charge, but registration is required. See <http://www.eco.de/veranstaltungen/7752.htm>.

VB2010 will take place 29 September to 1 October 2010 in Vancouver, Canada. Early bird registration rates apply until 15 June. For the full conference programme including abstracts for all papers and online registration, see <http://www.virusbntn.com/conference/vb2010/>.

MAAWG 20th General Meeting takes place 4–6 October 2010 in Washington, DC, USA. MAAWG meetings are open to members and invited guests. For invite requests see http://www.maaawg.org/contact_form.

Hacker Halted USA takes place 9–15 October 2010 in Miami, FL, USA. For more information see <http://www.hackerhalted.com/>.

HITBSecConf Malaysia takes place 11–14 October 2010 in Kuala Lumpur, Malaysia. For more information see <http://conference.hackinthebox.org/hitbsecconf2010kul/>.

RSA Conference Europe will take place 12–14 October 2010 in London, UK. 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. For more information see <http://www.ecrimeresearch.org/>.

Malware 2010, The 5th International Conference on Malicious and Unwanted Software, will be held 20–21 October 2010 in Nancy, France. This year's event will pay particular attention to the topic of 'Malware and Cloud Computing'. For more information see <http://www.malware2010.org/>.

Infosecurity Russia takes place 17–19 November 2010 in Moscow, Russia. See <http://www.infosecurityrussia.ru/>.

AVAR 2010 will be held 17–19 November 2010 in Nusa Dua, Bali, Indonesia. More details and a registration form are available at <http://www.aavar.org/avar2010/>.

VB2011 will take place 5–7 October 2011 in Barcelona, Spain. More details will be announced in due course at <http://www.virusbntn.com/conference/vb2011/>.

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.virusbntn.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@virusbntn.com Web: <http://www.virusbntn.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.