DECEMBER 2009

virus BULLETIN

Fighting malware and spam

CONTENTS

ISSN 1749-7027

IN THIS ISSUE

STARRY, STARRY NIGHT

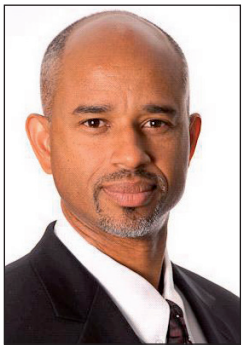
Peter Ferrie likens W32/Satevis to a viral version of a mix tape – a virus that is essentially made up of a collection of routines taken from other viruses.
page 4

SPAM HACK ATTACK

In October, thousands of usernames and passwords belonging to Hotmail users were posted publicly online. Gmail and Yahoo! were also targeted. Terry Zink asks: how did the hacker(s) gain access to all of these accounts and usernames? Should we be afraid that someone will guess our passwords? Why did they do it? What did they do with it? And should we worry about it happening to us?
page 12

VB100 ON WINDOWS 7

With a double whammy of a brand new platform and a record-breaking haul of 43 products to test, the VB test team had their work cut out this month. John Hawes has all the details of how the products fared on the shiny new Windows 7 platform.
page 16



'Ignorance of the risks of cybercrime is what poses the greatest threat to the new generation of Internet citizens.'

Jeff Debrosse, ESET

CYBERSECURITY AWARENESS FOR THE NEXT GENERATION

The global Internet penetration rate currently stands at approximately 24%. With a world population of 6.7 billion, that equates to roughly 1.6 billion Internet users. Meanwhile, as Internet usage has increased, cybercrime has become pervasive, pandemic and increasingly connected with other parts of the criminal ecosystem. It ranges from the theft of an individual's identity to the complete disruption of a country's Internet connectivity.

For those who have yet to connect to the Internet, there are significant challenges – one of which is cybercrime (in its many forms). There are technological measures that help mitigate cybercrime attacks, but technology alone is not the answer.

The next billion users on the Internet will come not from developed nations, but from developing countries. These new users will be fresh targets for cybercriminals. Awareness is a key factor in reducing cybercrime, and even basic levels of awareness of various types of risks and Internet-borne threats can yield positive results. This is primarily due to the fact that the end-user is the weakest link in the 'security chain'.

In an effort to educate and protect local communities, a number of organizations are currently spearheading campaigns and initiatives to teach citizens about technologies and tools that help reduce and/or prevent cybercrime. Regardless of the arguments as to what individuals, institutions (businesses, academia, etc.) and governments should do to combat cybercrime, one fact remains: doing nothing is the worst position to take.

Cybercrime targets information – data that is electronically stored, used and transmitted. For instance, even with varying levels of per capita income, the amount of money that stands to be lost through a phishing attack has the potential to be significant due to the sheer number of users at risk – economy of scale. The risk that cybercrime poses on a global scale is as limitless as human determination, ingenuity and ignorance.

Cybercrimes like phishing and data breaches are a threat to users across the globe. In the United States these threats are so severe that they were detailed as national security threats in the 2009 Annual Threat Assessment Intelligence Briefing to the Senate Intelligence Committee. This represents the scope of threats in a country whose users have had many years' experience of the Internet. Newcomers to the Internet will face the same threats – from cybercriminals that have had years of experience and who have optimized their attack and evasion techniques.

When companies conduct risk analyses, they often have to take into consideration the costs associated with protecting their organizations against malware and the likelihood that less aware end-users will take actions that will increase their risk. Analysis of malware traffic, behaviour and code are the standard methods used for identifying and reducing the malware risk. Taking behaviour analysis to the next level: the end-user provides a means of determining whether users have been exploited and now pose a threat to themselves and, potentially, their organizations. Traditionally, the end-user has been regarded as the 'weakest link', but learning from and leveraging end-user behaviour has the potential not only to add to the security layering, but also to increase the strength of the weakest link.

In developing countries, computing infrastructure build-out, deployment and subsequent end-user connectivity must be coupled with effective cybersecurity awareness training – in addition to localized application training. Ignorance of the risks of cybercrime is what poses the greatest threat to the new generation of Internet citizens. Coordinated global efforts in effective awareness training will transform these new Internet citizens from potential victims to increasingly aware and less vulnerable people as a whole.

NEWS

HAPPY HOLIDAYS

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

Yuletide greetings from the VB team (L-R): Helen Martin, Martijn Grooten, John Hawes, Simon Bates and Allison Sketchley.

IKEE AUTHOR DEVELOPS IPHONE APPS; APPLE SEES NO NEED FOR SECURITY

The author of the first worm for *Apple*'s *iPhone* has been offered a job with Australain *iPhone* application developer *Mogeneration*. 21-year-old Ashley Towns claims to have written the Ikee worm – which infects jailbroken *iPhones* – for purely altruistic reasons, in order to raise awareness of the dangers of using jailbroken *iPhones*.

When Towns announced his job offer via *Twitter*, one could almost hear the IT security community collectively sighing and shaking its head in disbelief as the irresponsible actions of this misguided and unrepentant young man were rewarded. Indeed, proof of the irresponsibility of Towns' actions came when, just two weeks after the release of Ikee, the malicious 'Duh' worm appeared – based on Towns' creation.

Despite Towns' creation having started the ball rolling with *iPhone* malware, no anti-virus protection has yet been made available for the device. *Apple* tightly controls the applications that run on its *iPhone* devices and the company's approval and collaboration would be required in order for security applications to be developed for the device. However, since both Ikee and Duh target jailbroken *iPhone*s – and no malware has yet appeared for unmodified devices – *Apple* has not felt the need to enter into discussion with any anti-malware developers.

CONGRATS

As we enter into the season of festivities and celebrations, our congratulations go to *Sophos*'s Graham Cluley, who last month won a hat trick of trophies at the *Computer Weekly* Awards. In recognition of his prolific online updates, spreading the word of safe computing (and the name of *Sophos*), Cluley bagged the awards for IT security blog of the year, *Twitter* user of the year and overall best blog of the year.

Prevalence Table – October 2009[1]

Malware	Type	%
Conficker/Downadup	Worm	9.02%
Autorun	Worm	7.06%
Virtumonde/Vundo	Trojan	6.98%
Heuristic/generic	Virus/worm	5.65%
OnlineGames	Trojan	5.51%
VB	Worm	5.16%
Agent	Trojan	5.10%
FakeAlert/Renos	Rogue AV	4.17%
Virut	Virus	3.86%
Heuristic/generic	Trojan	3.28%
Inject	Trojan	3.09%
Istbar/Swizzor	Trojan	2.92%
Encrypted/Obfuscated	Misc	2.64%
Adware-misc	Adware	2.55%
Suspect packers	Misc	2.28%
Alureon	Trojan	2.24%
Hupigon	Trojan	1.93%
Crypt	Trojan	1.90%
Small	Trojan	1.86%
Delf	Trojan	1.83%
Downloader-misc	Trojan	1.70%
Wimad	Trojan	1.66%
Sality	Virus	1.66%
PCClient	Trojan	1.42%
Zbot	Trojan	1.25%
Tanatos	Worm	1.14%
Lolyda	Trojan	1.04%
Bifrose/Pakes	Trojan	0.90%
Peerfrag/Palevo	Worm	0.68%
Sahat/ShopAtHome	Adware	0.68%
Iframe	Exploit	0.67%
Others[2]		10.46%
Total		100.00%

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

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

MALWARE ANALYSIS

TWINKLE, TWINKLE LITTLE STAR

Peter Ferrie
Microsoft, USA

Sometimes a virus gets it completely wrong (see *VB*, October 2008, p.4). Sometimes a virus gets it mostly 'right', but sometimes that's only because the virus in question is a collection of routines taken from other viruses which got it mostly right. That is exactly what we have here, in W32/Satevis.

The virus begins by determining its location in memory. This makes it compatible with Address Space Layout Randomization (ASLR), though the technique has existed for far longer than ASLR. However, instead of using the common call-pop technique to determine the location, the virus uses a call, but then uses an indirect read from the stack via a string instruction. In the past, this kind of alternative method would have avoided some heuristic detections, but these days the call-pop method is so common in non-malicious code that this obfuscated method might be considered suspicious. In any case, there are few anti-malware engines now that would rely on such a weak detection method.

KERNELIFEROUS

The virus sets up a Structured Exception Handler (SEH), and does so correctly (unlike Zekneol, see *VB*, November 2009, p.4). Then the virus walks the host import table, looking for a DLL whose name begins with 'kernel32'. This leads into what we might consider to be the first bug in the code, though it does not come into play until later. The bug is that since nothing further is checked, the name of the DLL that the virus finds could be 'kernel32<any string>'. For example, 'kernel32foo.bar', and it will be accepted. While this is very unlikely to occur, it is still a bug.

Once a kernel32-style DLL has been found, the virus retrieves the address of the first API that is imported from it and uses that address as a starting point for a search for the MZ and PE headers. Assuming that the headers are found, the virus parses the export table directly to retrieve the addresses of the APIs that it needs in order to infect files. For each API that kernel32 exports, the virus determines the length of the API name and calculates the CRC32 value using a routine that was written for 16-bit CPUs and which has been copied blindly for years by virus writers around the world. The virus searches its entire list of checksums for a match, which is a very inefficient method. Someone clearly didn't pay attention in computer science class. This action is repeated until all of the needed APIs have been located.

The virus also carries a little anti-debugging routine. One trick is an intentional divide-by-zero, which should cause an exception that the virus will intercept. In the past, some CPU emulators in anti-malware engines did not support such tricks. That might have been a problem in 1998, but these days support is widespread. The virus then attempts to open two *SoftICE* driver devices by name. However, this routine has also been copied blindly for years by virus writers, despite the fact that it hasn't worked since 2004. This is described more fully in *VB*, February 2009, p.4.

ONWARD AND FORWARD

The virus retrieves the address of the SfcIsFileProtected() API from sfc.dll, if that DLL is available (it was introduced in *Windows 2000*), using the GetProcAddress() API instead of parsing the export table directly. The use of the GetProcAddress() API avoids a common problem regarding import forwarding. The problem is that while the API name exists in the DLL, the corresponding API address does not. If a resolver is not aware of import forwarding, then it will retrieve the address of a string instead of the address of the code. In this case, support for import forwarding (which the GetProcAddress() API provides) is necessary to retrieve the SfcIsFileProtected() API from sfc.dll, since it is forwarded to sfc_os.dll in *Windows XP* and later.

The virus searches for files within the current directory and is interested in files whose suffix is 'EXE', 'CPL' or 'SCR'. For each such file that is found, the virus checks if the SfcIsFileProtected() API is available. If so, then the virus gets the full pathname of the file, and 'converts' it from ASCII to Unicode. However, the conversion is done using a routine in the virus that simply takes an eight-bit value and stores a zero-extended 16-bit value. This obviously doesn't correctly convert any character that is not part of the seven-bit US-ASCII set, but the virus author probably doesn't care about such things anyway. After the conversion, the virus checks if the file is protected, and will not infect the file if it is.

REDUNDANT SYSTEMS

If the file is not protected, then the virus removes any read-only attributes, opens the file and queries its size. This is despite the fact that the file size was included as part of the information that was returned when the virus found the file in the first place. The virus avoids infecting files that are smaller than 16KB or larger than about 64MB, along with files whose size is a multiple of either 113 or 117 (see below). This style of infection marker was introduced years ago by members of the 29A virus-writing

group, whose works appear to have influenced this virus writer.

If the file still appears to be infectable, then the virus queries its time stamps. This is despite the fact that the times (creation, last access and last write) are also available as part of the information that was returned when the virus found the file.

The virus opens the file and checks for the 'MZ' and 'PE' headers, along with several other fields. A minor bug exists here, too, which is that the virus checks only the first two bytes of the 'PE' signature. Thus, it would be possible to create a DOS file which happened to have the 'PE' characters in the right location, followed by something other than zeroes, and the virus would try to infect it. One of the other things that the virus checks is that the size of the 'MZ' header is 64 bytes. This was an old recommendation from *Microsoft* for quickly identifying potential *Windows* files. At the time, it applied to the 'New Executable' file format, as part of *Windows 3.0*, but it would be equally applicable to the current Portable Executable format. However, *Windows* itself has never checked the field.

The other things the virus checks for are that the file contains at least three sections, has non-zero values for the SizeOfOptionalHeader, SizeOfCode and BaseOfCode fields, and that the file targets the GUI subsystem (as opposed to being a console-mode or driver file). The virus does not exclude DLLs – presumably assuming that no DLL will have one of the suffixes of interest. As with the MZ header size, *Windows* has never checked either the SizeOfCode or the BaseOfCode field values, and it is possible to create a file whose SizeOfOptionalHeader is zero. Of course, such a file will not be infected by this virus.

INFECTIOUS GROOVES

If a file is found to be infectable, then the virus adjusts the file size to include the size of the virus, then rounds up the result to a multiple of the SectionAlignment value from the PE header. It then rounds this number up to a multiple of 117. The resulting value is used as the size in memory for the temporary copy of the host. Unfortunately, this value might be insufficient (see below), which will result in file corruption.

The virus requires that the file to infect has an import table. The virus attempts to find the section that contains the import table, and then walks the table, looking for a DLL whose name begins with 'kernel32'. However, the virus uses a faulty method to determine the location of the section table. The problem is that the virus relies on the value in the NumberOfRvaAndSizes field to determine the size of the optional header, instead of using the value in the SizeOfOptionalHeader field (see also *VB*, February 2009, p.7). As a result, it is possible to create a file with two section tables: one that this virus sees, and one that *Windows* sees.

This bug is repeated when the virus attempts to find the section with the largest file offset (in fact, the bug appears in the code a total of five times). This is used to determine where the data ends in the file, in order to check for overlay data. However, there is another bug in this code, which is that the physical size for the section is not checked. If the physical size for a section is zero, then the file offset can be set to any value, and that would cause problems for the virus.

The virus determines that a file has overlays if the amount of data is at least twice the size of the SectionAlignment field value. As a result, the virus misses the presence of small overlays, such as debug data. Such data will be destroyed when the virus infects the file.

If a file is found not to be infectable at this point, then the virus rounds up the original file size to a multiple of 113. This allows the virus to skip files that have been examined already, thus improving the efficiency of any future searches.

A NEW EPOCH

The virus uses an entrypoint-obscuring (EPO) technique. The EPO routine begins by attempting to find the section that contains the entrypoint. Within that section, the virus searches for FF15- and E8-style calls. This kind of EPO is similar in style to the W95/MTX virus from 2000. If an FF15-style call is seen, then the virus checks whether the address that follows points into the import table. Specifically, the virus checks whether the import table entry corresponds to an import from kernel32.dll. If the import comes from kernel32.dll, then the original call will be considered a candidate for replacement.

If an E8-style call is seen, then the virus checks if the destination remains within the current section. If it does, then the virus checks if it points to an FF25-style jump. If it does, then the original call will be considered a candidate for replacement.

For either call style, there is a 50% chance that the virus will replace the call immediately. However, if the search reaches the end of the section without making any change, and if a candidate has been located, then the virus will replace that candidate without exception. The replacement uses an E8-style call to point to the virus code.

After deciding on the entrypoint, the virus generates a new polymorphic decryptor. The engine was written by another

virus writer in 1999, and used in the W32/Aldebaran virus. It is quite a simple engine. It uses very few instructions but it contains some characteristics that are always present, which make it easy to identify. One potential problem with the engine is that it has no concept of maximum size. Thus, the decryptor may be so large that an exception occurs while appending the virus body. In fact, the decryptor may be so large that an exception occurs while producing the decryptor itself!

THIS SECTION RESERVED

If the polymorphic decryptor is generated successfully, then the virus appends its body to the decryptor, and places the whole thing at the end of the section whose data appeared last in the file, adjusting the virtual size appropriately. There is a significant problem with this approach. If that section was not the last in the file, then the new virtual size might result in that section overlapping the next one. Such a file cannot be loaded in *Windows NT* and later.

The virus marks the section as readable, writable and executable. This allows the virus to run in environments in which Data Execution Protection (DEP) is enabled. Then the virus does a most peculiar thing. It scans the data directories for a reference to the section that holds the virus body. If a reference is found, then the virus sets the size of the entry to the size of the section. This can cause some peculiar behaviour, particularly regarding the export table. In the event that an export address table entry originally pointed within the same section, but outside of the export table (and was therefore truly exported by the file), the entry will now appear to point into the export table and will therefore appear to be forwarded to another DLL, whose name will look ... quite foreign.

After infecting the file, the virus will check if it had a checksum. If it did, then the virus will recalculate it. The virus carries its own routine for this calculation, which combines code that is taken from imagehlp.dll along with some 16-bit code to perform a further adjustment to account for the existing checksum. This suggests that the virus author did not understand the algorithm at all.

Once all of the files have been infected in the current directory, the virus performs the same actions within the *Windows* directory and the system directory, before moving on to an entirely new target.

LINK IN THE CHAIN

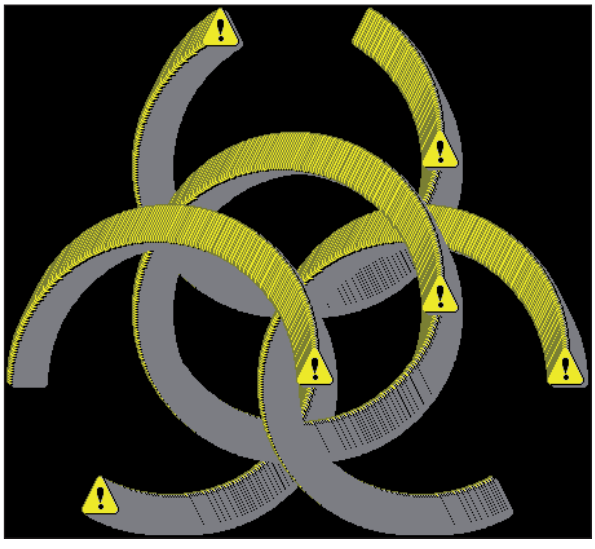
The virus searches within the current directory for files whose suffix is 'LNK'. For each such file that is found, the virus checks that the file is in LNK format, and that it contains a shell item ID list and points to a file system object. If that is the case, then the virus skips the shell item ID list and examines the file system object entry. The virus ignores the file attributes field, which could be used to determine if the object is a file or a directory, and simply assumes that the object is a file. This is essentially harmless, though, because even if a directory had one of the suffixes of interest, the virus would not be able to open it as a file. However, if the link points to a file whose suffix is of interest, and if all other tests pass as described above, then the virus will infect the file as usual. After infecting the link files in the current directory, the virus searches for link files in the %desktop% directory.

To minimize its memory consumption, the virus attempts to free any DLL that it has been using, even if the virus did not load the DLL itself. This might appear to be a bug, but actually it isn't one, because statically loaded DLLs cannot be unloaded. Thus, the attempt to free the DLL will be ignored by *Windows*, when appropriate.

BAITING THE HOOK

Once the infection routine has completed, the virus walks the host import table, looking for a DLL whose name begins with 'kernel32'. Then the virus searches for imports of any of the following functions: CreateFileA(), MoveFileA(), CopyFileA(), CreateProcessA(), SetFileAttributesA(), GetFileAttributesA(), SearchPathA(). Perhaps coincidently, this list is very similar to that of the W32/Cabanas virus from more than a decade ago. The virus hooks as many functions as are imported from that list. Interestingly, the virus uses the WriteProcessMemory() API to install the hooks, even though the memory is addressable directly. This does not bypass any memory protection that might be present. As a result, since the virus does not call VirtualProtect() first, and if the import table is in a read-only memory region, then no hook will be installed. However, the use of the API does avoid the need for an exception handler. In the event that the import table is in a read-only memory region, then any attempt to write directly to the memory would cause an exception, but the WriteProcessMemory() API will simply fail the write.

Each of the hook routines calls a single common routine, then unhooks itself, before calling the original API. The common routine retrieves the directory from the API's parameter list, changes to there, and searches within that directory for files to infect. The fact that the original API is not called until after the search has completed means that the process could appear to be unresponsive and obviously infected. Of course, the virus could use a thread



W32/ Satevis payload.

to perform the scan instead, but that introduces a different problem for the virus. The problem in that case would be that any thread that called the ExitProcess() API would cause all other threads to be terminated, essentially no matter what they were doing. While there are ways to deal with that, and some of them have been demonstrated by other viruses, the solutions are complex, and this virus is simple.

PAYLOAD

The virus has a graphical payload, which activates if an infected file is executed on the 31st day of any month. The payload is to draw a biohazard symbol in the centre of the screen, covering half of the screen in both dimensions.

The final step in the virus code is to allow the host to continue executing. The virus replaces the start of its code with some redirection code that points to the original API. Thus, the virus cannot be reached a second time, no matter how many times the hooked call is executed. For the FF15-style call, the replacement code begins with an 'inc [esp]' instruction to skip an additional byte, since the E8-style call is one byte shorter than the FF15-style call that it replaced. Then the virus stores an FF25-style jump to the original address, before jumping directly to that location.

CONCLUSION

There should be a term for a virus that is nothing but a collection of old routines. This is like the viral version of a mix tape. It's so very retro, I feel like disco-dancing now.

TUTORIAL

BEHAVIOURAL ANALYSIS OF FLASH FILES

Ken Dunham
iSIGHT Partners, USA

A notable escalation in web-based attacks has been seen over the past few years, especially with regard to malicious *Flash* files. *Flash* files are capable of redirection, execution of embedded malicious code and exploitation via vulnerabilities that exist in certain versions of *Flash*. Analysis of *Flash* files can quickly be made more complicated through the obfuscation of bytecode within malicious files, using common JavaScript obfuscation techniques in addition to professional tactics for obfuscating entire files to hinder analysis. Static and behavioural analysis can provide incident response teams and malcode researchers with a quick indication of the possible malicious activity associated with *Flash* files.

INTRODUCTION TO FLASH FILE FORMAT

Flash files have a MIME type of application/x-shockwave-flash and contain one of two possible header values: FWS or CWS. FWS represents a normal *Flash* file while CWS represents a compressed *Flash* file (SWF). Compression is very common and can be seen in the example shown in Figure 1.

The general format of a *Flash* file begins with the header, an eight-bit version number, and a 32-bit file length field:

```
[FWS/CWS] [Version] [Length] [Header] [[Tag Code + Length] [Tag Contents]]
```

Tags within *Flash* files may contain a variety of media such as image files, ActionScript, video streams, buttons and JavaScript. ActionScript and JavaScript are frequently the focus of malicious research. It is also advisable to look for unknown and undocumented tags within a *Flash* file which may be corrupt or have malicious content.

IDENTIFYING MALICIOUS CONTENT

A variety of tools exist to analyse *Flash* content. Some are limited to working only with older versions of ActionScript when such content is present in a file. Others only work to decompress compressed (CWS) *Flash* files so that the decompressed file (FWS) can then be analysed with other tools. There are a select few applications that are solid choices for triage of potentially malicious *Flash* files. While these tools fall short of in-depth reverse engineering and deeper analysis, they are excellent choices for the busy professional seeking to quickly triage potentially hostile content and/or egress communications.

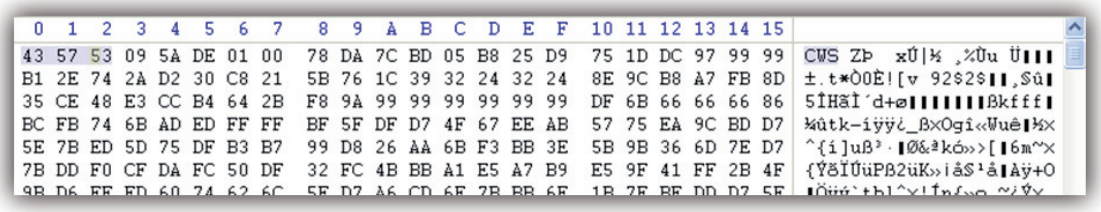


Figure 1: A hostile Flash file containing a CWS header.

ONLINE SCANNERS

Two free online scanners stand out above the rest for rapid triage of code. *Wepawet* and *Adopstools* are both excellent tools for the analysis of *Flash* files. In some cases dynamic analysis is also available.

- *Wepawet*: http://wepawet.cs.ucsb.edu/.

  Wepawet enables a researcher to upload both files and URLs that point to potentially hostile content. This is an excellent option for both real-time analysis of a threat or string extracted from an IDS log as well as incident response and/or forensic investigations that may turn up potentially hostile *Flash* content. At the time of writing this article, the scanner does not support dynamic analysis of *Flash 9* files.

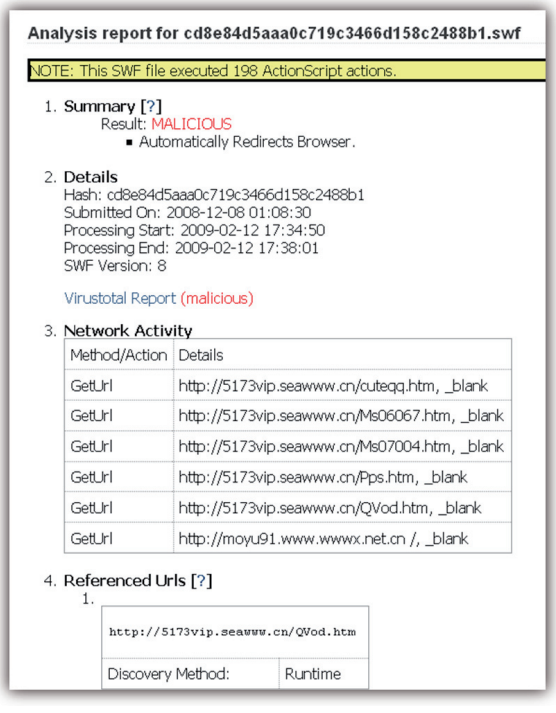


Figure 2: Wepawet analysis of a hostile SWF file reveals several GetURL addresses and other malicious identification.

Static output from the tool includes possible malicious methods (such as 'Loader.loadBytes method detected'), hash, submission and process date and time, and *Flash* version. It also includes a *VirusTotal* scan report and any URLs referenced in the file. Note that it is common for legitimate Adobe.com URL references to be found in such code.

- *Adopstool*s: http://www.adopstools.net/index.asp?section=tools&page=clickchecker

  For the *Adopstools* scanner the results are split into five sections: header and resources, preview and click test, tags list, GetURLs and ActionScripts, and dumping code. The last two are especially helpful for a busy professional attempting to identify any possible malicious URLs or scripts. Unfortunately this scanner can be a bit slow at times. The interface is more raw-code-analysis-oriented than the GUI-based *Wepawet* scanner.

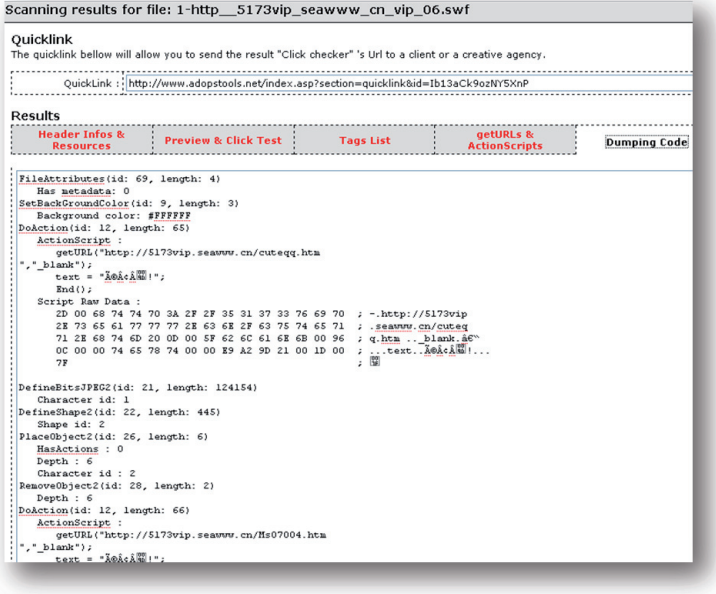


Figure 3: Adopstools includes a 'Dumping Code' section to view code within a Flash file.

Note: If you upload a defanged file such as badfile.swf_ this scanner will display a warning that it's not a *Flash* file, but it will proceed with scanning if the 'Scan' button is selected.

Identification and capture of potentially hostile scripts and/or URLs is critical for a security researcher. It is common at this point to attempt to capture code related to all possible remote files or links related to the *Flash* file for domain and abuse research, and/or de-obfuscation of extracted scripts of interest.

DECOMPILING USING TRILLIX

Eltima offers one of the most easy-to-use, robust GUI applications for *Flash* analysis. The program enables a security researcher to quickly identify tags and scripts, and also to export scripts of interest. If *Adobe Flash Studio* is installed, editing of FLA files (Flash Source) is also supported. ActiveX must be installed in order to use this program. Figure 4 shows how non-obfuscated URL content is clearly revealed via scripts decompiled by *Trillix*.

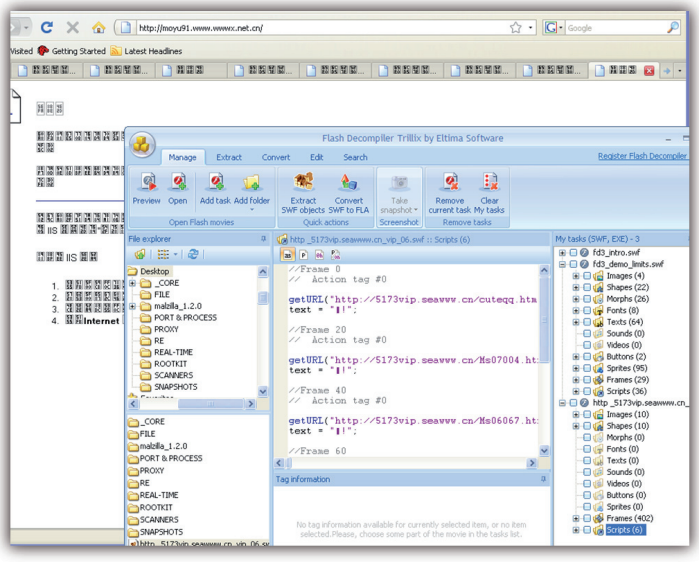


Figure 4: Trillix decompiles and displays scripts as well as running the Flash file via preview mode.

Caution: this program runs *Flash* file content dynamically by default. Be careful only to run this within a *Windows* lab environment to avoid accidental damage to other systems.

URLs or scripts of interest can be exported simply by using copy and paste or by using the 'Extract SWF objects' button. When the extraction option is used *Trillix* automatically extracts all scripts by default to a working directory and then displays that directory in a new window. For example, the case illustrated in Figure 4 resulted in Frame 0 and Frame 20 exports and associated ActionScript (.as) exports which contain getURL statements such as the following:

```
//Action tag #0
getURL("hxxp://5173vip.seawww.cn/cuteqq.htm \r",
"_blank");
text = "額!";
```

Script analysis is becoming increasingly difficult as both the ability and adoption of techniques for obfuscating scripts within *Flash* files advances.

DECOMPILING WITH FLASH TRACER

Flash Tracer is one of the easiest ways to dynamically analyse the behaviour of a *Flash* file – once you get it set up properly. The set-up can be a bit tricky, requiring the installation of a *Flash* debugger, flashtracer.xpi for use with *Firefox*, and then a special configuration file. A debugger version of *Flash* sends output from the trace() method to a log file which is then viewed with the *Flash Tracer* extension within *Firefox*. If a non-debugger version exists, uninstallation of the player is required for a debugger version to be installed.

Caution: this results in a dynamic execution of *Flash* content. Be careful only to run this within a lab environment to avoid accidental damage to other systems.

The following is an overview of how to install *Flash Tracer* on a *Linux* operating system such as *Ubuntu*. Three core steps are followed: installation of a debugger version, mm.cfg creation, and *Flash Tracer* installation and use.

1. Go to http://playerversion.com/ and view the report to see if *Flash* is installed and if a 'debugger' version exists.
2. If a *Flash Player* is installed but it is not a debugger version, uninstall it using *Synaptic* or other *Linux* tools.
3. Install *Flash Player Debugger for Linux* by downloading it from http://www.adobe.com/support/flashplayer/downloads.html. Extract files and navigate to the /plugin/debugger directory. Run the 'flashplayer-installer' in the terminal and follow the prompts to complete the installation.
4. Go to http://playerversion.com/ and confirm that a *Flash Player* 'debugger' version is installed correctly.
5. Create a log file by running a *Flash* file or creating it as a placeholder for the debugger. Locate and run a SWF file or create a placeholder at /home/{username}/.macromedia/Flash_Player/Logs/flashlog.txt. Replace {username} with the current user account name for *Linux*.
6. Create a file in the home directory for *Linux* called 'mm.cfg' with the following data:

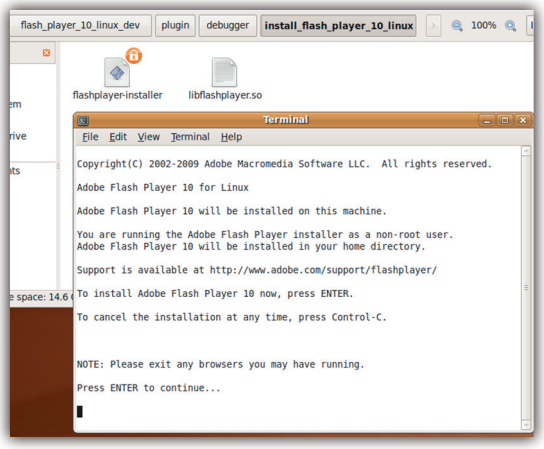


Figure 5: Flash Player debugger installing on a Linux computer.

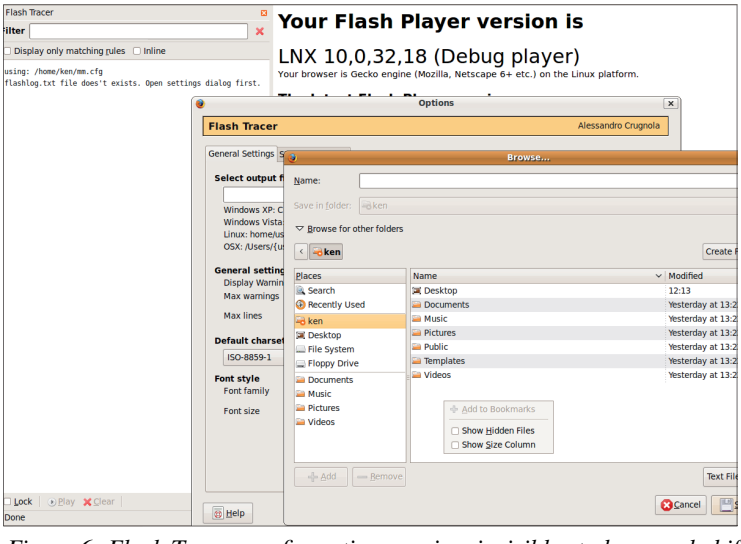


Figure 6: Flash Tracer configuration requires invisibles to be revealed if browsing to the flashlog.txt file.

```
ErrorReportingEnable=1
TraceOutputFileEnable=1
```

7. Download and install *Flash Tracer* from http://www.sephiroth.it/firefox/flashtracer/. If you saved it as a file, drag flashtracer.xpi over *Firefox* and restart *Firefox* after installation.
8. Open *Firefox* and configure *Flash Tracer* to point to the flashlog.txt file, replacing {username} with the user name for the current account: /home/{username}/.macromedia/Flash_Player/Logs/flashlog.txt. Note: be sure to show invisible directories in the Home folder of *Linux* (right-click on the directory listing window) to browse to flashlog.txt file.

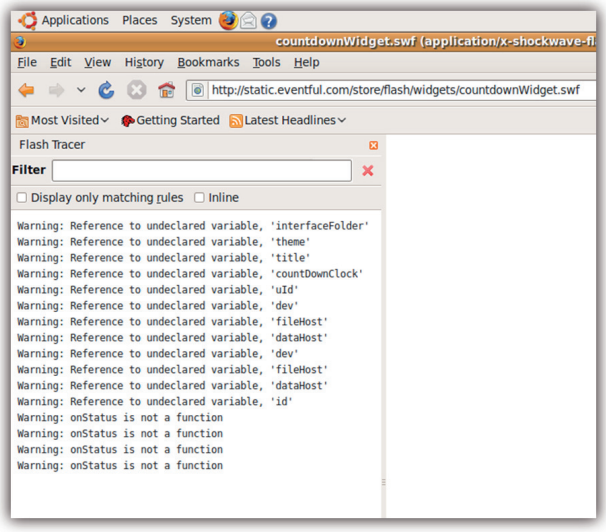


Figure 7: Flash Tracer displays the contents of flashlog.txt in a sidebar when a SWF is loaded from a remote server.

You may also just type in the path manually and click OK.

9. Load a hostile SWF and watch *Flash Tracer* read the trace() output to the *Firefox* sidebar. Note: any changes you make using this tool directly impact the flashlog, such as clearing the log file as you clear the *Flash Tracer* window.

Flash Tracer options are intuitive for pausing and clearing log file displays. Analysts should be looking for URLs that display, possibly pointing to remote exploit sites or redirected targets, and other actions such as getURL statements and undefined tags. Help with interpretation of debugger comments can be gained from the runtime error research published at http://livedocs.adobe.com/flex/201/langref/runtimeErrors.html. For example, FScommand and getURL issues that may exist in a suspect *Flash* file may be linked to JavaScript actions and egress communications as shown in the *Flash Tracer* example below for a known hostile file:

```
*** Security Sandbox Violation ***

FSCommand halted (AllowScriptAccess is ''):
FSCommand:showmenu
```

Common ActionScript references of interest for hostile activities include but are not limited to FSCommand, getURL, LoadMovie, LoadMovieNum, ExternalInterface, navigateToURL and URLRequest.

FLASH SECURITY

More information on *Flash* security as a whole can be found at https://www.flashsec.org/wiki/Main_Page.

CALL FOR PAPERS

CALLING ALL SPEAKERS: VB2010 VANCOUVER

Virus Bulletin is seeking submissions from those wishing to present papers at VB2010, which will take place 29 September to 1 October 2010 at the Westin Bayshore hotel, Vancouver, Canada.

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

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

A list of topics suggested by the attendees of VB2009 can be found below. However, please note that this list is not exhaustive, and the selection committee will consider papers on these and any other anti-malware and anti-spam related subjects.

- Cybercrime and law enforcement – tools, problems and perspectives
- Forensics
- Virtualization and malware on virtual machines
- Automated malware processing
- Rootkits, rootkit detection and cleaning
- Current and future challenges for AV
- Windows 7
- Behaviour-based detection and issues
- Phishing
- SMS spam
- Blog spam, trackback spam
- Anti-spam techniques in detail
- Multi-engine anti-spam
- Anti-spam testing
- Anti-malware testing
- New AV technologies
- Vulnerabilities of endpoint security products
- Sample sharing
- Multi-engine anti-virus protection
- In the cloud scanning/technology
- Integrating IPS/gateway/endpoints for holistic malware detection/reporting
- Malware trends within corporate enterprises
- Heuristics/fuzzy detection
- Device drivers
- JavaScript emulation
- Zero-day malware
- SMS vulnerabilities
- Botnets
- Customer experiences and case studies
- Reverse engineering and analysis tricks & techniques
- Neural networks
- Localized threats around the world
- Security on mobile devices
- Mac security
- Static code analysis
- Industry cooperation

SUBMITTING A PROPOSAL

The deadline for submission of proposals is **Friday 5 March 2010**. Abstracts should be submitted via our online abstract submission system. You will need to include:

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

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

Following the close of the call for papers all submissions will be reviewed by a selection committee; authors will be notified of the status of their paper by email.

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

Authors are advised that, should their paper be selected for the conference programme, they will be expected to provide a full paper that will be included in the VB2010 Conference Proceedings as well as a 30-minute presentation at VB2010 in Vancouver. The deadline for submission of the completed papers will be Monday 7 June 2010, and potential speakers must be available to present their papers in Vancouver between 29 September and 1 October 2010.

Any queries relating to the call for papers should be addressed to editor@virusbtn.com.

FEATURE

HOTMAIL, YAHOO!, GMAIL USERS HACKED – BUT HOW?

Terry Zink
Microsoft, USA

In October this year, thousands of usernames and passwords belonging to *Hotmail* users were posted on the technology website *Neowin* [1]. They were posted for everyone to see, and anyone could have taken them, logged into the accounts and done something with them. The accounts have since been reset. *Computerworld* reported on the story [2]:

> '*If Neowin's account is accurate, the Hotmail hack or phishing attack would be one of the largest suffered by a web-based email service.*
>
> '*Last year, a Tennessee college student was accused of breaking into former Alaska governor Sarah Palin's Yahoo! Mail account in the run-up to the US presidential election. Palin, the Republican vice presidential nominee at the time, lost control of her personal account when someone identified only as "rubico" reset her password after guessing answers to several security questions.*
>
> '*Shortly after the Palin account hijack, Computerworld confirmed that the automated password-reset mechanisms used by Hotmail, Yahoo! Mail and Google's Gmail could be abused by anyone who knew an account's username and could answer a single security question.*'

The *BBC* reports that *Gmail* and *Yahoo!* were also targeted [3]. The situation is that some hacker obtained information that most people think is secret and then posted it publicly. A number of questions arise: how did the hacker gain access to all of these accounts and usernames? Is the Sarah Palin story relevant in this case? Should we be afraid that someone will guess our passwords? Why did they do it? What did they do with it? And should we worry about it happening to us?

HOW DID IT HAPPEN?

Depending on the reviews you read elsewhere on the web, there are a lot of theories about how this information could have been obtained. Let's consider some of them.

1. The attacker hacked into Hotmail, Google and Yahoo! and stole the information

This particular mechanism involves the hacker breaking into *Hotmail*, *Google* and *Yahoo!*'s servers, stealing information, and then exiting before anyone had noticed. To do this, the hacker would need to exploit a known security weakness, or have known about an obscure security flaw that had not yet been patched, or have some sort of inside information that allowed them to bypass the security mechanisms with stolen credentials.

An external hack where someone breaks into *Hotmail*'s servers and accesses the account information is unlikely. It is much more likely that the attacker obtained the information through social engineering. Why is this more likely? For one, breaking into the servers would involve having to get past all of the firewalls and security measures that *Microsoft*/*Hotmail* has in place to keep intruders out. While not impossible, this would not be easy.

But secondly, even if an attacker were to break in and steal the account information, it is very unlikely that they could access the associated passwords. Passwords are not stored in clear text, they are encrypted using a one-way hash. All firms with good security store them this way.

One-way hashes are a basic security mechanism. They are based upon the idea that a function is easy to compute one way, but difficult to compute in the opposite direction. For example, the function $f(x) = x^2$, i.e. the squaring function, is easy to compute: 2^2 is 4, 4^2 is 16, 5.3^2 is 28.09. However, it is much more difficult to calculate square roots. We know that $\sqrt{16}$ is 4, or $\sqrt{64}$ is 8. We know this because we have our multiplication tables memorized, or we know certain square roots. But what is $\sqrt{79}$? That is not so easy. Of course, we have calculators that can determine this, but it is more computationally expensive to do so. Password encryption algorithms work the same way. It is possible to encrypt your password using an algorithm that encodes it, but reverse engineering it is computationally expensive. Of course, it is almost always possible to decode it if you know the algorithm, but this would be so time-consuming that by the time you had broken it the data would be stale.

If you ever forget your password for a website and click the link to recover it, there are two options:

1. You are given a password reset where you click the link and type in a new password.
2. You click the link and the password is sent to you in clear text.

For option 1, the reason you must reset your password is because even the folks who are storing it (e.g. *Google*, *Yahoo!* or *Hotmail*) do not know your password. It is stored in hashed text (i.e. a random string of characters that is created by the use of the encryption algorithm). They cannot give it to you because it is computationally infeasible. If a hacker were to break in and steal your password, all they would have is the hashed text – and entering your hashed text into the password field is the equivalent of entering the wrong password. The account would not authenticate.

Storing passwords in hashed text is standard practice in the industry, so even if a hacker broke in and stole information from *Hotmail, Google* and *Yahoo!*, there wouldn't be much useful there to steal (in terms of passwords).

This suggests that the attacker tricked the user into handing over their user account and password through some other mechanism.

2. Hackers guessed the password

In 2008, Republican vice-presidential nominee Sarah Palin had her email account hacked. How? An attacker guessed her password.

Some websites have a set of security questions that will allow you access to your password if you answer them correctly. This may work if few people know you, but for a public figure like Palin a lot of personal information is publicly available. Answers to questions like 'What is your father's name?' or 'What year did you graduate from college?' can easily be discovered using a quick Internet search. It wouldn't take that much effort to guess a username and figure out the password.

However, in the *Hotmail*, *Google* and *Yahoo!* case, whilst I suspect that social engineering was used to obtain the information, I do not suspect security-question guessing. Note that while vice-presidential candidate Sarah Palin had her account hacked by somebody guessing her login information, this is not a scalable model for spammers. Palin is well known and you could possibly guess her information simply by reading about her online. But to access 10,000 accounts that way is too time consuming and the people being hacked are not well known. It would not be possible to guess their information, other than by chance.

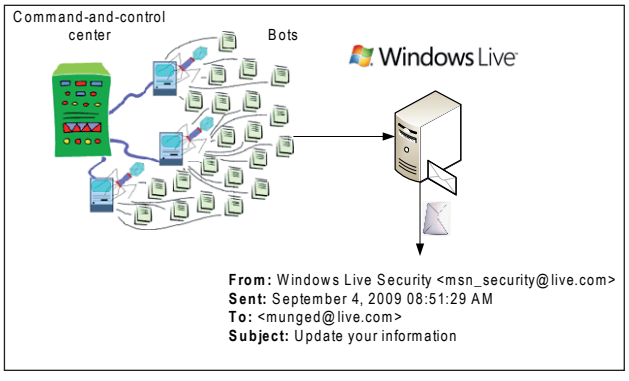
3. The users fell for a social engineering scam

The general consensus is that these *Hotmail*, *Google* and *Yahoo!* users were victims of phishing scams. Such a scam would look something like this:

A *Hotmail* user receives a spam message in their inbox, which probably looks as if it has come from *Windows Live*. There is some call to action wherein the message says, for example, that *Hotmail* is upgrading its infrastructure and requires users to log into their account and verify their credentials.

In addition, there was probably some bot attack that broke *Hotmail*'s CAPTCHA service on the sign up page, so these spam messages would actually have been sent from *Hotmail* internally.

These types of spams can be more difficult to filter than those sent from another service. So we have *Hotmail* users spamming *Hotmail* users, possibly with a From: address like 'Windows Live Mail Security <live.security.something@...>'. Some users did not recognize that this was a phishing scam, entered their credentials and the damage was done.



If the user entered their information by clicking the link and filling in their details, it would have been relayed back to the spammer who would then have the user's credentials.

Spoofing scams like these are among the oldest spammer tactics. The most commonly associated mechanism is phishing where the spammer impersonates a bank, but spammers will also impersonate the IRS, the Better Business Bureau, *CNN*, and so forth. All of these are attempts to trick the user into taking an action, whether it is downloading and installing malware or giving up their username and password.

4. The spammers/hackers attacked some other weak site and stole information from there

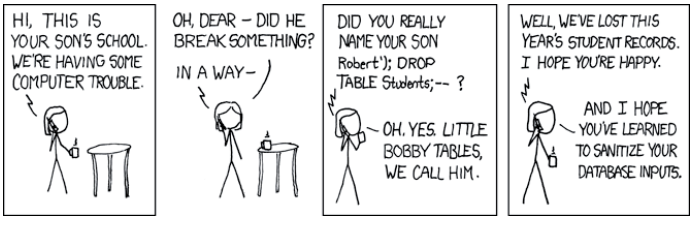
Users falling prey to a phishing scam is one of the most likely explanations for this attack, but it is not the only possibility. The problem is that there are so *many* other possible attack vectors. Here's one: spammers don't have to target *Hotmail* users via a phishing scam. Notice that it was not only *Hotmail* users that surrendered their credentials, but also *Yahoo!* and *Google* users. A hacker would have a difficult time hacking *Yahoo!*, *Google* and *Microsoft* directly, but what if they attacked an online discussion forum or a blogging service?

Many websites across the Internet allow you to log into their websites using your email address as the username. How many people use their email address… and also use the same password across multiple sites? If a hacker were to break into an online forum – one with a low level of security – they could count on the fact that users tend to reuse usernames and passwords. Hackers get to take advantage of statistics – given enough people, some of them will be hits (i.e. using the same username/password combination).

Recall that the more mature services store passwords in hashed text. Since *BBC News* confirmed that the accounts were genuine and predominantly originated in Europe, I'm willing to bet that some discussion forum in Europe had its users' usernames and passwords stored in clear text and was broken into, and the information stolen. The attacker then went and verified which ones unlocked the users' accounts and discarded the rest. They then eventually posted them online for all to see.

Of course, even this may not necessarily be the whole story; it could have been easier than that. According to *The Register*, the most commonly occurring password was '123456' and '123456789' was the second most common [4]. These represent about 0.82% of the total passwords. So, if you acquired a large list of usernames and tried each of these two passwords, then there is a slightly less than 1% chance that one of the passwords will work. 1% is small, but it's greater than 0%, and if you decided to automate it, you would have success in no time.

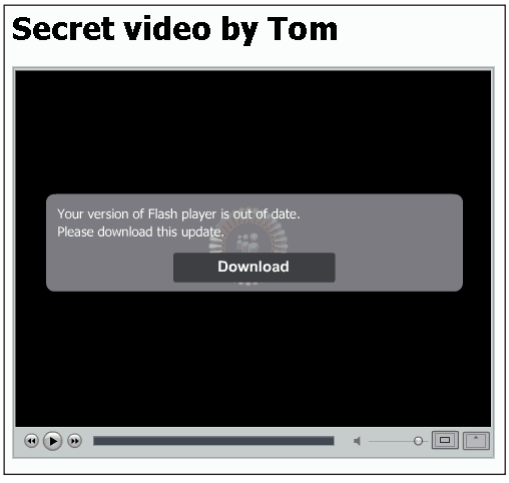
Techniques for breaking into a discussion forum's backend are beyond the scope of this article, but it often involves exploiting weaknesses in the software such as cross site scripting (XSS) or SQL injection attacks. *Microsoft* has a software design process that requires coders and programmers to go through threat analysis and consider how those threats can be mitigated. However, the do-it-yourself hobbyist, while well-meaning, doesn't always have the security background to be conscious of such attacks [5].



5. The users fell victim to a keystroke logger

There are possibilities other than a phish, hack or statistical hack. A user could have been the victim of a keystroke logger. For example, Win32/Koobface spreads by sending messages to a victim's social network contacts with text such as 'You should watch my latest video', accompanied by a URL. When recipients visit the link, they are instructed that they need to download an update to their *Adobe Flash Player* plug-in in order to view the video. However, the download is actually the Koobface installer.

Koobface attempts to gain access to users' sensitive financial information such as credit card numbers. It can also redirect access from search engines to malicious sites.



While Koobface does not install a keystroke logger, other pieces of malware do. For example, Taterf is a family of worms that spreads through mapped drives in order to steal login information for popular online games (Taterf was the second most prevalent worm detected by *Microsoft*'s *Malicious Software Removal Tool* in the first half of 2009 [6]). Certain keystroke loggers can detect when a user visits *Hotmail*, *Google* or *Yahoo!*, and when they do, they log the keystrokes that a victim makes and send them back to the command-and-control centre. This gives the attacker access to the user's information.

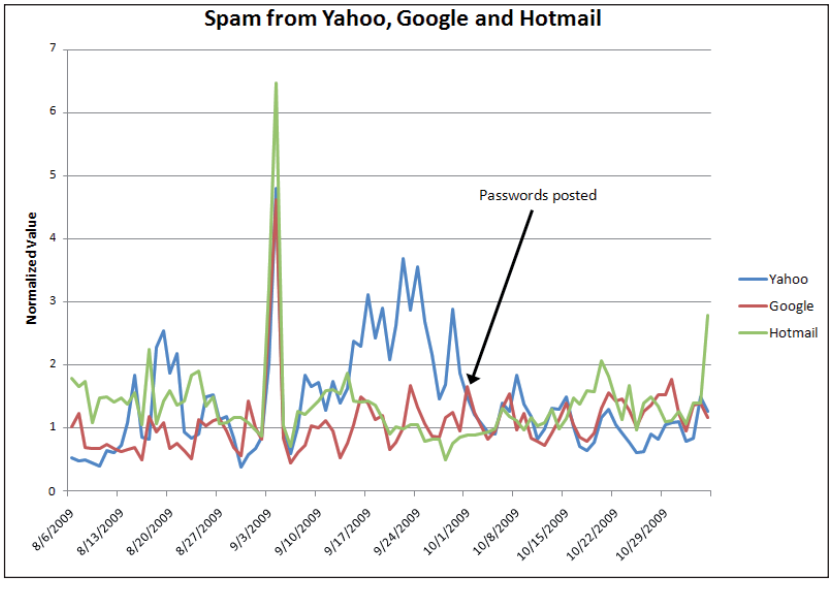
There are other ways to get infected, these include downloading music from disreputable sites, installing pirated software or visiting malicious web pages and becoming a victim of a drive-by download. In this instance, a piece of malware grabbing 'only' *Hotmail* passwords seems minor compared to stealing financial data. However, it would not be unusual for an attacker to gain access to data this way and a webmail password is a relatively innocuous piece of data to steal.

AN INCREASE IN SPAM?

The attack vector is wide and it probably involved tricking the user into taking action and unwittingly giving up their credentials, rather than breaking into *Hotmail* and acquiring them that way. But now we shift our focus elsewhere – did we see an increase in spam from these compromised accounts?

Why would a spammer steal usernames and passwords from *Hotmail*, *Yahoo!* and *Gmail* only to give them up later? I can think of a few reasons:

a) They stole the information to prove that they could do it in order to highlight the insecurity of the email space.



b) They used the stolen information to set up accounts on *Windows Live Spaces* (a blog) or open *SkyDrive* accounts (to store spam images).

c) They used the stolen information to send out volumes upon volumes of spam.

Option (a) is unlikely. People do not steal credentials these days to prove that they can, they do it for financial gain.

I cannot comment on (b) but I can comment on (c). Spam from services like *Hotmail*, *Yahoo!* and *Gmail* tends to be more difficult to filter because IP reputation filtering cannot be used without causing an unacceptably high level of false positives. I work for *Microsoft Forefront Online*, where amongst other tasks I collect various email statistics. For the last three months I have collected data on mail originating from IPs in these webmail services. I used the IPs in *Hotmail*'s SPF record, *Gmail*'s SPF record, and publicly available lists of *Yahoo!*'s IPs [7]. The chart above illustrates how much spam we receive from those three. I have normalized the values of the y-axis to hide the exact amount of spam that we receive from them.

The usernames and passwords were posted on 1 October 2009. Since that time, the amount of spam we received from all three services has declined somewhat. Instead, what we saw were huge increases on 3 September and 4 September followed by a rapid draw down – this was a month before the information was posted. *Yahoo!* spam increased throughout September but eventually declined right before the passwords were posted, whereas the other two services returned to normal levels straight after the outbreak. I checked *AOL*'s statistics and they also saw a huge spike on 3–4 September, but otherwise showed no significant deviation from their norm.

To me, this suggests the following:

1. Since the information was made public, there has not been an increase in spam.
2. It is difficult to say whether or not these accounts actually were used to spam; the only way to verify this would be to have the account names and go back through our logs, searching for them. I don't have the account usernames. I also do not know if the posted usernames are the full dataset that was compromised.
3. There was a huge spike on 3–4 September, which *may* correlate to these accounts. If I were to hazard a guess, I'd say that the spammer abused the accounts for these two days (only) and then abandoned them. He then posted them a month later to boast about what he did and to hint that he could do it again in the future.

Then again, there could be no relation at all and this could all be a coincidence. Isolated events are notoriously difficult to detect because there is so much variation within day-to-day events – that is, it can be difficult to separate the signal from the noise. Patterns that occur over time are easy to spot, but incidents like this are less so.

So, what do we know? We know that some users had their usernames and passwords stolen. We know that in early September, traffic from these services spiked. We know that a month later, the credentials were posted publicly and thus rendered useless. Whatever the motive was for stealing the accounts and then discarding them, email and Internet security still remain a serious issue to this day.

REFERENCES

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

[2] http://www.computerworld.com/s/article/9138945/Hacker_leaks_thousands_of_Hotmail_passwords_says_site.

[3] http://news.bbc.co.uk/2/hi/technology/8292928.stm.

[4] http://www.theregister.co.uk/2009/10/07/hotmail_phish_password/.

[5] Cartoon from http://xkcd.com/327/.

[6] See Microsoft's Security and Intelligence Report, version 7, p49. http://microsoft.com/sir.

[7] http://public.yahoo.com/~carloc/ymail-cidrs.txt.

COMPARATIVE REVIEW

WINDOWS 7

John Hawes

So *Windows 7* is finally with us. The hordes of users and admins who have put off migrating away from the stalwart *XP* can breathe a sigh of relief and finally start using a modern operating system. *Vista* can be consigned to the scrap heap of history, with the best of its innovations living on in it successor and the rest swiftly forgotten.

Perhaps that's going a little far; as a new and untried entity, *Windows 7* will at least have to do a little work to earn the approval and trust of cautious users. Initial impressions have generally been fairly positive, with speed, stability and style impressing many early adopters. Some teething problems were noted with many security products, but that was way back at the public beta stage and by now they should all have been resolved. We can only hope as much anyway, as this month's comparative takes place on the new platform, with the deadline for product submission having been just days after its official public release.

PLATFORM, TEST SETS AND METHODOLOGY

Unlike the general consensus elsewhere, our initial impressions of *Windows 7* were not entirely favourable. A trial installation of the *Ultimate* edition – to see how it got on with our hardware and tools, and to get a feel for what changes we needed to be aware of – proved somewhat problematic. A troublesome install process finally got us to a fully operational set-up, but *Explorer* seemed prone to odd behaviour, displaying only blackness within its shimmery semi-transparent framing until the right combination of clicks restored it to life. Meanwhile, the first blue screen was achieved within half an hour of installation.

Fortunately, the *Pro* edition selected for our tests proved more robust and well behaved. Getting all our test systems installed, activated and backed up with images was not an arduous task, with most of the steps fairly standard (although finding our way to some of the configuration controls proved a little bewildering thanks to some unnecessary adjustments to the layout).

With our lab hardware fully supported from the off, few changes were required to the standard installation besides a couple of handy tools to be used during testing – an archiving package to access submissions sent as archives and a PDF reader to check out manuals in case of unclear or unfamiliar products. Being rather simple folk easily overwhelmed by fancy graphics, we opted to revert the display to the plain, unflashy 'classic' style, intending to check out each product in the context of the snazzy 'Aero' options briefly, just to make sure they didn't look too out of place.

Getting the test sets and associated tools put together and onto the systems was also a relatively simple task. The test set deadline was 24 October, and the latest WildList available on that date, the September list, provided few surprises. The most dangerous of the Virut strains which rocked the last comparative was retired from the list, and our troublesome large set of samples thus removed to the polymorphic set. Additions to the WildList were dominated by online gaming and social networking threats, along with a sprinkling of autorun worms and Conficker variants. The polymorphic set was enlarged in terms of numbers of samples, but not greatly in terms of entirely new items, while the set of worms and bots was trimmed of some older items and enhanced with a selection of more recent arrivals. As usual, the trojans set was compiled entirely afresh, mostly with samples gathered during September while we were busy working on the last comparative. The RAP sets were populated as usual in the few weeks before the test, and in the week following the 28 October deadline for product submissions – meaning that testing could not start until well into November.

The deadline day proved a busy one, with products coming in thick and fast – a few new arrivals to spice things up, the usual flood of familiar faces, many of them providing both suite and AV-only variants, and one even submitting a free edition alongside the standard paid-for version. Many of our occasional entrants failed to materialize, perhaps put off by the potentially tricky new platform, but nevertheless the numbers stacked up to a monster 43 products. With a record field to test on what was likely to be a difficult platform, we knew that time would be against us.

Noting this time pressure, and having put together a fairly large and challenging set of infected samples to test against, we decided to make things extra hard for ourselves by expanding and deepening our performance tests. The standard speed sets were enhanced with a selection of files from the new operating system, while the clean set got a fairly large addition from CDs provided with hardware devices and magazines, and popular and recommended downloads from various software sites.

The speed tests were extended to take into account the performance-enhancing caching technologies included in many products these days. While in the past only one set of figures was reported for default handling of the speed sets, for this test we decided to include both 'cold' and 'warm' figures – that is, for the initial encounter with the files, and for subsequent rescans of the same items, measured multiple times and averaged to minimize anomalies. These

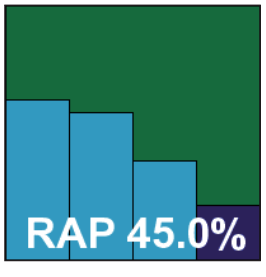
measurements were taken both on access and on demand, although the on-demand figures are perhaps somewhat less useful – most products will have been updated at least once between on-demand scans of the same items, which should mean that any cached data should be purged and items looked at afresh in case improved detection powers lead to something being spotted. The on-access data is much more relevant, as files may be accessed numerous times between updates and checking known files faster will significantly reduce the system footprint of the security solution.

We also introduced an update to our on-access measuring tool, opening files with the execute flag set to spark detection in a fuller range of products, and also taking MD5s of each file encountered and granted access to, in order to keep better track of unwanted changes to the testbeds. During testing we also gathered some more detailed performance measures, including records of CPU and memory consumption under various conditions, but given the heavy workload this month it was not possible to wrestle these figures into presentable shape in time for inclusion in the final report.

With all these schemes ready to go, and a tally of 43 products to get through, we shut ourselves away in the lab ready for a long and arduous, but what we hoped would be a productive month of testing.

AhnLab V3Net I.S. 8.0.2.0

ItW	99.99%	**Polymorphic**	99.58%
ItW (o/a)	99.99%	**Trojans**	65.55%
Worms & bots	96.85%	**False positives**	0

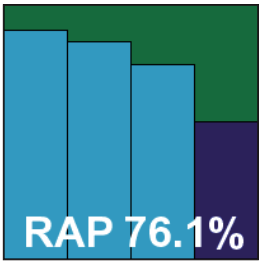


AhnLab's offering kicks off this month's review with few changes from its last few appearances. The installation process is fairly smooth and speedy, with minimal interruption from *Windows 7*'s UAC system – a single prompt for confirmation on commencing the install. The interface is fairly pleasant and reasonably usable, with a few quirks likely to fool the unwary, but generally simple to navigate and operate. Running through the tests proved unproblematic, although matters were slightly complicated by the separation of logging into items categorized as mere 'spyware' from those definitely malicious. After some careful merging of logging data some reasonable scores were recorded across the detection sets.

In the speed tests, scanning speeds were pretty decent but on-access overheads were a trifle heavy. No false positives were recorded, but in the WildList set a single sample of the last remaining W32/Virut strain was missed, thus denying *AhnLab* a VB100 once again.

Alwil avast! 4.8 Professional 4.8.1359

ItW	100.00%	**Polymorphic**	99.39%
ItW (o/a)	100.00%	**Trojans**	92.35%
Worms & bots	100.00%	**False positives**	0



This may be the last appearance in *VB*'s tests of the current version of *Alwil*'s popular *avast!* product, with a long-anticipated new edition due for release very soon. The install is uncomplicated and fairly speedy but does require a reboot of the system to complete, while the design of the interface remains somewhat unusual but provides a good range of fine-tuning for the more demanding user if switched to the advanced version. Running individual scans is a little fiddly, and logging can be problematic – initially limited to a fairly small size and, if a non-existent folder was mistakenly selected to write logs to, the process was silently disabled.

Detection rates were pretty solid across the test sets, with a steady decline as expected across the RAP sets but a strong starting level making for a very respectable overall average. Speeds were excellent, with some impressive improvements on access when files had been checked before. The WildList presented no difficulties and with no false positives either, *Alwil* earns this month's first VB100 award.

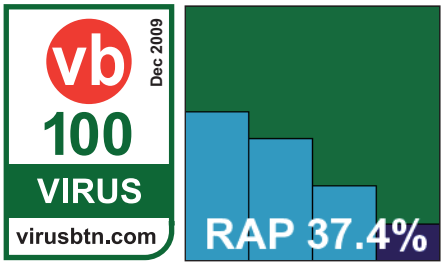
ArcaBit ArcaVir 2010 10.10.3201.4

ItW	100.00%	**Polymorphic**	61.83%
ItW (o/a)	100.00%	**Trojans**	54.99%
Worms & bots	94.96%	**False positives**	0

It has been a while since *ArcaBit* made an appearance in VB100 testing. The product's installer defaults to Polish, but is otherwise straightforward and very speedy, the installation process requiring less than a minute all told (although a reboot is required at the end). Running the tests proved a little more arduous, with multiple UAC prompts presented at various stages of accessing and adjusting the controls and extremely long pauses waiting for browser windows to be presented. Nevertheless, scanning speeds were decent – fast on demand and overheads not too heavy on access.

On-demand tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
AhnLab V3Net I.S.	1	99.99996%	60	96.85%	11	99.58%	6774	65.55%	0	0
Alwil avast! Professional	0	100.00%	0	100.00%	8	99.39%	1504	92.35%	0	0
ArcaBit ArcaVir	0	100.00%	96	94.96%	5411	61.83%	8850	54.99%	0	0
Authentium Command Anti-Malware	0	100.00%	1	99.95%	3	99.85%	2982	84.84%	0	0
AVG Internet Security	0	100.00%	0	100.00%	28	98.79%	1806	90.82%	0	0
Avira AntiVir Personal	0	100.00%	0	100.00%	0	100.00%	1056	94.63%	0	0
Avira AntiVir Professional	0	100.00%	0	100.00%	0	100.00%	1056	94.63%	0	0
BitDefender Antivirus	0	100.00%	0	100.00%	0	100.00%	1478	92.48%	0	0
Bullguard	0	100.00%	0	100.00%	0	100.00%	1321	93.28%	0	0
CA Internet Security Suite Plus	3	99.70%	0	100.00%	958	92.05%	11043	43.84%	1	0
CA Threat Manager	2	99.80%	0	100.00%	959	92.00%	12085	38.54%	0	0
eEye Blink Professional	0	100.00%	0	100.00%	265	83.90%	4860	75.29%	1	0
eScan Internet Security Suite	0	100.00%	0	100.00%	0	100.00%	1251	93.63%	0	0
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	1876	90.46%	0	0
Filseclab Twister Anti-TrojanVirus	1920	98.00%	71	96.27%	12298	38.09%	3850	80.42%	2	0
Fortinet FortiClient	0	100.00%	0	100.00%	6	99.92%	3579	81.80%	0	0
Frisk F-PROT	0	100.00%	1	99.95%	0	100.00%	3082	84.32%	0	0
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	1316	93.31%	0	0
F-Secure PC Protection	0	100.00%	0	100.00%	0	100.00%	1316	93.31%	0	0
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	637	96.76%	0	0
K7 Total Security	0	100.00%	0	100.00%	0	100.00%	5787	70.57%	0	0

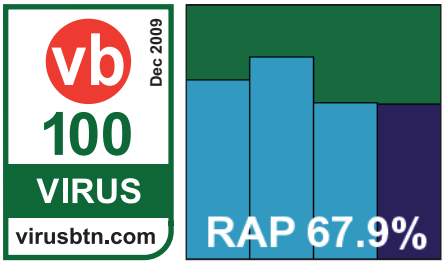
Detection rates were not bad in general. There was a marked decrease in coverage in the more recent weeks of the RAP sets, but the WildList was covered without problems despite the large numbers of previously unseen Virut samples. With the clean sets throwing up no show-stoppers either, *ArcaBit* earns its first VB100 award after a handful of sporadic appearances; we hope to see the product becoming a more regular entrant in the future.



Authentium Command Anti-Malware 5.1.0

ItW	100.00%	**Polymorphic**	99.85%
ItW (o/a)	100.00%	**Trojans**	84.84%
Worms & bots	99.95%	**False positives**	0

Authentium's product goes very much for simplicity, with a pared-down interface providing the bare minimum of control options, all of which are reasonably easy to find. Opening reports proved slow in the extreme, most likely thanks to the unusually large size which would not be experienced by normal users, but otherwise testing progressed without major difficulty.



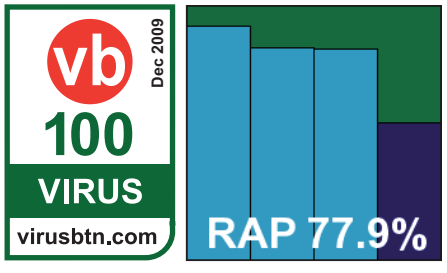
Scanning speeds were on the good side of medium and pretty light in terms of on-access overheads. Detection scores were fairly decent, with an especially strong showing in the proactive week of the RAP sets, and with no problems in the WildList and no false positives, *Authentium* safely qualifies for a VB100 award.

On-demand tests contd.	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Kaspersky Anti-Virus 2010	0	100.00%	0	100.00%	0	100.00%	1128	94.26%	0	0
Kaspersky Anti-Virus 6	0	100.00%	0	100.00%	0	100.00%	1167	94.06%	0	0
Kingsoft Anti-Virus 2010 Advanced	0	100.00%	1	99.95%	2387	56.60%	7239	63.19%	0	0
Kingsoft Anti-Virus 2010 Standard	0	100.00%	1	99.95%	2387	56.60%	15945	18.91%	0	0
Kingsoft Anti-Virus 2010 Swinstar	1	99.99996%	11	99.42%	2872	47.98%	9201	53.21%	0	0
McAfee Total Protection Suite	0	100.00%	0	100.00%	0	100.00%	2661	86.46%	0	0
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	2815	85.68%	0	0
Microsoft Forefront Client Security	8	99.29%	11	99.42%	5	99.78%	5796	70.52%	0	0
Microsoft Security Essentials	0	100.00%	0	100.00%	6	99.92%	1739	91.16%	0	0
Nifty Corporation Security 24	0	100.00%	27	98.58%	0	100.00%	2422	87.68%	0	0
Norman Security Suite	0	100.00%	0	100.00%	270	83.35%	4944	74.86%	0	0
PC Tools Internet Security	0	100.00%	1	99.95%	0	100.00%	1353	93.12%	0	0
PC Tools Spyware Doctor with AV	0	100.00%	1	99.95%	0	100.00%	1353	93.12%	0	0
Preventon Antivirus	0	100.00%	0	100.00%	193	89.10%	4069	79.31%	0	0
Qihoo 360 Security	0	100.00%	0	100.00%	0	100.00%	2071	89.47%	0	5
Quick Heal AntiVirus Lite	0	100.00%	0	100.00%	30	98.97%	3827	80.54%	0	0
Sophos Endpoint Security and Control	0	100.00%	0	100.00%	0	100.00%	2433	87.62%	0	0
Sunbelt Vipre	0	100.00%	3	99.84%	2018	65.24%	6600	66.43%	0	0
Symantec Endpoint Security	0	100.00%	0	100.00%	0	100.00%	1515	92.29%	0	0
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	582	97.04%	0	0
VirusBuster Professional	0	100.00%	0	100.00%	193	89.10%	4259	78.34%	0	0
Webroot AntiVirus with SpySweeper	0	100.00%	57	97.00%	0	100.00%	2659	86.48%	0	0

AVG Internet Security 9.0.697

ItW	100.00%	**Polymorphic**	98.79%
ItW (o/a)	100.00%	**Trojans**	90.82%
Worms & bots	100.00%	**False positives**	0

AVG's product had a very lengthy and complicated installation process, with numerous components to be put in place and configured. When the product is finally installed, it demands to be allowed to make an 'optimization scan'. If delayed, this scan is run anyway before any scheduled scan can take place – as we discovered when we set a scheduled job to run overnight, only to find on arrival the next morning that the optimization process was still running, and the requested job was yet to begin. Perhaps not helped by the incomplete optimization process, on-demand scans showed no sign of speeding up when run again over previously scanned data, and on access only a minimal improvement was observed on revisiting previously scanned files.

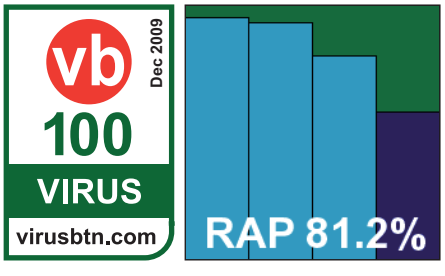


The interface occasionally proved rather slow to respond, especially when updating its display during large scans, but was generally reasonably easy to navigate, and a decent although not exhaustive level of configuration was available. Detection results were pretty solid, with no problems in the WildList and an excellent showing in the reactive portion of the RAP sets. With no false positives in the clean sets either, a VB100 is duly earned by *AVG*.

Avira AntiVir Personal 9.0.0.407

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.63%
Worms & bots	100.00%	**False positives**	0

On-access tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
AhnLab V3Net I.S.	1	99.99996%	60	96.85%	11	99.58%	7386	62.44%
Alwil avast! Professional	0	100.00%	0	100.00%	8	99.39%	1495	92.40%
ArcaBit ArcaVir	0	100.00%	96	94.96%	5411	61.83%	8872	54.88%
Authentium Command Anti-Malware	0	100.00%	0	100.00%	3	99.85%	2847	85.52%
AVG Internet Security	0	100.00%	0	100.00%	28	98.79%	1950	90.08%
Avira AntiVir Personal	0	100.00%	1	99.95%	6	99.92%	1057	94.62%
Avira AntiVir Professional	0	100.00%	0	100.00%	0	100.00%	1101	94.40%
BitDefender Antivirus	0	100.00%	0	100.00%	0	100.00%	1478	92.48%
Bullguard	0	100.00%	0	100.00%	0	100.00%	1322	93.28%
CA Internet Security Suite Plus	3	99.70%	0	100.00%	958	92.05%	16317	17.02%
CA Threat Manager	2	99.80%	2	99.89%	959	92.00%	12085	38.54%
eEye Blink Professional	13	99.999%	0	100.00%	397	82.01%	5211	73.50%
eScan Internet Security Suite	0	100.00%	0	100.00%	0	100.00%	1316	93.31%
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	2306	88.27%
Filseclab Twister Anti-TrojanVirus	1920	98.00%	64	96.64%	14235	30.39%	5814	70.43%
Fortinet FortiClient	0	100.00%	0	100.00%	6	99.92%	3579	81.80%
Frisk F-PROT	0	100.00%	1	99.95%	0	100.00%	3168	83.89%
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	1379	92.99%
F-Secure PC Protection	0	100.00%	0	100.00%	0	100.00%	1363	93.07%
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	720	96.33%
K7 Total Security	0	100.00%	0	100.00%	0	100.00%	5875	70.12%



Perhaps responding to the increased interest in free solutions of late, *Avira* opted to enter its free version in this month's test, and the product did not disappoint. The basic design and layout was pretty familiar to us from having used the professional edition, with a few minor adjustments, starting with the personal usage terms and conditions presented during the snappy install process. A few other areas also seemed different, with the default scanning depths perhaps a trifle less strict, and the on-access scanner lacking an option to simply block without prompting for an action. In the on-demand area, the GUI seemed to provide no option to scan a folder, offering to scan only entire drives or partitions, but a context-menu scan option provided more flexibility. These issues proved a little frustrating during our intensive on-access test, but not too upsetting, and otherwise the depth of configuration proved admirable.

Performance was excellent, with some very fast scanning speeds both on access and on demand, while detection rates proved as splendid as we have come to expect from the company. The test sets were demolished without apparent effort, with even the proactive portion of the RAP sets handled impressively. With no problems in the WildList, and no false alarms, *Avira*'s free Personal edition comfortably earns its first VB100 award.

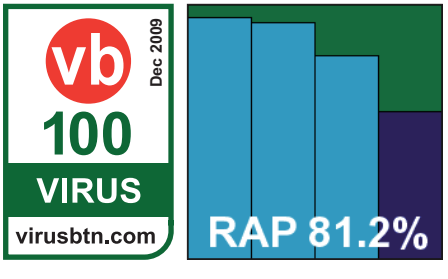
Avira AntiVir Professional 9.0.0.730

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.63%
Worms & bots	100.00%	**False positives**	0

The full paid-for version of *AntiVir*, as mentioned above, is pretty similar to the free one on the surface, but with a wider range of options and a deeper level of control

On-access tests contd.	WildList viruses		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Kaspersky Anti-Virus 2010	0	100.00%	0	100.00%	0	100.00%	1410	92.83%
Kaspersky Anti-Virus 6	0	100.00%	0	100.00%	0	100.00%	1626	91.73%
Kingsoft Anti-Virus 2010 Advanced	0	100.00%	1	99.95%	2387	56.60%	7329	62.73%
Kingsoft Anti-Virus 2010 Standard	0	100.00%	1	99.95%	2387	56.60%	16045	18.41%
Kingsoft Anti-Virus 2010 Swinstar	1	99.99996%	11	99.42%	2872	47.98%	9275	52.83%
McAfee Total Protection Suite	0	100.00%	0	100.00%	0	100.00%	2493	87.32%
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	2664	86.45%
Microsoft Forefront Client Security	20	98.07%	14	99.26%	6	99.92%	6126	68.85%
Microsoft Security Essentials	0	100.00%	0	100.00%	6	99.92%	2091	89.37%
Nifty Corporation Security 24	0	100.00%	27	98.58%	0	100.00%	2422	87.68%
Norman Security Suite	13	99.999%	0	100.00%	397	82.01%	5211	73.50%
PC Tools Internet Security	0	100.00%	2	99.89%	0	100.00%	1359	93.09%
PC Tools Spyware Doctor with AV	0	100.00%	2	99.89%	0	100.00%	1359	93.09%
Preventon Antivirus	0	100.00%	1	99.95%	193	89.10%	4081	79.24%
Qihoo 360 Security	0	100.00%	0	100.00%	0	100.00%	1590	91.91%
Quick Heal AntiVirus Lite	0	100.00%	0	100.00%	59	96.47%	6363	67.64%
Sophos Endpoint Security and Control	0	100.00%	0	100.00%	0	100.00%	2433	87.63%
Sunbelt Vipre	0	100.00%	3	99.84%	2033	65.08%	7035	64.22%
Symantec Endpoint Security	0	100.00%	0	100.00%	0	100.00%	1674	91.48%
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	696	96.46%
VirusBuster Professional	0	100.00%	0	100.00%	193	89.10%	4358	77.84%
Webroot AntiVirus with SpySweeper	0	100.00%	0	100.00%	0	100.00%	1171	94.04%

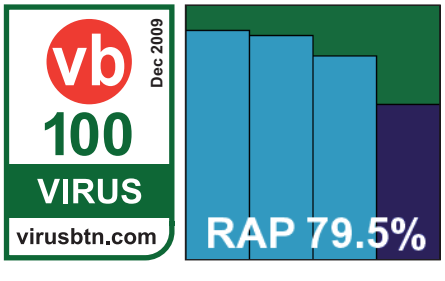
available. The set-up process is similarly simple although some post-install options are presented, including some extras such as detection of suspicious iframes. Logging is also clearer and more sophisticated than in the Personal edition, as befits a product intended to be put to use in a business environment.



Otherwise, little difference was observed – detection rates were identical to the free edition, while speed measures were as superb. Again no problems emerged in the WildList and no false positives were presented, and *Avira* adds a second VB100 to this month's haul.

BitDefender Antivirus 201013.0.16

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	92.48%
Worms & bots	100.00%	**False positives**	0



BitDefender's 2010 edition provides another redesign and another unusual look and feel. The install process is rather lengthy and features a number of command prompt windows flashing into view and disappearing again in an instant. A reboot is needed to complete the process. The new GUI has a simple, straightforward, rather chunky appearance,

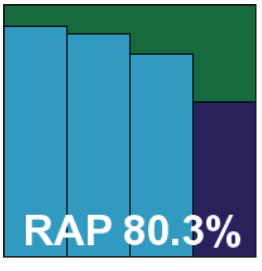
On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
AhnLab V3Net I.S.	10.49	10.81	10.49	30.41	30.22	30.41	10.73	10.88	10.73	9.66	10.02	9.66
Alwil avast! Professional	264.27	581.39	5.36	30.79	32.20	24.88	32.49	40.08	20.91	120.22	67.63	17.74
ArcaBit ArcaVir	6.58	6.62	6.58	16.20	16.48	16.20	24.54	29.32	24.54	14.43	16.15	14.43
Authentium Command Anti-Malware	6.29	6.28	6.29	13.57	13.76	13.57	19.08	25.05	19.08	12.02	14.62	12.02
AVG Internet Security	0.71	0.71	0.68	12.47	12.83	12.35	7.40	7.56	6.81	5.06	5.15	3.95
Avira AntiVir Personal	4.90	5.02	4.58	43.98	47.37	43.98	17.55	22.06	16.36	17.45	21.22	14.62
Avira AntiVir Professional	4.84	5.03	4.61	44.38	52.97	44.38	17.18	21.86	16.93	15.24	20.04	18.34
BitDefender Antivirus	11.31	171.00	1.49	16.48	26.63	12.76	5.68	7.78	4.04	3.78	4.90	4.23
Bullguard	2.68	2.67	2.68	24.88	24.88	24.88	8.59	8.56	8.59	6.68	6.72	6.68
CA Internet Security Suite Plus	181.68	1453.47	1.11	26.77	15.30	32.84	14.84	114.50	6.25	108.20	90.17	90.17
CA Threat Manager	1.48	1.78	1.37	39.73	41.75	33.74	22.26	28.97	18.79	27.74	21.64	17.45
eEye Blink Professional	2.97	2.96	2.97	2.67	2.70	2.67	6.17	7.03	6.17	4.28	4.72	4.28
eScan Internet Security Suite	2.27	2.27	2.26	2.69	2.70	2.67	0.49	0.50	0.49	0.36	0.37	0.36
ESET NOD32 Antivirus	2.40	2.48	2.40	17.59	17.72	17.59	15.12	16.03	15.12	12.44	14.24	12.44
Filseclab Twister Anti-TrojanVirus	1.12	1.12	1.12	19.39	19.47	19.24	5.53	6.04	5.49	5.13	5.15	4.68
Fortinet FortiClient	4.51	4.53	4.51	9.58	9.21	9.58	22.90	18.50	22.90	11.63	16.15	11.63
Frisk F-PROT	7.25	7.29	7.21	12.70	13.14	12.70	32.94	34.35	32.94	23.52	23.02	23.52
F-Secure Internet Security	7.57	7.69	7.57	24.15	24.63	24.15	14.40	18.79	14.40	77.29	90.17	77.29
F-Secure PC Protection	7.79	2906.94	2.65	24.39	2463.05	23.57	14.40	400.75	11.50	83.23	541.00	8.94
G DATA AntiVirus	2.62	968.98	2.62	18.24	1642.04	18.24	10.06	343.50	10.06	10.21	360.67	10.21
K7 Total Security	6.92	7.02	6.92	11.05	10.87	11.05	27.02	35.89	27.02	17.45	1.56	17.45

with the layout variable for each of a selection of user profiles – an interesting and effective approach to allowing the advanced user a decent level of control while avoiding frightening the novice. A number of other interesting features are included, such as home network configuration controls, vulnerability management and system configuration options, alongside the core anti-malware protection elements which proved as solid as ever.

Detection rates were excellent across the test sets, while in the performance measures scanning speeds proved fairly slow on first sight of files but improved notably on revisiting them, with a particularly impressive improvement on access. The WildList was handled comfortably, and with no false positives *BitDefender* earns a VB100 award.

Bullguard 8.7.1.17

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



Incorporating the *BitDefender* detection engine, *Bullguard*'s product proved much faster and easier to install, but again a reboot is needed for full operation. Its overwhelmingly red interface felt a trifle cluttered, but with a little exploration proved nicely laid out and fairly simple to use – although the process of setting up and running a custom scan is a little long-winded, and requires the approval of a UAC prompt.

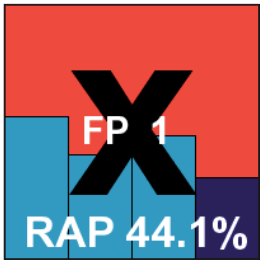
Detection rates, as expected, were along the same lines as those achieved by *BitDefender* – a very respectable showing – while in the speed tests medium rates were recorded with no change on second viewing of the files. No problems cropped up in the WildList or the clean sets, and a VB100 is duly earned by *Bullguard*.

On-demand throughput (MB/s) contd.	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Kaspersky Anti-Virus 2010	1.99	13.46	1.99	0.61	2.35	0.61	0.24	0.90	0.24	0.66	108.20	0.66
Kaspersky Anti-Virus 6	4.51	35.89	4.51	47.83	223.91	47.83	19.39	70.72	19.39	14.82	54.10	14.82
Kingsoft Anti-Virus 2010 Advanced	1.34	1.34	1.34	27.37	26.48	27.37	5.44	5.74	5.44	13.36	20.42	13.36
Kingsoft Anti-Virus 2010 Standard	1.35	1.36	1.35	26.20	25.26	26.20	5.39	5.67	5.39	14.05	18.03	14.05
Kingsoft Anti-Virus 2010 Swinstar	2.97	3.14	2.97	57.28	66.57	57.28	23.57	30.44	23.57	17.74	23.52	17.74
McAfee Total Protection Suite	1.44	1.53	1.44	10.95	11.02	10.95	6.87	6.48	6.87	4.57	4.55	4.57
McAfee VirusScan Enterprise	111.81	145.35	2.20	18.66	19.17	17.35	8.23	8.59	8.10	6.04	5.85	5.46
Microsoft Forefront Client Security	2.95	2.95	2.95	14.24	14.24	14.24	20.55	21.28	20.55	12.88	13.53	12.88
Microsoft Security Essentials	2.69	3.74	2.69	13.14	13.53	13.14	18.22	20.38	18.22	11.63	12.58	11.63
Nifty Corporation Security 24	2.50	726.73	2.50	22.09	182.45	22.09	8.50	32.49	8.50	6.40	26.39	6.40
Norman Security Suite	1.68	1.79	1.68	2.72	2.69	2.72	6.17	5.49	6.17	4.28	3.78	4.28
PC Tools Internet Security	1.14	1.08	1.14	7.56	38.49	7.56	5.78	5.82	5.78	4.85	4.77	4.85
PC Tools Spyware Doctor with AV	1.27	1.16	1.27	8.66	32.62	8.66	6.36	5.84	6.36	5.46	4.81	5.46
Preventon Antivirus	46.89	88.09	NA	4.49	12.32	4.49	11.62	20.55	11.62	10.61	11.76	10.61
Qihoo 360 Security	1.84	1.80	1.84	18.38	18.11	18.38	7.05	6.91	7.05	5.46	5.23	5.46
Quick Heal AntiVirus Lite	1.87	2.02	1.34	38.19	41.05	40.71	9.04	9.90	8.78	8.14	9.41	7.17
Sophos Endpoint Security and Control	207.64	264.27	2.23	19.39	19.39	14.57	14.48	16.14	11.50	9.09	9.33	7.62
Sunbelt Vipre	116.28	171.00	NA	18.87	23.46	NA	4.05	4.17	NA	6.22	6.68	NA
Symantec Endpoint Security	2.36	2.28	2.36	22.49	23.24	22.49	10.19	10.50	8.23	8.94	9.75	8.94
Trustport Antivirus	1.47	1.44	1.47	7.48	8.72	7.48	6.03	5.78	6.03	3.74	3.95	3.74
VirusBuster Professional	6.28	6.28	1.73	20.11	16.81	18.59	12.66	12.86	9.98	11.51	11.89	9.41
Webroot AntiVirus with SpySweeper	2.60	2.60	2.60	14.70	15.64	14.70	15.03	14.66	15.03	8.32	8.32	8.32

CA Internet Security Suite Plus 2010

ItW	99.70%	**Polymorphic**	92.05%
ItW (o/a)	99.70%	**Trojans**	43.84%
Worms & bots	100.00%	**False positives**	1

CA's home-user offering arrives following a major overhaul, with a redesigned interface promising some stylistic innovations. The installation begins with some extremely large icons, and after a long and slow process requires a reboot before presenting a final interface which is equally large-featured. The design is indeed unusual, with its swirling 3D tabs and icons apparently inspired by computer systems used on the TV show *CSI: Miami*. Clearly, it is intended to provide a simple and user-friendly experience for the most inexperienced users. For us, however, it proved baffling in the extreme, with the tiny amount of configuration available proving both tricky to find and perplexing to make use of; perhaps with experience its mysteries will be unravelled.



An attempt to run scans from the GUI – when the appropriate area was at last uncovered – proved very slow to access the filesystem browsing details. A context-menu entry is provided for simpler initiation of specific scans, but is also somewhat confusing, with multiple nested options and the option to exclude an area from scanning given prominence over the scan itself. Scanning speeds seemed remarkably fast – as we have come to expect from *CA* solutions – but on repeated attempts showed some worrying oddities. Most rescans proved slightly faster than the first attempt, as might be expected, but some were significantly slower and apparently scanning at a greater depth (with no change to the options). On one occasion a component of the useful *Sysinternals* suite was alerted on as a potential

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
AhnLab V3Net I.S.	0.019	0.019	NA	0.031	0.031	0.031	0.085	0.084	0.085	0.095	0.095	0.095
Alwil avast! Professional	0.025	0.000	0.195	0.042	0.003	0.052	0.042	0.002	0.061	0.049	0.001	0.060
ArcaBit ArcaVir	0.006	0.006	0.138	0.049	0.046	0.051	0.032	0.030	0.034	0.024	0.022	0.064
Authentium Command Anti-Malware	0.024	0.025	NA	0.079	0.078	NA	0.046	0.045	NA	0.062	0.060	NA
AVG Internet Security	0.004	0.003	0.013	0.070	0.069	0.066	0.093	0.091	0.100	0.145	0.141	0.171
Avira AntiVir Personal	0.009	0.005	0.008	0.020	0.005	0.020	0.053	0.034	0.052	0.058	0.057	0.056
Avira AntiVir Professional	0.009	0.009	0.046	0.020	0.020	0.021	0.052	0.052	0.053	0.058	0.056	0.057
BitDefender Antivirus	0.009	0.004	0.391	0.041	0.007	0.046	0.125	0.010	0.134	0.163	0.013	0.172
Bullguard	0.212	0.210	0.209	0.044	0.042	0.043	0.135	0.137	0.130	0.169	0.175	0.162
CA Internet Security Suite Plus	0.009	0.009	NA	0.028	0.026	0.028	0.056	0.058	0.056	0.036	0.032	0.036
CA Threat Manager	0.008	0.008	0.009	0.022	0.022	0.060	0.039	0.037	0.085	0.041	0.042	0.081
eEye Blink Professional	0.009	0.008	NA	0.086	0.085	NA	0.150	0.149	NA	0.169	0.167	NA
eScan Internet Security Suite	0.417	0.001	0.425	0.077	0.001	0.057	0.130	0.002	0.128	0.181	0.001	0.178
ESET NOD32 Antivirus	0.002	0.002	0.001	0.009	0.008	0.009	0.058	0.059	0.062	0.055	0.053	0.056
Filseclab Twister Anti-TrojanVirus	0.005	0.006	0.006	0.017	0.017	0.017	0.109	0.110	0.108	0.017	0.016	0.015
Fortinet FortiClient	0.181	0.000	0.195	0.093	0.000	0.098	0.064	0.002	0.055	0.126	0.003	0.114
Frisk F-PROT	0.010	0.009	0.009	0.077	0.076	0.078	0.025	0.023	0.025	0.036	0.035	0.037
F-Secure Internet Security	0.004	0.002	NA	0.056	0.005	NA	0.108	0.004	NA	0.029	0.006	NA
F-Secure PC Protection	0.004	0.001	NA	0.054	0.003	NA	0.109	0.005	NA	0.031	0.004	NA
G DATA AntiVirus	0.096	0.003	0.572	0.079	0.007	0.087	0.164	0.015	0.168	0.225	0.020	0.222
K7 Total Security	0.020	0.002	0.001	0.093	0.002	0.005	0.035	0.008	0.007	0.057	0.012	0.013

hacking tool. Despite having been missed on two previous scans and going unnoticed again on two subsequent runs.

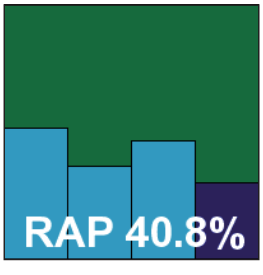
SEE UPDATE P43

In the infected sets, detection was less than excellent, with three items in the WildList set not detected: an autorun worm and a pair of online gaming password-stealers. Furthermore, while running the performance tests a .DLL file included with the *Windows 7* operating system (in the system32 folder) was alerted on as a 'Startpage' trojan; *CA*'s new-look product is thus denied a VB100 award this month.

CA Threat Manager 8.1.655.0

ItW	99.80%	**Polymorphic**	92.00%
ItW (o/a)	99.80%	**Trojans**	38.54%
Worms & bots	100.00%	**False positives**	0

According to the vendor, *CA*'s business product is no longer to be referred to as *'eTrust'* – but despite this it continues to carry *'eTrust'* branding at various points and persists in using a rather old-fashioned and less than satisfactory interface. However, we understand that the long-awaited redesign is on the horizon at last.



We have learnt through long and painful experience how to cope with the quirks and oddities of this product's layout, although the responsiveness issues noted in previous tests were less evident here than on some other platforms. Some particular areas of frustration remained, including the reverting of some option selections from scan to scan, the absence of archive scanning on access despite the provision of a setting to enable it, and the awkward logging which put such a strain on the interface trying to interpret and display the data that on one attempt the machine overheated and rebooted.

Eventually, though, it did manage to display its own logs in a fairly usable format – a first for the product – and detection rates seemed somewhat better than previous rather disappointing levels. However, despite the autorun worm being handled properly this time, the two gaming trojans

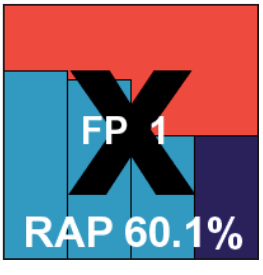
File access lag time (s/MB) contd.	Archive files			Binaries and System files			Media and Documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Kaspersky Anti-Virus 2010	0.005	0.003	NA	0.037	0.003	0.037	0.064	0.013	0.064	0.088	0.017	0.088
Kaspersky Anti-Virus 6	0.004	0.000	0.211	0.038	0.001	0.001	0.070	0.007	0.006	0.097	0.009	0.008
Kingsoft Anti-Virus 2010 Advanced	0.005	0.002	NA	0.034	0.005	0.003	0.175	0.006	0.005	0.055	0.006	0.003
Kingsoft Anti-Virus 2010 Standard	0.004	0.002	NA	0.030	0.003	0.007	0.174	0.005	0.030	0.053	0.004	0.010
Kingsoft Anti-Virus 2010 Swinstar	0.005	0.003	NA	0.017	0.005	0.017	0.040	0.005	0.040	0.051	0.007	0.051
McAfee Total Protection Suite	0.006	0.003	NA	0.082	0.034	0.082	0.140	0.059	0.140	0.211	0.065	0.211
McAfee VirusScan Enterprise	0.007	0.005	0.411	0.058	0.028	0.054	0.145	0.076	0.138	0.205	0.101	0.200
Microsoft Forefront Client Security	0.005	0.000	NA	0.066	0.001	0.066	0.035	0.002	0.035	0.065	0.002	0.065
Microsoft Security Essentials	0.007	0.002	NA	0.067	0.005	0.067	0.037	0.005	0.037	0.066	0.006	0.066
Nifty Corporation Security 24	0.013	0.004	NA	0.049	0.008	0.049	0.110	0.031	0.110	0.132	0.020	0.132
Norman Security Suite	0.006	0.006	NA	0.085	0.085	0.085	0.156	0.156	0.156	0.177	0.175	0.177
PC Tools Internet Security	0.003	0.002	NA	0.009	0.007	NA	0.017	0.019	NA	0.027	0.026	NA
PC Tools Spyware Doctor with AV	0.013	0.007	NA	0.169	0.008	NA	0.063	0.043	NA	0.062	0.059	NA
Preventon Antivirus	0.006	0.002	NA	0.091	0.003	NA	0.005	0.001	NA	0.013	0.002	NA
Qihoo 360 Security	0.001	0.006	NA	0.036	0.001	NA	0.037	0.004	NA	0.030	0.007	NA
Quick Heal AntiVirus Lite	0.005	0.005	NA	0.021	0.021	0.021	0.086	0.088	0.086	0.098	0.096	0.098
Sophos Endpoint Security and Control	0.003	0.003	0.360	0.049	0.048	0.052	0.038	0.038	0.049	0.082	0.081	0.096
Sunbelt Vipre	0.007	0.019	NA	0.046	0.033	NA	0.255	0.093	NA	0.162	0.106	NA
Symantec Endpoint Security	0.008	0.006	0.001	0.046	0.046	0.046	0.061	0.059	0.061	0.053	0.052	0.053
Trustport Antivirus	0.024	0.000	1.155	0.164	0.002	0.193	0.254	0.057	0.279	0.368	0.013	0.410
VirusBuster Professional	0.005	0.004	0.012	0.044	0.043	0.044	0.030	0.030	0.050	0.093	0.090	0.107
Webroot AntiVirus with SpySweeper	0.000	0.001	NA	0.030	0.028	0.030	0.022	0.024	0.022	0.029	0.032	0.029

were missed once again. In the clean sets there was no sign of the false positive found by the consumer product, but nevertheless, *CA*'s business solution is also denied a VB100 award this month.

eEye Blink Professional 4.5.0

ItW	100.00%	**Polymorphic**	83.90%
ItW (o/a)	99.99%	**Trojans**	75.29%
Worms & bots	100.00%	**False positives**	1

The *Blink* product submitted for this month's test is a late-stage beta, due for final release around the time this review will be published, and thus a few oddities are only to be expected. After a fairly straightforward and reasonably pacey install process, some areas of the nicely designed interface failed to operate properly, presenting some rather stark messages reading simply 'Parameter is incorrect'. However, after a reboot, and with some patience, testing was completed without serious problems. We noted that the firewall bundled with the product is disabled by default, but some of the other additions, such as the vulnerability scanner and intrusion-detection controls, impressed us greatly. The anti-malware component is only a minor part of the offering, and is thus granted less space in the configuration areas than might be desired by more demanding users.

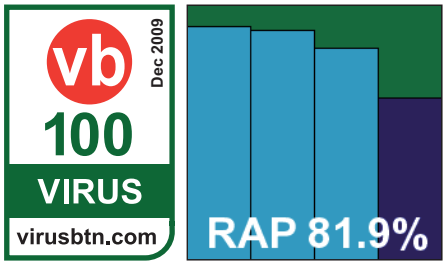


The product incorporates the *Norman* engine, and the implementation of sandboxing of unknown files may well account for some rather sluggish scanning speeds over executable files on demand. The sandbox came into its own in the detection tests, with the on-demand results proving rather better than the on-access ones, where less intensive scanning is provided. This was something of a problem for

eEye in the WildList set, though, where a handful of W32/Virut samples were missed by the on-access component, although spotted by the sandbox on demand. In the clean sets, the same .DLL file which caused trouble for the *CA* consumer product was alerted on. Thus, despite a generally solid performance, *eEye* does not qualify for a VB100 award this month.

eScan Internet Security Suite 10.0.1004.561

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.63%
Worms & bots	100.00%	**False positives**	0



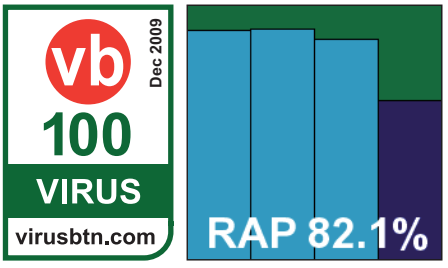
The latest version of *eScan* has another rather lengthy installation process with a number of long pauses, and a reboot to cap things off. When up and running, the interface proved somewhat poorly laid out but fairly usable with a little practice. Once again there were problems accessing browser windows when setting up scans. The product includes a number of extra features, including controls for managing removable USB devices and application control.

During the process of running some of the more demanding scans of the infected sets, an error window was presented, warning the user that the product had stopped working. However, scanning seemed to continue unimpeded and further investigation showed that on-access protection was also fully operational. Scanning speeds in the clean set were slow in the extreme, with no sign of speeding up on repeated runs, but the product remained solid and well behaved throughout. Detection rates continue to impress with strong scores across all sets, and with no issues in the WildList or clean sets a VB100 award is well deserved.

ESET NOD32 Antivirus 4.0.467.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.46%
Worms & bots	100.00%	**False positives**	0

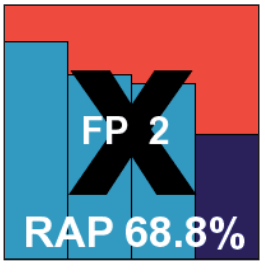
ESET's product remains much as it has been for some time: pleasantly designed with an efficient and lucid layout. The install process is simple and needs no reboot, and protection is up and running with ease. Configuration is as in-depth as could be desired, although options to enable the scanning of archives on access seemed to produce no increase in scanning when enabled.



At one point during the most intensive scan of the infected sets the product became a little overwhelmed, consuming rather more than its share of memory and requiring a reboot to return the system to a functioning state. In more normal activities no problems were observed however, with scanning speeds unaffected by repeated runs but fast enough to be beyond complaint. Detection rates were very solid, with a commendable regularity across the reactive part of the RAP sets and still fairly strong in the proactive portion. With no trouble handling the WildList or clean sets, *ESET* adds yet another VB100 award to its tally.

Filseclab Twister Anti-TrojanVirus 7.3.4.99.85

ItW	98.00%	**Polymorphic**	38.09%
ItW (o/a)	98.00%	**Trojans**	80.42%
Worms & bots	96.27%	**False positives**	2



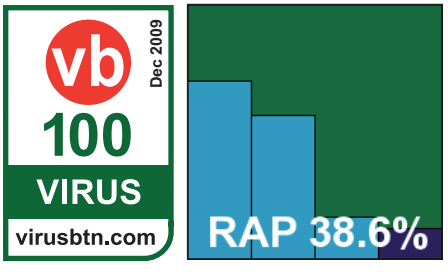
Filseclab's product has a slow installation process and requires a reboot to complete. The interface is pleasantly designed and simply laid out (although the configuration screen is rather cluttered with a wealth of options described in less than helpful language). It seemed splendidly stable and responsive throughout testing. On-demand scanning proved fairly slow and showed no sign of speeding up once familiar with files, while the on-access protection did not appear to fully intercept file accesses, merely logging detections after allowing them to be accessed. As a result, the on-access speed measurements may appear faster than they ought.

Detection rates were generally fairly good, with solid scores in the trojans set and decent levels across the RAP sets despite a steady decline as the samples grew fresher. In the WildList set a number of items were not detected, including fair numbers of the W32/Virut strain – a failing that was also seen in the other polymorphic strains in the detection

sets. In the clean sets a small number of false positives were noted, with some components of the popular freeware image manipulation solution *The Gimp* misidentified rather vaguely as 'Trojan.Obfuscated' – clearly a very generic detection algorithm applied slightly too severely in this case. Between them these issues are enough to deny *Twister* a VB100 award once again, despite continuing signs of improvement.

Fortinet FortiClient 4.0.1.054

ItW	100.00%	**Polymorphic**	99.92%
ItW (o/a)	100.00%	**Trojans**	81.80%
Worms & bots	100.00%	**False positives**	0



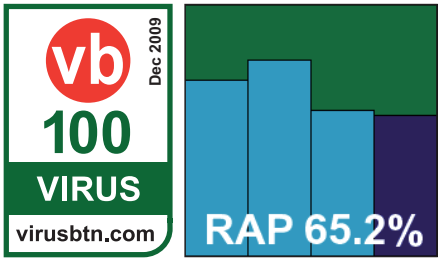
FortiClient proved a little tricky to install on *Windows 7*, with two UAC prompts before the installer got started on a process doomed to fail very shortly. Re-running the installation numerous times while applying varying options to the useful compatibility troubleshooting tool provided by the operating system eventually got things rolling. When the product was finally installed and running the interface offered excellent clarity of design and a fairly thorough selection of options – appropriate for a predominantly business-focused solution. One issue observed with the GUI was that the 'restore defaults' control failed to reset changes made in advanced subsections.

Scanning speeds were in the mid-range, but stability was maintained even under pressure and detection rates showed notable improvement over recent tests. No issues were observed in the WildList or clean sets, and a VB100 award is duly earned.

Frisk F-PROT 6.0.9.3

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	84.32%
Worms & bots	99.95%	**False positives**	0

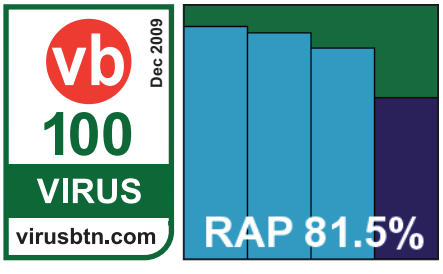
F-PROT continues to offer icy minimalism, with a swift and straightforward install process impeded only by a single UAC prompt and the need for a reboot to complete. The interface provides few options but caters for the basics in an admirably clear way. Scanning speeds were fairly reasonable but showed no sign of advanced caching of known-clean files, and detection rates were decent but not overly impressive.



With full coverage of the WildList set and no false positives, *F-PROT* also earns a VB100 award this month.

F-Secure Internet Security 2010 10.00 build 246

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.31%
Worms & bots	100.00%	**False positives**	0

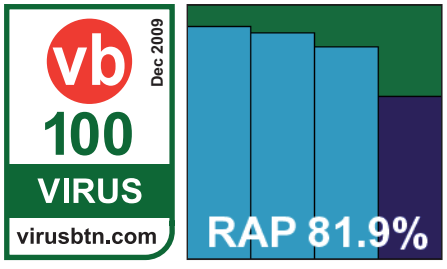


F-Secure's latest product version features a notable redesign, starting with a heavily automated install process requiring minimal user intervention – even offering to remove any existing protective solutions – but taking some time and needing a reboot. On restarting the system a notable heaviness was apparent, with *Windows* taking some time to come back to life, and a number of large and intrusive pop-ups from the HIPS system warned of potentially unwanted behaviour on the part of several standard *Windows* components, including the *Malicious Software Removal Tool* (although such behaviour may have been influenced by the lack of an Internet connection to check with cloud-based systems).

Our first attempt at running the test proved fruitless as the on-access component appeared completely non-functional, but on reinstalling on a second test machine the issue did not recur. Once everything was working properly testing proceeded without further interruption, with some fairly decent scanning speeds and splendid detection rates. Even the highly inefficient and precarious logging system proved more reliable on this occasion. There were no problems in the WildList and no false positives in the clean sets, and as a result a VB100 award is easily earned.

F-Secure PC Protection 9.01

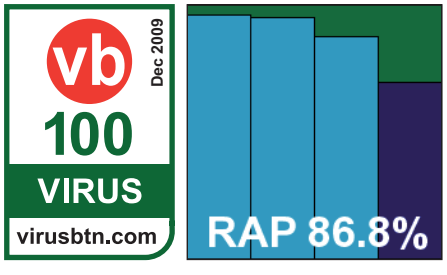
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.31%
Worms & bots	100.00%	**False positives**	0



F-Secure's second submission this month is the company's rebrandable version provided to users via ISPs and so on. It is fairly similar to the 2010 version in design and user experience, even down to the annoying pop-ups warning about *Windows* components. Scanning speeds were similarly reasonable and detection rates likewise excellent, and with an identical showing in the core sets a second VB100 award goes to *F-Secure* this month.

G DATA AntiVirus 2010 20.2.1.13

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.76%
Worms & bots	100.00%	**False positives**	0



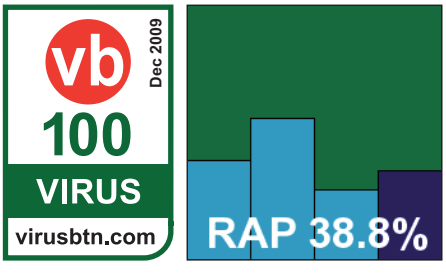
G DATA's 2010 edition has a rather higher than usual number of steps to its installation process, including the set-up of the malware feedback system for reporting detections back to base. The latest version of the interface is clear and uncluttered with a pleasantly logical layout. Configuration is made available at a reasonable depth – with some more specialist requirements perhaps missing, but quite ample for the average user.

A few oddities were observed, with the most notable examples being a somewhat low default limit on archive scanning (300KB) and the intrusion of a UAC prompt before any on-demand scan can be run. Logging is also a little frustrating, with reports stored in an awkward format which proved something of a strain for the product to interpret into human-readable form if allowed to grow too large. Initial scanning speeds were fairly slow, as expected from a multi-engine approach, but on repeat viewing of previously seen files speeds proved lightning fast, with the same pattern of improvement showing again in the on-access tests, demonstrating some sterling effort at keeping overheads down through caching.

Detection rates, as we have come to expect from *G DATA*, were stratospheric, setting a seriously tough benchmark for others to aim for across all the sets, with even the proactive portion of the RAP sets handled admirably. With barely a whisper of a miss in the standard sets the WildList proved something of a breeze, and with no false alarms either *G DATA* easily earns another VB100 award for its effort.

K7 Total Security 10.0.0020

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	70.57%
Worms & bots	100.00%	**False positives**	0

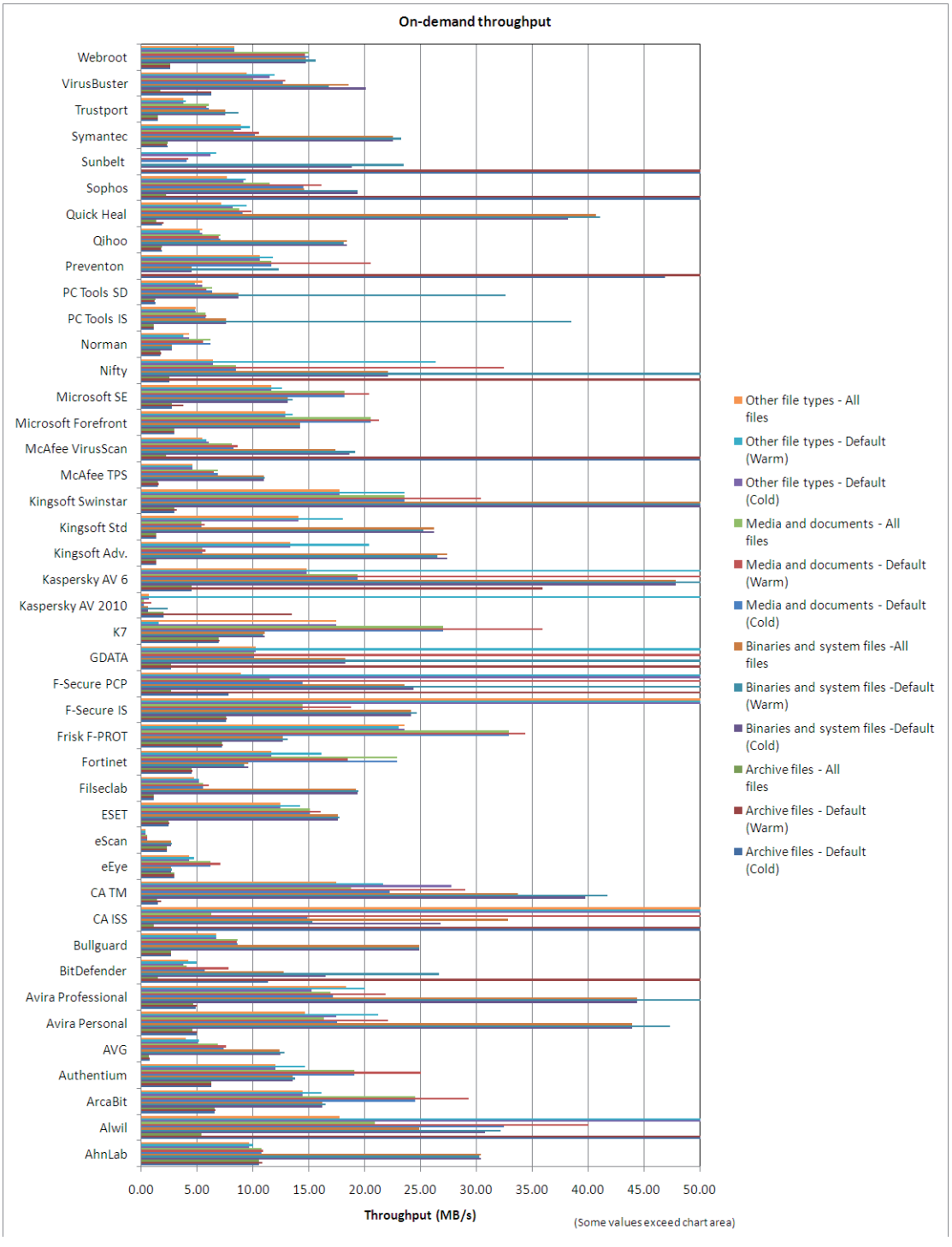


K7's installation process is nice and speedy, with a single UAC prompt at the start, a standard set of stages including a check for conflicting third-party software, and no reboot required. The interface is simple and pleasant, providing an ample level of configuration for the average home user in a rational and usable layout. Logging was a minor problem, with the viewer window freezing on attempting to view unusually large logs, but this minor issue is unlikely to affect the majority of users. The only other oddity observed was the occasional zero missing from scan duration times, which was no more than a little confusing.

Detection rates proved pretty decent, with most of the older sets handled with aplomb and a decent score in the trojans set, while the RAP scores proved a little uneven, with the 'week +1' set handled marginally better than the 'week -1' set. The WildList presented no difficulties however, and with no false positives in the clean sets either, *K7* wins a VB100 award and our gratitude for a nice easy run through the tests.

Kaspersky Anti-Virus 2010 9.0.0.736

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.26%
Worms & bots	100.00%	**False positives**	0



Kaspersky's latest consumer offering is as glossy and shiny a beast as ever; the install is no slower than the average and getting at the new-look interface didn't take long. The redesign caused a few moments of confusion on first approach, but soon became familiar and simple to use. A vast wealth of fine-tuning options are provided under the attractive surface, including some interesting features like the keylogger-proof 'virtual keyboard'.

Archive scanning		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
AhnLab V3Net I.S.	Default	X	√	X	X	√	√	X	√	√
	All	X	X	X	X	X	X	X	X	√
Alwil avast! Professional	Default	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
	All	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
ArcaBit ArcaVir	Default	2	√	√	√	√	√	√	√	√
	All	X/2	X/√	√	X/√	X/√	X/√	X/√	X/√	X/√
Authentium Command Anti-Malware	Default	5	5	5	5	√	5	2	5	√
	All	X	X	X	X	X	X	X	X	X
AVG Internet Security	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Avira AntiVir Personal	Default	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/ √	X/√	X/√	X/√	X/√	X/√	√
Avira AntiVir Professional	Default	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Antivirus	Default	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	√
	All	X/√	X/√	X/√	2/√	X/√	X/√	X/√	1/√	√
Bullguard	Default	√	√	8	√	√	√	8	√	√
	All	√	√	8	√	√	√	8	√	√
CA Internet Security Suite Plus	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	1	X	X	X	1	√
CA Threat Manager	Default	X	X/9	X/9	1/9	X/9	X/9	X/9	1/√	√
	All	X	X	X	1	X	X	X	1	√
eEye Blink Professional	Default	X	1	X	1	1	1	2/5	2	√
	All	X	X	X	X	X	X	X/5	X	√
eScan Internet Security Suite	Default	√	√	8	√	√	√	√	8	√
	All	√	√	9	√	√	√	√	9	√
ESET NOD32 Antivirus	Default	√	v	√	√	√	√	5	√	√
	All	X	X	X	X	X	X	X	X	√
Filseclab Twister Anti-TrojanVirus	Default	7/ √	5/√	5/ √	6/√	1	6/√	X	7/√	v
	All	X	X	X	X	X	1	X	2	X
Fortinet FortiClient	Default	X	√	√	√	√	√	√	4	√
	All	X	√	√	√	√	√	√	4	√
Frisk F-PROT	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	2	X	X	X	2	√
F-Secure Internet Security	Default	X	√	8	√	√	√	8	√	√
	All	X	X	X	X	X	X	X	X	X
F-Secure PC Protection	Default	X	√	8	√	√	√	8	√	√
	All	X	X	X	X	X	X	X	X	X
G DATA AntiVirus	Default	√	√	√	√	√	√	√	√	√
	All	√	√	4/ √	√	√	√	8/ √	8/ √	√
K7 Total Security	Default	√	√	√	√	√	√	√	√	√
	All	1	X	1	1	X	X	X	1	√

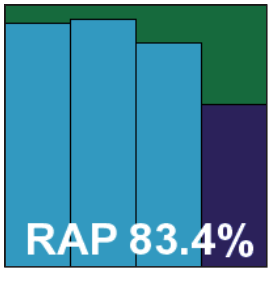
Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels

Archive scanning contd.		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Kaspersky Anti-Virus 2010	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Kaspersky Anti-Virus 6	Default	√	√	√	√	√	√	√	√	√
	All	X/ √	X/ √	X/ √	X/ √	X/ √	X/ √	X/ √	X/ √	√
Kingsoft Anti-Virus 2010 Advanced	Default	X	√	X	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Kingsoft Anti-Virus 2010 Standard	Default	X	√	X	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Kingsoft Anti-Virus 2010 Swinstar	Default	X	X	X	X	X	X	X	X	√
	All	X	X	X	X	X	X	X	X	√
McAfee Total Protection Suite	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
McAfee VirusScan Enterprise	Default	X/2	X/ √	X/√	X/√	X/√	X/√	X/√	X/√	√
	All	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Microsoft Forefront Client Security	Default	√	√	√	√	√	√	√	√	√
	All	X	X	1	X	X	X	X	1	√
Microsoft Security Essentials	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	1	√
Nifty Corporation Security 24	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Norman Security Suite	Default	X	√	X	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
PC Tools Internet Security	Default	2	√	√	√	X	√	√	√	√
	All	X	X	√	X	X	X	X	X	X
PC Tools Spyware Doctor with AV	Default	2	√	√	√	X	√	√	√	√
	All	X	X	√	X	X	X	X	X	X
Preventon Antivirus	Default	2	2	2	2	X	2	√	3	√
	All	X	X	2	X	X	X	X	X	X
Qihoo 360 Security	Default	√	√	8	√	√	√	8	√	√
	All	X	X	X	X	X	X	X	X	X
Quick Heal AntiVirus Lite	Default	X/2	X/5	X/5	2/5	X	2/5	X/1	2/5	√
	All	X/2	X	X	X	X	X	X	X	√
Sophos Endpoint Security and Control	Default	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	√
	All	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	√
Sunbelt Vipre	Default	X	X	√	X	X	X	X	X	√
	All	X	X	√	X	X	X	X	X	X
Symantec Endpoint Security	Default	3/ √	3/ √	3/ √	3/ √	3/ √	3/ √	1/5	3/ √	√
	All	X	X	X	X	X	X	X	X	√
Trustport Antivirus	Default	√	√	√	√	√	√	√	√	√
	All	X/ √	X/ √	X/ √	√	X/ √	X/ √	X/ √	1/ √	√
VirusBuster Professional	Default	2	√	√	X	X	√	√	√	X/ √
	All	X	X	X	X	X	X	X	X	X/ √
Webroot AntiVirus with SpySweeper	Default	X	9	5	5	√	√	5	√	√
	All	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

Reactive and Proactive (RAP) detection scores	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1		week +1	
AhnLab V3Net I.S.	62.70%	57.52%	38.65%	52.96%	21.08%	44.99%
Alwil avast! Professional	89.83%	85.13%	76.05%	83.67%	53.53%	76.14%
ArcaBit ArcaVir	58.43%	47.87%	29.32%	45.20%	14.15%	37.44%
Authentium Command Anti-Malware	70.25%	79.29%	61.34%	70.29%	60.62%	67.87%
AVG Internet Security	91.54%	83.45%	82.76%	85.92%	53.80%	77.89%
Avira AntiVir Personal	94.73%	92.97%	79.57%	89.09%	57.57%	81.21%
Avira AntiVir Professional	94.73%	92.97%	79.57%	89.09%	57.57%	81.21%
BitDefender Antivirus	89.92%	87.54%	79.79%	85.75%	60.82%	79.52%
Bullguard	91.05%	88.25%	80.32%	86.54%	61.43%	80.26%
CA Internet Security Suite Plus	55.64%	40.98%	48.20%	48.27%	31.52%	44.09%
CA Threat Manager	51.01%	36.20%	46.17%	44.46%	29.71%	40.77%
eEye Blink Professional	73.91%	70.42%	48.05%	64.13%	48.01%	60.10%
eScan Internet Security Suite	91.46%	89.77%	82.93%	88.05%	63.50%	81.92%
ESET NOD32 Antivirus	89.87%	90.11%	86.07%	88.68%	62.17%	82.05%
Filseclab Twister Anti-TrojanVirus	85.36%	72.26%	68.64%	75.42%	48.96%	68.81%
Fortinet FortiClient	69.94%	56.27%	16.48%	47.56%	11.85%	38.63%
Frisk F-PROT	69.76%	77.52%	57.63%	68.31%	55.80%	65.18%
F-Secure Internet Security	91.09%	88.68%	82.93%	87.57%	63.44%	81.54%
F-Secure PC Protection	91.49%	88.98%	83.24%	87.90%	63.81%	81.88%
G DATA AntiVirus	95.64%	94.91%	87.47%	92.67%	69.02%	86.76%
K7 Total Security	38.50%	55.14%	27.13%	40.26%	34.52%	38.82%

Scanning speeds were pretty slow in some areas, especially over the sets of media and documents which most products fly through. While they did show some signs of improvement on second and subsequent attempts, the rescans still took a long while.



On the other hand, detection rates proved superb pretty much across the board, and with no issues handling the core sets and no false alarms, *Kaspersky* comfortably earns a VB100 for its 2010 edition.

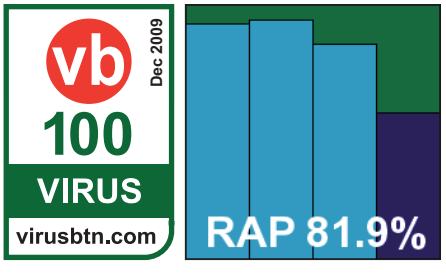
Kaspersky Anti-Virus 6.0 for Windows Workstations 6.0.4.1212

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.06%
Worms & bots	100.00%	**False positives**	0

Kaspersky's second offering this month has a slightly more businesslike name and is presumably a corporate version, but in look and feel it is not so very different from the home-user edition – somewhat plainer perhaps, and with some of the advanced features absent. Again the wealth of configuration options is a pleasure to behold and the user experience is extremely smooth and trouble free. Scanning speeds were much faster this time too, and showed signs of considerable improvement on repeat attempts thanks to the 'iSwift' and 'iChecker' technologies mentioned in the control system.

Reactive and Proactive (RAP) detection scores contd.	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1		week +1	
Kaspersky Anti-Virus 2010	92.62%	94.04%	85.22%	90.63%	61.70%	83.40%
Kaspersky Anti-Virus 6	92.27%	93.77%	84.04%	90.03%	57.32%	81.85%
Kingsoft Anti-Virus 2010 Advanced	44.39%	45.45%	22.25%	37.36%	32.44%	36.13%
Kingsoft Anti-Virus 2010 Standard	15.71%	23.24%	13.08%	17.34%	14.13%	16.54%
Kingsoft Anti-Virus 2010 Swinstar	40.71%	43.21%	29.22%	37.71%	23.21%	34.09%
McAfee Total Protection Suite	78.50%	82.05%	72.17%	77.57%	53.98%	71.67%
McAfee VirusScan Enterprise	70.75%	79.25%	71.13%	73.71%	51.56%	68.17%
Microsoft Forefront Client Security	76.90%	73.57%	64.93%	71.80%	44.27%	64.92%
Microsoft Security Essentials	89.95%	87.61%	74.86%	84.14%	48.82%	75.31%
Nifty Corporation Security 24	91.54%	93.03%	78.45%	87.67%	53.05%	79.02%
Norman Security Suite	73.42%	70.08%	47.66%	63.72%	47.53%	59.67%
PC Tools Internet Security	66.80%	64.88%	61.89%	64.53%	23.61%	54.30%
PC Tools Spyware Doctor with AV	66.80%	64.88%	61.89%	64.53%	23.61%	54.30%
Preventon Antivirus	78.51%	69.13%	48.52%	65.39%	38.36%	58.63%
Qihoo 360 Security	85.67%	84.48%	79.73%	83.29%	58.94%	77.21%
Quick Heal AntiVirus Lite	76.43%	63.43%	52.05%	63.97%	36.26%	57.04%
Sophos Endpoint Security and Control	89.87%	86.30%	84.57%	86.91%	73.21%	83.48%
Sunbelt Vipre	71.31%	65.76%	63.76%	66.94%	42.15%	60.75%
Symantec Endpoint Security	79.67%	84.09%	32.76%	65.51%	17.66%	53.55%
Trustport Antivirus	96.24%	94.67%	89.03%	93.32%	67.43%	86.84%
VirusBuster Professional	78.32%	69.26%	48.09%	65.22%	38.60%	58.57%
Webroot AntiVirus with SpySweeper	89.36%	84.31%	84.19%	85.95%	70.15%	82.00%

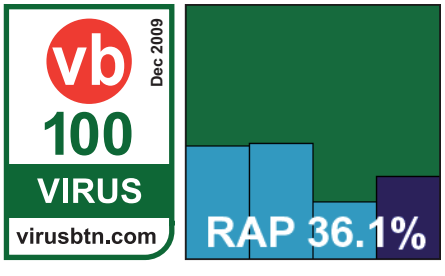
Detection rates were excellent in all sets, and no problems were encountered in the certification requirements, thus earning *Kaspersky* a second VB100 award this month.



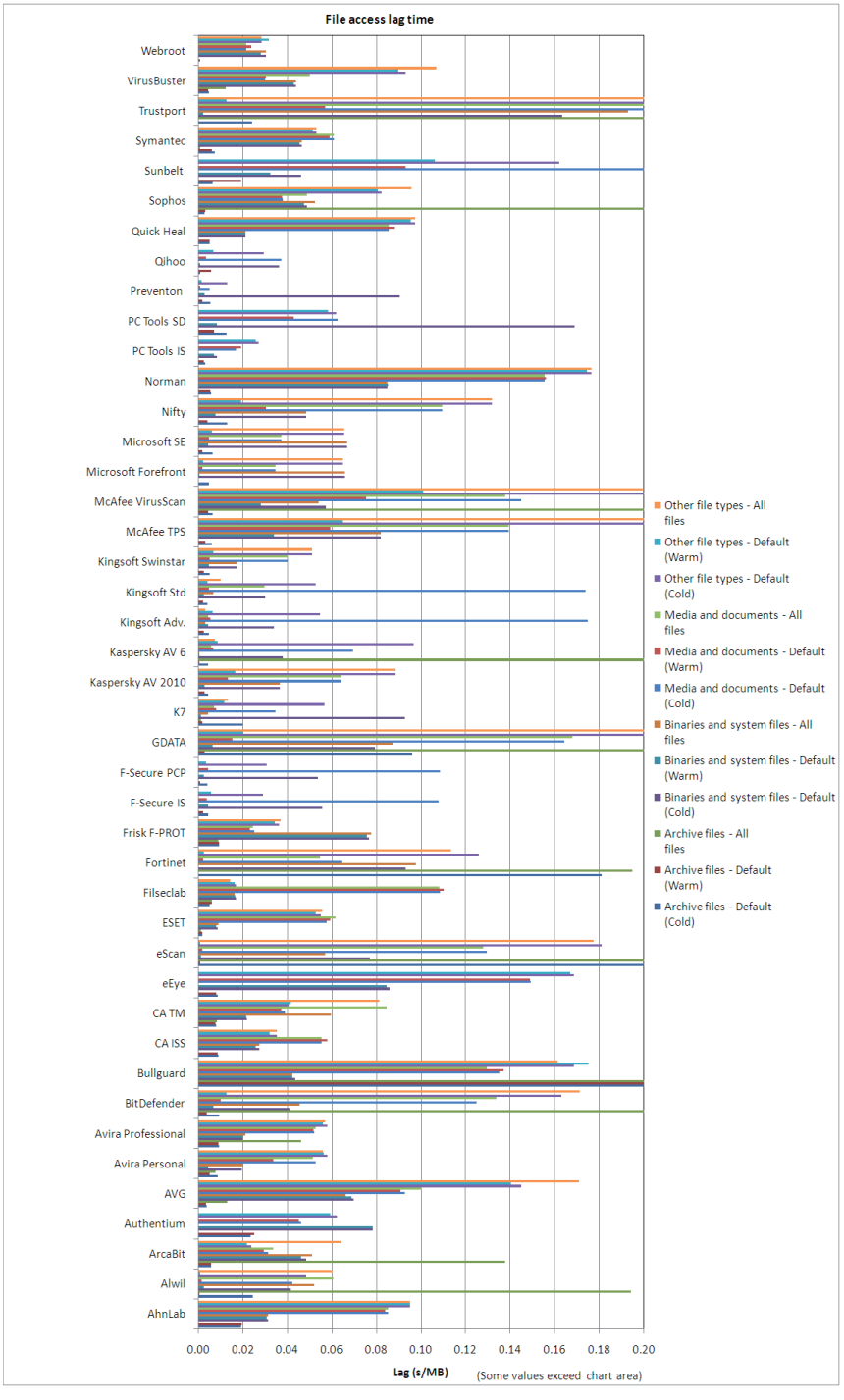
Kingsoft Anti-Virus 2010 Advanced 2008.11.6.63

ItW	100.00%	**Polymorphic**	56.60%
ItW (o/a)	100.00%	**Trojans**	63.19%
Worms & bots	99.95%	**False positives**	0

Kingsoft's Advanced edition has a fairly straightforward installation process: fast and unchallenging with only the mention of cloud-based intelligence worthy of comment; no reboot is required to complete. The interface is simple and unflashy, presenting all the required controls without fuss but occasionally looking a little sparse thanks to the use of some rather odd fonts.



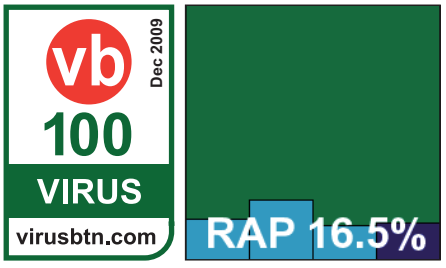
Logging proved sturdy and responsive – something of a rarity for this month's test and certainly worthy of praise. Scanning speeds were middle of the road and detection rates proved rather unpredictable, with problems being



caused by both polymorphic viruses and samples that were less than a few weeks old. No such issues were encountered in the WildList however, despite the Virut strain in there, and with no false alarms generated either, *Kingsoft* earns a VB100 award for its Advanced edition.

Kingsoft Anti-Virus 2010 Standard 2008.11.6.63

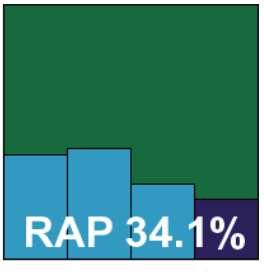
ItW	100.00%	**Polymorphic**	56.60%
ItW (o/a)	100.00%	**Trojans**	18.91%
Worms & bots	99.95%	**False positives**	0



Kingsoft's Standard version is, as usual, identical to the Advanced edition – on the surface at least. In the past we have noted a sizeable speed difference between the two, but this time the two performed much on a par with each other. In terms of detection, however, a fairly major difference was observed, with much lower scores here in the trojans and RAP test sets – once again seeing that rather surprising jump up and down across the RAP weeks – and a similar level of polymorphic misses too. However, with no issues in the WildList and no false alarms, *Kingsoft*'s second entry also makes the required grade for a VB100, which is duly awarded.

Kingsoft Anti-Virus 2010 Swinstar edition 2009.07.30.01

ItW	99.99%	**Polymorphic**	47.98%
ItW (o/a)	99.99%	**Trojans**	53.21%
Worms & bots	99.42%	**False positives**	0

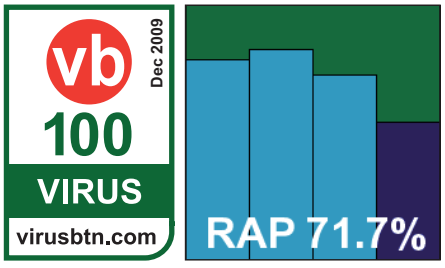


Kingsoft's '*Swinstar*' version is apparently a preview of upcoming technology, and is indeed quite different from its predecessors in many respects, starting with an installer package of not much over half the size of the previous two versions. The install is even faster and simpler, and the interface a little more glitzy and stylish but still fairly simple and easily navigated. More sensible default settings and a greater range of configuration are available. Scanning speeds are also a little better.

Again no false alarms were generated in the clean sets, but in the WildList set a single sample out of several thousand of the W32/Virut strain was missed, thus denying *Kingsoft* the chance of a hat trick this month.

McAfee Total Protection Suite

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



McAfee's home-user product was one of several this month which required Internet access during the set-up phase; in this case, not only do updating and activation take place online but so does the entire installation process. For me this would be entirely unacceptable; the several systems I use for my own purposes are all regularly reimaged to a known-clean state, and wherever possible I scrupulously avoid connecting to the web until security is installed and active (preferably fully updated too). It could, of course, be that I have grown paranoid from long experience in the security industry and exposure to too many scare stories, but such factors seem not to have influenced the designers at *McAfee*.

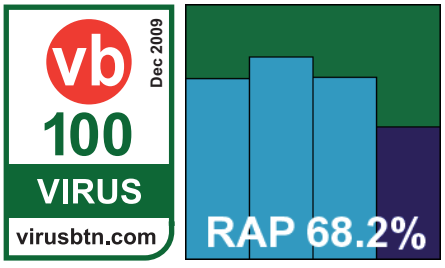
Once the product is installed, after a fairly drawn-out process, it presents a rather drab, grey outlook on the world which the test team found rather depressing. Although well stocked with buttons to click, the product provides virtually no control over its behaviour, merrily skipping through our test sets deleting and disinfecting samples without hesitation or approval. Again this would be less than ideal for my personal needs – fear of false positives and sloppy disinfection of precious files makes many users prefer quarantining and manual checking before any permanent damage is done. Logging also proved an issue, capped at a very small fixed level which cannot apparently be adjusted, so although the product reported having spotted and destroyed numerous files and threats, it could provide no details of what it had done and where.

Scanning speeds were mediocre and showed no signs of improvement over time, but we finally got through the test. Numerous reboots were required as, lacking the ability to disable the protection, we were forced to boot into another operating system to replace destroyed sets. Results were obtained by laboriously checking the files left behind on disk and counting only those left in place unchanged as misses. A satisfactory level of detection was observed, solid across most sets. The WildList presented no difficulties and there were no false alarms, so *McAfee*'s consumer offering is adjudged (just about) worthy of a VB100 award.

McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	85.68%
Worms & bots	100.00%	**False positives**	0

The *VirusScan* product for the corporate market has a much more grown-up attitude to its users, providing a more solid and sensible approach. The installation process is simple and clean, with the offer to disable *Windows Defender* a highlight, and the product itself is similarly businesslike, unflashy and properly thought out.

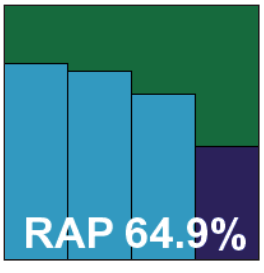


It ran through the tests in good time without problems, showing excellent stability and general good behaviour throughout. In the final verdict it actually scored slightly lower than its wayward consumer sibling in the newer test sets, thanks to the daily offline updater being plucked somewhat earlier than we were able to install, update and snapshot the total product, but scores remained pretty decent. The WildList proved not much of a challenge, and with no false alarms *VirusScan* ably earns itself a VB100 award and much gratitude for a relatively painless experience.

Microsoft Forefront Client Security 1.5.1972.0

ItW	99.29%	**Polymorphic**	99.78%
ItW (o/a)	98.07%	**Trojans**	70.52%
Worms & bots	99.42%	**False positives**	0

The *Forefront* product requires a rather complex install process thanks to our hermetically sealed lab, with multiple reboots to get the various components in place. This non-standard set-up prevents us from properly commenting on the process as would be experienced in the real world. Once up and running however, the product is pleasantly simple to use, the very minimal configuration provided making for light work as no in-depth measurements could be taken.



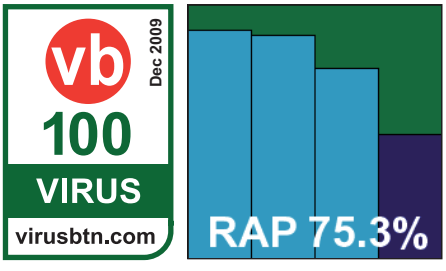
Parsing the results, we saw some pretty decent scanning speeds and fairly lightweight on-access figures, with a very noticeable increase in speed once files had been initially processed and remembered. Detection scores were a little less pleasing though, with levels much lower than expected in most areas. Thinking at first some error had been made when applying updates, the tests were re-run but the same results were obtained. On checking the version information displayed, the updates appeared to be from several days prior to the deadline for the test – suggesting that the wrong updates had been included with the submission. With a number of W32/Bagle samples recently added to the WildList not detected, *Forefront* is regretfully ruled out of contention for a VB100 award this month.

SEE UPDATE p.43

Microsoft Security Essentials 1.0.1611.0

ItW	100.00%	**Polymorphic**	99.92%
ItW (o/a)	100.00%	**Trojans**	91.16%
Worms & bots	100.00%	**False positives**	0

Microsoft's new, free home-user solution was reviewed in these pages just last month (see *VB*, November 2009, p.18), so its layout and usage provided no surprises. The design is simple but perfectly workable, with enough options and sensible default behaviour to satisfy our requirements comfortably. It ran through the test without hindrance or upset, running for what seemed like a rather long time over the infected sets, but which would later prove to be not so bad compared to some others in the field this month. In the proper speed tests, rates were pretty impressive, with some good use of caching to lighten on-access overheads once files had been confirmed safe.



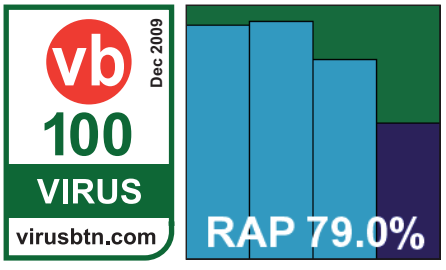
After the problems noted with the corporate product there were some worries about detection rates, but clearly the submission for the *Security Essentials* product had been made more carefully; scores proved very solid indeed, with a very gentle decline across the RAP sets and a fairly sharp drop in the proactive week but remaining highly competitive. False positives being absent, and the WildList handled ably, *Security Essentials* comfortably takes its first VB100 award.

Nifty Corporation Security 24 5.6.0.0

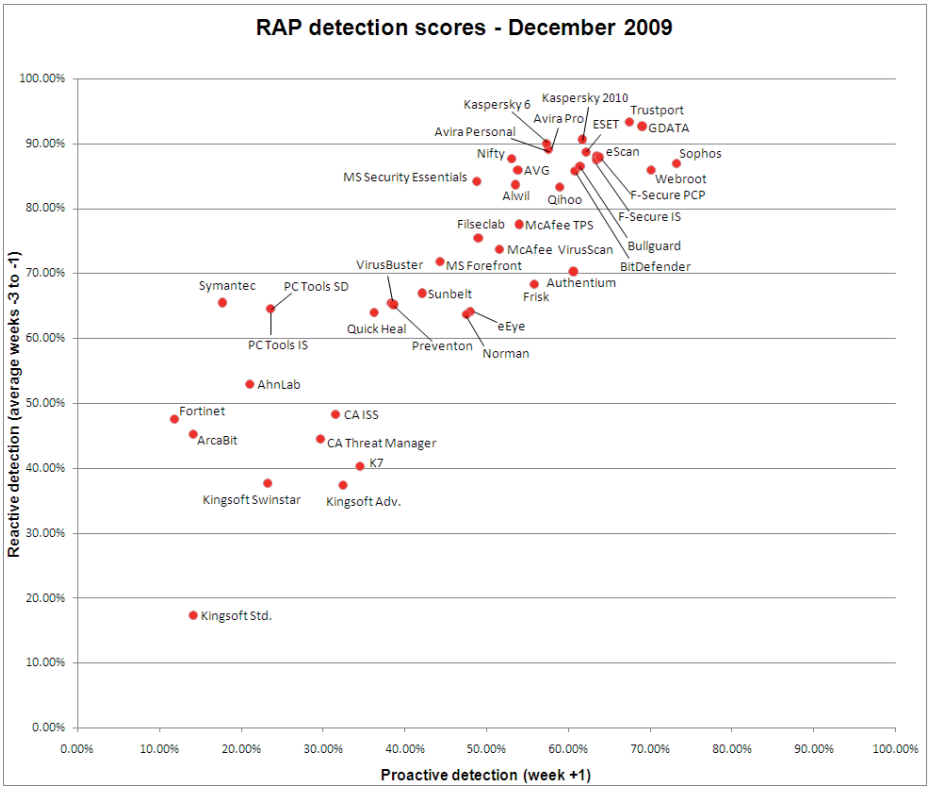
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	87.68%
Worms & bots	98.58%	**False positives**	0

This was *Nifty*'s second appearance in our tests, and once again the product was only available in Japanese. Installation

proved fairly simple – a little slow, but running through the familiar gamut of steps before demanding a reboot. With the GUI still trying to summon some of its display fonts from the operating system (where they were sadly not to be found in our test set-up) navigating proved somewhat difficult, especially since the guides provided by the developers on the previous occasion had been rendered out-of-date by changes to the interface and the operating system alike.

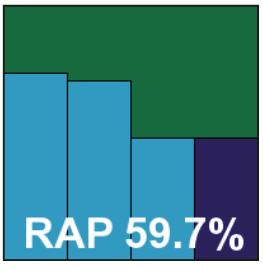


Nevertheless, we bravely soldiered on, eventually obtaining results through various techniques after one of the longest spells spent on a single product in VB100 history. Scores, as expected from the *Kaspersky* engine incorporated into the product, were pretty decent. Speeds were somewhat sluggish on first attempt but, as we had surmised they might be, considerably quicker on repeated scans. Easily satisfying the technical if not aesthetic demands of the VB100, an award is duly earned by the *Nifty Corporation*.



Norman Security Suite 7.3.0

ItW	100.00%	**Polymorphic**	83.35%
ItW (o/a)	99.99%	**Trojans**	74.86%
Worms & bots	100.00%	**False positives**	0



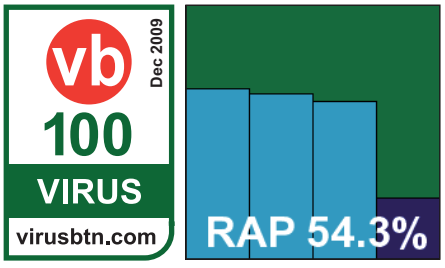
Norman's suite solution has caused a few headaches in the past, and we were most grateful to see a considerably redesigned version submitted this month. The new version, after a very speedy install indeed, proved much more useable, stable and responsive, although the apparent absence of the ability to run a manual scan, either from the GUI or the context menu, set things back a little as well as provoking some bewildered amusement.

Another issue which seemed to defy all logic was the scheduled scan, confidently timed for late on a Friday night so that the bulk of the scanning would be complete by Monday. On arriving back after the weekend, we found the scan had uncovered an item of potentially aggressive commercial software early in the job, and had sat waiting for instructions for two days without continuing its scanning, leaving the vast bulk of the scheduled job still to run.

Having shaken our heads a little at these quirks, we did eventually manage to gather the required data, which showed some solid scores, aided by the sandbox. However, as expected after having seen the results of the *Blink* product, there was a slight failing on access with the Virut samples, although on-demand coverage was better. This was enough to deny *Norman* a VB100 award this month.

PC Tools Internet Security 7.0.0.508

ItW	100.00%
ItW (o/a)	100.00%
Worms & bots	99.95%
Polymorphic	100.00%
Trojans	93.12%
False positives	0



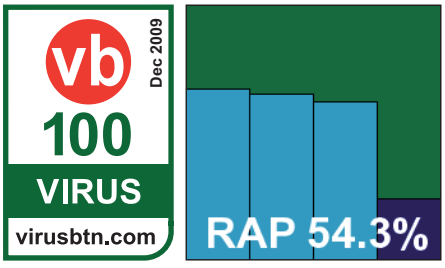
PC Tools' product range has had a pretty shaky time in recent *VB* comparatives – seemingly coinciding with the company having been taken over and the product ceasing to incorporate a third-party engine. Running through the familiar installer, which took rather a long time and needed a reboot to finalize things, we were a little worried that nothing had changed this time, but running through the tests on the top-of-the-range *Internet Security* suite product proved much more satisfactory than on the last few occasions, with no problems with stability or bad behaviour of any kind. The interface, which has become more usable through familiarity and seems pretty much unchanged since the last submission, is fairly appealing and has a decent range of controls, most of which are sensibly located and labelled.

Under the hood though, it is clear that some great strides forward have been taken. Above and beyond the solid stability, detection rates have soared since the rather pitiful efforts of just a few months ago, possibly aided by the experience of the company's new owners, and in the main sets – particularly the trojans – some truly excellent scores were achieved. The RAP sets were also handled fairly well, steady across the reactive weeks and with a steep dip into the proactive set, but overall not bad at all. Scanning speeds were somewhat mediocre, and especially slow handling .JAR archive files, but the WildList was handled impeccably and without false positives *PC Tools* is firmly back in the VB100 award winners' camp.

PC Tools Spyware Doctor with AntiVirus 7.0.0.51

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.12%
Worms & bots	99.95%	**False positives**	0

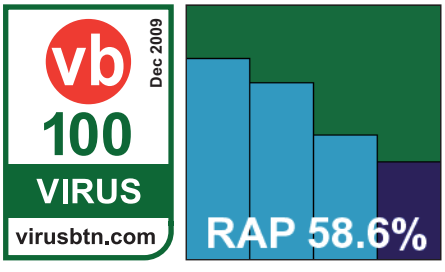
The second *PC Tools* entry this month is essentially the same as the suite product minus a few of the extras, and has the same fairly slow installation process, punctuated this time by the offer of a *Google* toolbar. The product also presents a very similar-looking interface. This time, however, all was not so well, with the first install seeming to have a partially functioning on-access component. While malicious code was detected on execution, the on-read and on-write protection boasted of in the interface appeared to be completely absent, despite numerous restarts and adjustments of the settings. Finally, however, the right combination of clicks managed to get it up and running, and on a second install on fresh hardware it seemed happier to start of its own accord.



Scanning thus proceeded without further interruption, with the same excellent detection rates as the *IS* product, and also the same fairly slow scanning times. The core requirements of the VB100 were easily satisfied, and a second award is thus earned by *PC Tools*, along with some compliments on the developers' sterling efforts at improving the product.

Preventon Antivirus 1.0.28

ItW	100.00%	**Polymorphic**	89.10%
ItW (o/a)	100.00%	**Trojans**	79.31%
Worms & bots	100.00%	**False positives**	0



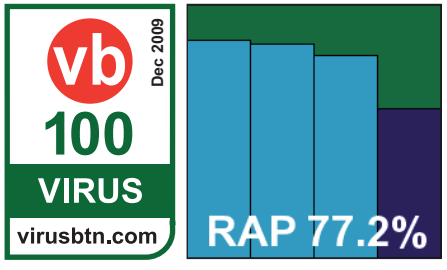
A newcomer to this month's comparative, *Preventon* provides its own version of a third-party engine which appears generally to be sold via ISPs and other rebranding sales channels. Our first impressions were good, with a nice, simple install process, and a well-designed GUI aiming firmly for the simple end of the market. The simplicity did nothing to impair performance or usability however, with a sensible set of defaults and a sprinkling of useful controls that were easy to find in the bright, colourful interface. One issue that did perplex us was the pair of arrow buttons provided, which we assumed would move us left and right through the tabs but seemed not to; we eventually divined that they were actually browser-style forward and back buttons rather than simple left and right.

This minor moment of confusion aside, a few problems with auto-quarantining – which slowed things down considerably in the larger infected sets – and limited

logging were easily overcome with some advice from the vendor and a little care in running jobs, and results were easily acquired. Scanning speeds were fairly decent, and detection rates pretty solid, with a fair-sized decline in the more recent weeks of the RAP sets. Without false alarms and with complete coverage of the WildList, *Preventon* is a worthy winner of a VB100 award on its first attempt.

Qihoo 360 Security 1.0.0.1068

ItW	100.0%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.47%
Worms & bots	100.00%	**False positives**	0



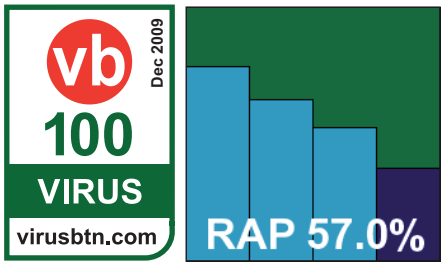
A second newcomer to this month's test, and like the previous entrant *Qihoo* was a surprise last-minute appearance with a third-party engine (*BitDefender* in this case). *Qihoo* hails from China and, this being a fairly new product, the company has yet to translate its product interface into other languages. Aided by a thorough guidebook and a little inspired guesswork, the team found the install fast and simple and the interface clearly and rationally designed, allowing some options to be discovered simply through logic without recourse to understanding the markings.

Scanning speeds were no more than mid-range but detection rates, as demonstrated by other incarnations of the same engine, were splendid, with solid scores across the sets. The WildList and clean sets proved little problem bar a handful of files marked merely as 'suspicious', and *Qihoo* also makes the VB100 grade at first attempt.

Quick Heal AntiVirus Lite 2009 10.0

ItW	100.00%	**Polymorphic**	98.97%
ItW (o/a)	100.00%	**Trojans**	80.54%
Worms & bots	100.00%	**False positives**	0

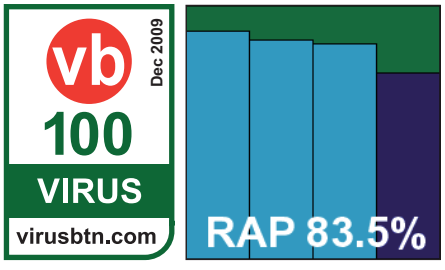
Quick Heal's product offers a pre-installation scan along with the usual set of steps, but is still in place in excellent time. The design is bright and eye-catching, the layout reasonably rational and not too tricky to find one's way around, and a fair level of controls is provided for most needs, so testing proceeded apace.



Speeds were not as rapid as we have come to expect from the product in the past, but still perfectly decent, and detection rates were fairly decent too, with a steady decline observed across the RAP sets. The WildList and clean sets were handled well, so *Quick Heal* also wins a VB100 award this month.

Sophos Endpoint Security and Control 9.0.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	87.62%
Worms & bots	100.00%	**False positives**	0



With the latest edition of this product *Sophos* again introduces some additional functionality without noticeably affecting the user experience. In this case we understand that encryption features have been merged into the company's corporate offerings, but after another fairly lengthy install process the interface seemed unchanged, at least at a cursory glance.

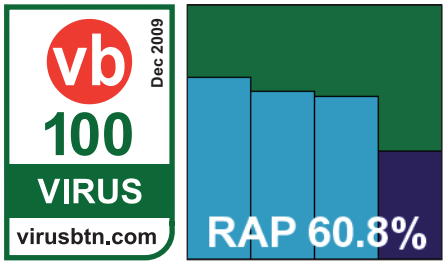
The GUI is simple and logical and presents an excellent range of options, as demanded by the product's business audience – although some items, such as always scanning memory and boot sectors when running a manual scan, are tucked away in a super-advanced section alongside other controls of a far more technical nature. We noted a few quirks in the layout which had the potential to confuse, such as the separation of scan settings into two areas, and also spotted some disagreement in data presented when opening the scan interface part-way into a running scan. While the newly opened scan window reported one set of figures, these seemed only to measure activity from the point at which the window was opened. Meanwhile, the display in the main interface offered a different set of statistics for the same scan.

These minor quibbles aside, scanning speeds proved pretty decent and detection rates solid. Detection rates were

particularly good in the RAP sets where some excellent figures were noted, especially in the proactive set; we observed enormous numbers of detections being covered by a relatively tiny number of unique identities, so it seems like *Sophos*'s focus on generic coverage is paying dividends. With no problems in the WildList and no false positives, *Sophos* earns another VB100 award after a minor upset last time around.

Sunbelt Vipre 3.1.2842

ItW	100.00%	**Polymorphic**	65.24%
ItW (o/a)	100.00%	**Trojans**	66.43%
Worms & bots	99.84%	**False positives**	0



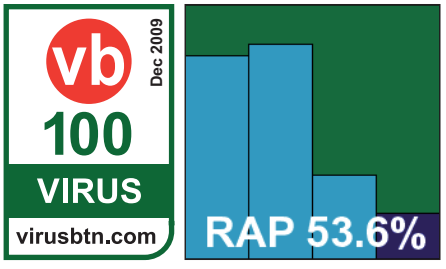
Perhaps one of the most long-anticipated VB100 appearances, *Sunbelt*'s *Vipre* has been around for a few years now. The product was featured in a standalone review in these pages last summer (see *VB*, July 2008, p.16), and has been building a strong reputation for itself despite little participation in the standard tests. For some time we have been getting regular enquiries from our readers as to why *Vipre* has yet to appear in the VB100, and it is with great excitement that we finally get to record and report some results. Given the company's marketing of the product as lightweight and easy on resources, we were particularly interested in its performance figures.

The installation process runs along fairly typical lines, at a rapid pace, but requires a reboot to complete. The interface is fairly clean and attractive and provides a reasonable range of configuration options, although we could not find a way to protect against more than the default set of file extensions on access – or indeed, to delve into archives on demand.

Stability proved solid though, and speeds were pretty decent too, with an impressive improvement on access once files had become known to the product. Detection rates were not bad either, with a few issues in the polymorphic set mostly explained by rare and obscure items not covered at all, and scores in the trojans and RAP set fitting into the better end of the middle of the field. The WildList proved no obstacle despite the set of tricky Virut samples, and with no false positives either *Vipre* earns a VB100 on its first appearance; we hope to see many more.

Symantec Endpoint Security 11.0.5002.333

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	92.29%
Worms & bots	100.00%	**False positives**	0



Unlike many of its competitors, *Symantec* continues to enter only its corporate product for most of our comparative reviews – although we do hope to see some more regular appearances from the ubiquitous *Norton* consumer solutions in future.

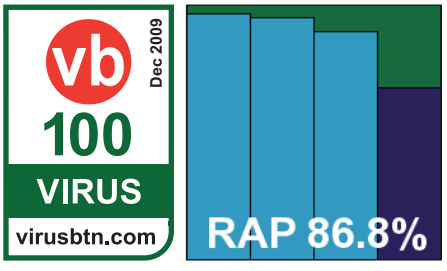
The corporate product is a little less sober and businesslike than it used to be. After a fairly unflashy, somewhat slow install which requires a reboot to complete, a curvy and colourful interface appears, with a fairly simple layout. Some in-depth configuration is provided in more serious-looking 'advanced' areas – although some administrators may wish for a little more depth. In places options need to be set multiple times for minor variations on the same theme, making the process of setting up an on-demand scan something of a chore.

We've noted before that scanning infected items can be rather slow with this product – something which may be due to the intensive logging that is carried out as scanning proceeds. Where many other products this month have frustrated us by limiting their logs to unusably small sizes, *Symantec* has gone the other way and provided almost 2GB of information for us to plough through. On one occasion we had a more serious issue with the logging system, when a scan seemed to get snagged somehow, spending more than 30 minutes on a single file. Rebooting the system seemed to clear the jam, but the product insisted that the scan was still running, and thereafter refused to add any information about more recent jobs to the history display system.

These were fairly obscure issues of course, that are unlikely to be encountered in real-world day-to-day use, and in the core data all seemed to be fine. Scanning speeds were pretty good, and on-access overheads excellent, while detection scores were splendid up until a fairly steep decline in the latest weeks of the RAP sets. No problems were encountered in the WildList or clean sets however, and *Symantec* duly earns another VB100 award.

Trustport Antivirus 2020.5.0.0.4064

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.04%
Worms & bots	100.00%	**False positives**	0

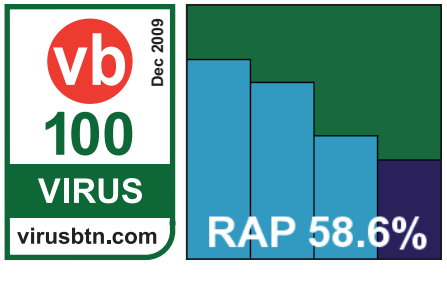


Trustport's installer follows the standard paths, with a few sidetracks for some set-up of the multi-engine system, and does so at a fair speed, finishing with a reboot. The multi-GUI control system is not best suited to UAC-affected systems, as numerous prompts for confirmation must be endured to access the various components, and again some problems were observed opening browser windows for on-demand scans, which could take an excessively long time. We also noted the system was quite clearly slower to come to life on reboot, and after a number of on-access detections there seemed to be some oddity with pop-ups, which kept reappearing at regular intervals long after they had been observed and acknowledged, even after the system was rebooted.

Scanning speeds were fairly sluggish, but in some areas did show some improvement the second time over the same files on access. On the positive side, detection rates were outstanding as usual, with the highest scores overall this month in the trojans set and no issues at all elsewhere. With the core requirements easily met, *Trustport* comfortably earns a VB100 award.

VirusBuster Professional 6.2.30

ItW	100.00%	**Polymorphic**	89.10%
ItW (o/a)	100.00%	**Trojans**	78.34%
Worms & bots	100.00%	**False positives**	0

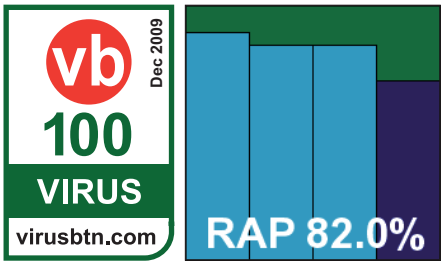


VirusBuster's installation is fast and easy, although the interface when it comes up looks increasingly elderly and in need of updating. The design is somewhat clunky and unintuitive, with on-demand scans requiring repeated recourse to advanced tabs, which must be called up separately in each of the numerous stages. There are also a few snags and glitches in the display, with lines and text boxes overlapping and poorly laid out on screen.

Otherwise everything proved pretty plain sailing, with some fairly decent scanning speeds and reasonable detection rates too, declining steadily into the final portions of the RAP sets. The WildList and clean sets presented no difficulties, and a VB100 award is duly earned.

Webroot AntiVirus with SpySweeper 6.0.1.143

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.48%
Worms & bots	97.00%	**False positives**	0



The final entry on this month's monster roster of products, *Webroot*'s installation process kicks off with a very busy page covering registration code, EULA, install options and the offer of a (free!) *Ask* toolbar, all at once. The install process is then fairly brisk until a reboot is demanded, and some post-install set-up of community scheme participation is also required.

The product itself is slowly revealing its mysteries thanks to long exposure, but remains something of a challenge to navigate and control properly, with custom on-demand scans a particularly arduous chore. GUI buttons can take a huge amount of time to respond, particularly at the end of a scan when it sometimes feels like it would be quicker to allow the product to destroy our test sets than to wait for the 'deselect all' and 'quarantine selected' to respond – even with little or nothing selected. Logging is also severely restricted, although a custom fix from the developers provided us with a way around this. On-access scanning appears not to function on-read by default, with an option to enable it buried deep in the elaborate configuration structure. In most cases scores were divined by a mixture of logging and checking copied test sets for files either not written or allowed to write only after disinfection.

In the end, scanning speeds were fairly good. On-access overheads were heavier than expected, but detection rates

pretty decent, as one would expect from the *Sophos* engine that underlies the product. The WildList proved no major challenge, and with no false positives either *Webroot* also takes away a VB100 award.

CONCLUSIONS

Crawling exhausted from the lab after our biggest month of testing ever, with a mind-numbing 43 products crammed into a mere three weeks of testing, we found it surprisingly difficult to draw any specific conclusions from such a large and varied set of data. As usual there were some excellent performances and some disappointments, some high scorers and some fast speeds counterbalanced by some at the other ends of both scales.

Generally we found *Windows 7* a fairly amenable platform, afflicted by a number of fairly basic bugs which will hopefully be ironed out in the first service pack (which surely cannot be long in coming). Our poor test hardware, battered from some seriously heavy usage, began to show signs of wear, with some of the more heavyweight products causing one system in particular to overheat regularly. The range of products under test had few specific issues running on the new operating system, although a few had some problems getting installed and for many some more thought is needed as to how to interact with the UAC system less intrusively.

In terms of passes and fails, this has been a good month for most products, with a fairly small number of false positives – perhaps thanks in part to the tightening of our own rules concerning what is considered 'fair game' for the clean sets. The WildList, despite more rapid changes in its makeup, presented few major challenges, but continues to be a good gauge of which products are consistently up to the mark. Some further improvements to the complexity of the list are expected soon, which should make it a much more complete and challenging measure. We had a number of new faces in the test this month, several of whom will be able to present themselves to their customers with certain proof of their bona fides – a valuable thing in these days of rogue products flooding the Internet with their deceitful claims.

What issues were observed with products mainly confined themselves to frustrations and irritations rather than outright show-stoppers. Curious and inexplicable time lags were frequent, especially when trying to browse local filesystems, and many of the interfaces proved far less responsive than most users will accept. With a mix of corporate and consumer products being tested, we saw some vast differences in the approach to user interaction, with many at the home-user end trying to take responsibility and control away from the user entirely – an approach which seems to limit their market somewhat to only the least engaged audiences.

One of the biggest issues we had this month was with logging, with problems arising both from the lack of complete data and data being obscured and/or encrypted. Some products which store their data in proprietary formats and rely on parsing and processing raw data into humanly readable forms can easily get overwhelmed by logs over a certain size. Meanwhile, others seem to think it acceptable to simply destroy any data once a certain size threshold has been reached; if software has been doing things to my computer, I want it to be able to tell me about it and account for its activities, whether or not it has been busy doing other things since. Aside from this worry, it renders testing rather difficult, and we may have to impose some stricter requirements on logging provision for future comparatives.

Something else which will have to wait is the introduction of our additional performance measures. A vast horde of data was gathered during this month's test, but as deadlines closed in on us and the slower, more recalcitrant products took longer and longer to provide usable data, we had to make a decision to put off the lengthy job of processing and interpreting all this information for presentation to our readers. Hopefully we will be able to make it available soon, and having gone through the process of preparation we should be able to include it regularly in comparatives from now on.

Looking to the future, the next test will be our annual excursion on *Linux* – surely a blessing for our tired eyes and weary fingers thanks to the less well-populated field of potential competitors. After that we will be back up to full speed for another *XP* comparative, and what looks likely to be another challenge to this month's record-breaking haul of submissions. We can only hope that on a more seasoned and familiar platform, and with some points taken on board from this month's comments, products will be better behaved and easier to push through our ever-growing range of tests.

Technical details

All products were tested on identical systems with *AMD Athlon64 X2* Dual Core 5200+ processors, 2 GB RAM, dual 80GB and 400GB hard drives, running *Microsoft Windows7 Professional, 32-bit edition.*

Any developers interested in submitting products for VB100 testing 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.

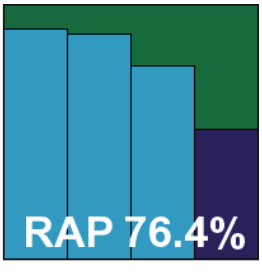
VB100 ON WINDOWS 7: UPDATE

Following the mammoth VB100 comparative, the *VB* lab conducted thorough reviews of the results in collaboration with the product developers. Having performed checks and re-tests on several products, it was found that two products were incorrectly reported as having had problems.

Virus Bulletin extends its apologies to the companies concerned. As always *VB* continues to strive for excellence in its testing and makes every effort to correct any inaccurate data as rapidly as possible.

Microsoft Forefront Client Security 1.5.1972.0

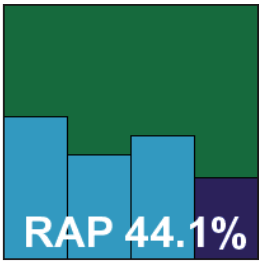
ItW	100.00%	**Polymorphic**	99.78%
ItW (o/a)	100.00%	**Trojans**	91.70%
Worms & bots	100.00%	**False positives**	0



After close analysis, it was discovered that *Microsoft*'s corporate solution, *Microsoft Forefront Client Security*, had not been run with the default settings, as per the standard procedures of the VB100. When tests were re-run using the correct settings the product was found to be capable of detecting all the samples in the WildList test set, and a VB100 award is thus awarded to the product retrospectively. The product's detection scores in the trojan and RAP sets also increased after the adjustment to the settings.

CA Internet Security Suite Plus 2010

ItW	99.70%	**Polymorphic**	92.05%
ItW (o/a)	99.70%	**Trojans**	43.84%
Worms & bots	100.00%	**False positives**	0



Further analysis was also carried out of the false positive alerted on by *CA*'s consumer product *CA Internet Security Suite Plus 2010*. It was found that, while the false positive existed in the installer submitted by the company, it was not present in the updated definition set that was also included in the submission. As users would be updated to the fixed protection level prior to running any scans, the issue should not emerge in the real world. The product's problems with the WildList were confirmed however, so *CA*'s *Internet Security Suite Plus* is still denied a VB100 award in this test.

A full set of revised results tables and an updated RAP chart can be found at http://www.virusbtn.com/virusbulletin/archive/2009/12/vb200912-comparative.

END NOTES & NEWS

ACSAC 2009 takes place 7–11 December 2009 in Honolulu, Hawaii. For details see http://www.acsac.org/.

The 26th Chaos Communication Congress (26C3) takes place 27–30 December 2009 in Berlin, Germany. The Congress offers lectures and workshops on a multitude of topics and attracts a diverse audience of hackers, scientists, artists and utopians from around the world. For more information see http://events.ccc.de/congress/2009/.

Black Hat DC 2010 will be held 31 January to 3 February 2010 in Arlington, VA, USA. Online registration is now open. For details see http://www.blackhat.com/.

RSA Conference 2010 will be held 1–5 March 2010 in San Francisco, CA, USA. Early bird registration rates apply until 5 December 2009. For details see http://www.rsaconference.com/.

The 11th annual CanSecWest conference will be held 22–26 March 2010 in Vancouver, Canada. For more details see http://cansecwest.com/.

The MIT Spam Conference 2010 is scheduled to take place 25–26 March 2010. Venue announcements, and other details will be announced in due course at http://projects.csail.mit.edu/spamconf/.

Black Hat Europe 2010 takes place 12–15 April 2010 in Barcelona, Spain. A call for papers will open in January. See http://www.blackhat.com/.

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

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

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

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

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

CARO 2010, the 4th International CARO workshop will take place 26–27 May 2010 in Helsinki, Finland. For more information see http://www.caro2010.org/.

The 22nd Annual FIRST Conference on Computer Security Incident Handling takes place 13–18 June 2010 in Miami, FL, USA. The conference promotes worldwide coordination and cooperation among Computer Security Incident Response Teams. For more details see http://conference.first.org/.

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/.

VB2010 will take place 29 September to 1 October 2010 in Vancouver, Canada. *VB* is currently seeking submissions from those wishing to present papers at the conference. Full details of the call for papers are available at http://www.virusbtn.com/conference/vb2010/. For details of sponsorship opportunities and any other queries relating to VB2010, please contact conference@virusbtn.com.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

- Single user: $175
- Corporate (turnover < $10 million): $500
- Corporate (turnover < $100 million): $1,000
- Corporate (turnover > $100 million): $2,000
- *Bona fide* charities and educational institutions: $175
- Public libraries and government organizations: $500

Corporate rates include a licence for intranet publication.

See http://www.virusbtn.com/virusbulletin/subscriptions/ for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:
Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com Web: http://www.virusbtn.com/