AUGUST 2009

virus BULLETIN

Fighting malware and spam

CONTENTS

ISSN 1749-7027

IN THIS ISSUE

THOSE WERE THE DAYS

'I hate FUD as much as the next guy, but it did serve a purpose.' Per Hellqvist highlights the positives of the days of sensationalist media headlines.
page 2

HASH BROWNS

Peter Ferrie details a virus that, while not ground-breaking, is a good lesson in being wary of received wisdom.
page 4

LIAR, LIAR

Alisa Shevchenko and Dmitry Oleksiuk introduce a new method for retrieving information from a possibly compromised system.
page 6

CLUSTER ANALYSIS

Robert Sandilands describes a clustering technique aimed at helping in the daily efforts of analysing large numbers of samples.
page 9

VB100

John Hawes presents the results of the latest VB100 comparative review of anti-malware products on Windows Vista Business Edition SP2.
page 14

'I hate FUD just as much as the next guy, but it did serve a purpose. People were more aware... The sensational headlines kept up interest.'

Per Hellqvist, Symantec

WHY IS SECURITY (STILL) A UTOPIA?

Sometimes I wonder if the 'good ol' days' weren't just that – good old days. Worms and virus outbreaks were hitting us almost daily. The media used attention-grabbing headlines to broadcast stories about viruses infecting computers around the world. The cynics accused us of fear mongering and of selling our software using FUD (fear, uncertainty and doubt). It seems a little strange to say this, but the craziness actually served a purpose. While ordinary people were reading and hearing about malware on a daily basis, they were also thinking about it. People were talking about security, and interest grew. Computers were patched, attachments remained unopened and love letters unanswered. 'Anti-This' and 'Anti-That' were invented, firewalls separated the inside from the outside and I used a Hydra in a presentation to illustrate the danger of the multi-faceted threats of Nimda.

In a way, that was how we wanted it to be. I have been in the security industry since the mid-1990s and I have been working hard around the clock to keep security at the forefront of people's minds here in the cold north. I average around 150 presentations a year and am interviewed in the media every other day (that might not sound like much to many of you, but keep in mind that I mainly cover Sweden). Security is still a hot topic up here, but it's not talked about as much as in the good old days.

Now, don't get me wrong – I hate FUD just as much as the next guy, but it did serve a purpose. People were more aware. Today, the bad guys use rootkits to hide inside the computer, infect us using drive-by downloads and have removed all the fancy bling, making my job much harder. Often, the bad guys' rationale is to steal your money and then use your computer invisibly to attack some other victim somewhere else on the Internet. How do we warn users about invisible dangers? How do we warn about the many dangers that, in reality, won't bother users in their daily activities (unless their ISP cuts their access)? How can we motivate users to pay for protection against something that will attack someone *else* – albeit via their computer? How do we persuade them to pay for invisible protection against invisible threats?

The sensational headlines kept up interest. The less you read or hear about something, the less you think about it. As far as computer security is concerned, the more time that has passed since a user last read or heard about something scary, the likelier it is that he will click the next 'interesting' thing in his mailbox.

Today's situation only serves the bad guys – and statistics prove it. Look at the number of detections for new items of malware being added to your favourite AV every day. Look at the number of 'SQL'd' websites serving malware. Look at IC3.gov and read about the amount of money stolen from Internet users every year (spoiler: in 2008 it was $264.59 million in the US alone). The bad guys celebrate Christmas every day.

So, why won't we ever be secure? Vulnerabilities and techie stuff aside, Occam's razor has the answer: many people don't care and don't *want* to care. Kids I've spoken to at Dreamhack (the world's largest computer game festival, held here in Sweden) don't seem bothered if they are infected as long as it doesn't interrupt their gaming experience. They reinstall *Windows* and then it's game-on again. Older folk generally tend to take infection as a personal insult and find malware scary. Users in-between find it a nuisance and try to avoid it, but don't always know how to, and frankly they don't really care all that much – just as long as they can read their email, pay their bills and browse the web.

So, what do we do? We work even harder to make security software as tough as we can make it and invisible at the same time. People don't want to care about malware, and they shouldn't have to. That is our job.

NEWS

MAAWG TAKES STEPS TO TACKLE BOTS

MAAWG, the Messaging Anti-Abuse Working Group, has issued a new set of guidelines for the global ISP industry which it hopes will help the industry work more closely with consumers to tackle the growing problem of bot infections.

The best practices document outlines a three-step approach which suggests ways in which bots can be detected on end-users' machines (discussing various tools that can be used to detect infections while protecting users' privacy), effective ways in which users can be notified that their machine has been compromised, and ways in which ISPs can help guide their customers in the removal of the malware.

A survey released by MAAWG last month indicated that while close to 80 per cent of consumers are aware of bots, only 20 per cent believe their machines will become infected – highlighting a continuing need for user-education and for steps such as these that get the industry working with its end-users to help mitigate the problem.

APPLE PATCHES IPHONE

Apple has released a patch for a critical SMS vulnerability in its *iPhone* following a description of the vulnerability and demonstration of a possible attack by researchers at the Black Hat security conference. *Apple* was first notified of the problem – which consists of a memory corruption issue in the decoding of SMS messages – in June. The vulnerability left *iPhone* users open to attack via receipt of a maliciously crafted SMS message which could lead to an unexpected service interruption or arbitrary code execution.

Details of the patch are provided on *Apple*'s support site (http://support.apple.com/kb/HT3754). At the VB2009 conference next month, Jason Matasano will discuss the risks and benefits of using the *iPhone* in a corporate environment, including examples of the potential malware implications (see http://www.virusbtn.com/conference/vb2009/programme for details).

MCAFEE BUYS MX LOGIC

McAfee announced at the end of last month that it is set to acquire email filtering, archiving and continuity services firm *MX Logic* in a bid to boost its software as a service (SaaS) offerings. *McAfee* will pay $140m in cash for the company, followed by a further $30m if certain performance targets are met. News of the acquisition comes just a couple of months after *McAfee* acquired whitelisting firm *Solidcore*. The acquisition is expected to complete in the third quarter of 2009.

Prevalence Table – June 2009

Malware	Type	%
Waledac	Worm	22.19%
OnlineGames	Trojan	13.76%
FakeAV	Trojan	12.13%
Zbot	Trojan	11.82%
Agent	Trojan	9.10%
Virut	Virus	5.93%
Suspect packers	Misc	3.92%
NetSky	Worm	3.32%
Mytob	Worm	2.56%
Downloader-misc	Trojan	1.82%
Fraudload	Trojan	1.72%
Invoice	Trojan	1.46%
VB	Worm	0.98%
Mydoom	Worm	0.97%
Encrypted/Obfuscated	Misc	0.74%
Dropper-misc	Trojan	0.72%
Zlob/Tibs	Trojan	0.66%
Bredolab	Trojan	0.65%
Basine	Trojan	0.59%
Iframe	Exploit	0.56%
Bagle	Worm	0.42%
Small	Trojan	0.40%
Alman	Worm	0.36%
Lineage/Magania	Trojan	0.34%
Delf	Trojan	0.29%
Fujacks	Worm	0.24%
Murlo	Trojan	0.23%
Marker	Macro	0.18%
Inject	Trojan	0.16%
Sality	Virus	0.15%
Mywife/Nyxem	Worm	0.15%
Grum	Worm	0.14%
Brontok/Rontokbro	Worm	0.12%
Others[1]		1.22%
Total		100.00%

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

MALWARE ANALYSIS

MAKING A HASH OF THINGS

Peter Ferrie
Microsoft, USA

File format tricks abound in ELF files. One of these was described in last month's issue of *Virus Bulletin* (see *VB*, July 2009, p.4). In that trick, a particular section of the file was overwritten by virus code. A variation of that technique is described here.

MISPLACED TRUST

In contrast to the 'Caveat' virus, which overwrites the '.note.ABI-tag' section of ELF files, the 'Hasher' virus (so-named by its author) is interested in the '.hash' section. The virus begins by searching for files within the current directory. When a file is found, the virus attempts to open and map it. If the mapping process fails, the virus closes the file without attempting to unmap anything.

However, the virus is very trusting of the contents of the file. The first three variants of the virus all assume that the file is in ELF format without verifying this fact. A field inside the supposed ELF header is used, without checking that the file is large enough to support the field's presence. A sufficiently small file will cause the code to crash. A truncated ELF file, or a file with a sufficiently large value in the e_shnum field, among other things, will also cause the virus to crash, since the code contains no bounds checking of any kind. The .D variant of the virus requires that a file is at least 1,024 bytes long, but this is insufficient to avoid crashes when pointers reach outside of the file.

THE MAKER'S MARK

The virus is interested in ELF files for the *Intel* x86-based CPU. At this point the .C and .D variants of the virus check whether the file is infected already, while the .A and .B variants perform this check later. The infection marker for the .C and .D variants is the last byte of the e_ident field being set to 1. This has the effect of inoculating the file against a number of other viruses, since a marker in this location is quite common. The .C and .D variants set this value in the file immediately. This has the effect of preventing the files from being examined again, in case an error occurs while infecting them. In addition, the .D variant requires that the ABI is either for *Linux* or is not specified.

For each such file that is found, the virus searches within the Section Header Table entries for the SHT_HASH entry. If the SHT_HASH entry is found, then with the exception of the .D variant, the virus checks if the section is large enough to hold the virus body. The file cannot be infected by any of the first three variants if the section is too small.

HASH COOKIES

At this point, the .A and .B variants check if the file is infected already. The infection marker for the .A variant is the number of hash buckets being set to one. This is a legal value, but it effectively disables the hashing mechanism. The infection marker for the .B variant is the first byte in the hash section being a 'push' instruction.

The hash table exists to improve the performance of locating symbols. Instead of searching linearly through the symbol table, the hash table allows the searching to be achieved using perhaps only a few comparisons. The hash table consists of an array of buckets, which is a collection of pointers whose number ideally corresponds to the number of unique hashes in the symbol table. However, the number can be made arbitrarily smaller than that, which saves space.

To find a symbol, its hash value is calculated (the hashing algorithm is published in the file format specification), and the bucket is indexed by using the hash value modulo the number of buckets. A bucket is simply a starting point for searching within a particular chain. The number of chains corresponds exactly to the number of symbols in the file. If either a bucket entry or a chain entry of zero is encountered, then the symbol does not exist in the file. In the most extreme case, the number of buckets can be set to one, in which case the entire chain might be searched for a match, as it is for the case where no hash table exists at all.

A HOLE IN THE BUCKET

The .A variant of the virus disables the lookup by setting the number of buckets to one, and the number of chains and the first bucket entry to zero. This corresponds to a single empty bucket, and thus no symbols. The virus code is appended immediately after the end of this new hash table, since the table is no longer usable. As a result of the change, symbol lookup no longer works for an infected file, but the file remains executable as before. The entrypoint of the file is altered to point directly to the virus code.

The .B variant of the virus alters the characteristics of the Section Header Table entry, by replacing the SHT_HASH entry with a SHT_NULL entry. As a result of the change, the hash table seems no longer to exist in the file, and thus the entire table becomes available for the virus. The virus code is placed over the top of the hash table, and the entrypoint of the file is altered to point directly to the virus code.

STASH THE HASH

The .C variant of the virus requires that the size of the .hash section is large enough to hold both the number of chains and the virus body. This would be a rare occurrence, but the virus author included the technique for completeness. If the section is large enough, then the virus reduces the number of buckets by the size of the virus body in dwords. There is a bug in this code, which is that the virus forgets to include room for at least one bucket. The new bucket number is checked against a value that is less than zero, but it should be checked against a value that is less than one. (Interestingly, the virus author included an overview document which describes the technique, and the document included an algorithm written in C which contains the correct check. It seems that the bug was introduced when the virus author ported the algorithm to assembly language.) As a result, the number of buckets can be reduced to zero, in which case a divide-by-zero error will occur when the virus is building the new bucket list. Given that a 'bucket list' is also a list of things to do before the end of one's life, this bug is rather appropriate. If the list is empty, the process dies.

If the list is valid, then the virus erases the existing hash table entirely, and creates a new one in its place. The number of chains remains the same, but the placement of the chains is altered according to the new number of buckets. For each symbol, the hash value is created, and the corresponding bucket entry (the hash value modulo the number of buckets, as described above) is examined. If the entry is empty, then the hash value becomes the bucket value. If the bucket value exists already, then the chain is walked until the end is found, after which the hash value is appended to the chain. Once the bucket list has been created, the virus body is appended to the hash table, and the entrypoint of the file is altered to point directly to the virus code.

KICK THE BUCKET

The .D variant of the virus searches the Section Header Table for the SHT_HASH and SHT_DYNAMIC entries. Both of them must exist in order for the virus to infect the file. The .D variant also requires that there are at least nine buckets in the hash table. The reason for this is because the .D variant intends to reduce the size of the hash table by 32 bytes (which corresponds to eight buckets) and because at least one bucket must exist (as described above). If the hash table contains at least nine buckets, then the .D variant reduces the number of buckets by eight, and then erases and rebuilds the hash table in the same way as for the .C variant. The size of the hash table is then reduced by 32 bytes in the Section Header Table.

Once the hash table modifications have been made, the .D variant of the virus makes further adjustments to the Section Header Table entries. The second and following sections, up to and including the hash table section, have their memory and file offsets increased by 32 bytes. The contents of those sections are also moved down in the file by 32 bytes. An implicit assumption exists here, which is that the section is legally movable. This is not the case for code and data sections, since they might contain direct references to each other which would also need to be adjusted. Thus, if the hash table appears after code or data sections, then the resulting infected file will no longer run.

Next, the .D variant of the virus examines the Program Header Table. Another assumption is made here, which is that the Program Header Table exists. If the Program Header Table does not exist, then the .D variant will crash. If any entry in the Program Header Table corresponds to one of the moved sections, then the .D variant will increase the entry's memory and file offset by 32 bytes. Also, if any entry in the dynamic segment corresponds to one of the moved sections, then the .D variant will increase the entry's memory offset by 32 bytes.

PHaT CODING

After making the appropriate adjustments to the Program Header Table, the .D variant of the virus examines the Program Header Table again. The lowest non-zero virtual address of all of the entries, and the last PT_LOAD entry, is saved for later. If the PT_PHDR entry is seen, then the .D variant increases its memory and file size by 32 bytes. Once all of the Program Header Table entries have been examined, the .D variant of the virus moves all of the sections after the last PT_LOAD entry down in the file by 32 bytes. The .D variant then inserts a new PT_LOAD entry into the newly created gap, whose file offset begins at the current end of the file. The virtual address of the entry is set to two pages below the previously lowest virtual address, taking into account the amount by which the file exceeds a multiple of four kilobytes. Two pages are required for the virus code, because even though the virus code is less than four kilobytes long, the new size of the file might exceed another multiple of four kilobytes, resulting in the virus code extending beyond the boundary of one page. The entrypoint of the file is altered to point directly to the virus code, and then the virus code is appended to the file.

CONCLUSION

The addition of a new section header is an interesting technique, since it has long been thought that files are packed too tightly for space to be found. While not ground breaking in any way, this virus does show that one should be careful about received wisdom.

FEATURE 1

EVERYBODY LIES: REACHING AFTER THE TRUTH WHILE SEARCHING FOR ROOTKITS

Alisa Shevchenko, Dmitry Oleksiuk
eSage Lab, Russia

The main goal of a rootkit hunter (whether a human or a machine) boils down to retrieving information about a possibly compromised system in order to make a judgment about its state of health. But because the main goal of a rootkit is to conceal the real state of the system, the hunter is likely to make many false assumptions, and to constantly strain after the few obscure sources of information which can be considered trustworthy in a possibly compromised system.

To put it another way, choosing the right source of information is the cornerstone of the rootkit detection quest. This is also a challenge with a moving target, because what started out as a good source of information might become a bad source once a few steps of rootkit evolution have taken place.

In this article we will introduce a new method for retrieving information about a possibly compromised system – a technique which we consider to be an easier and safer alternative to existing techniques. First, we will discuss the advantages and limitations of known approaches to gathering system information, which are widely used in anti-virus and anti-rootkit solutions. Next, we will outline the proposed alternative technique, its pros and cons, known ways in which the technique can be defeated, and finally we will make a modest reference to its implementation in a real anti-rootkit utility.

COMMON WAYS TO REACH THE TRUTH

Existing anti-virus and anti-rootkit solutions implement various approaches to rootkit detection, such as matching system information obtained from different sources ('cross-view') and checking the integrity of code/structures, either by comparing them to a trusted model or by searching for generic anomalies.

Regardless of the approach taken, the options available for the retrieval of valid information about the current state of the system are quite limited. In fact, there exist two mechanisms that allow possibly subverted system structures to be avoided:

1. Prior to gathering system information, kernel code is restored system-wide (global unhooking) in locations that are suspected of having been modified by a rootkit.

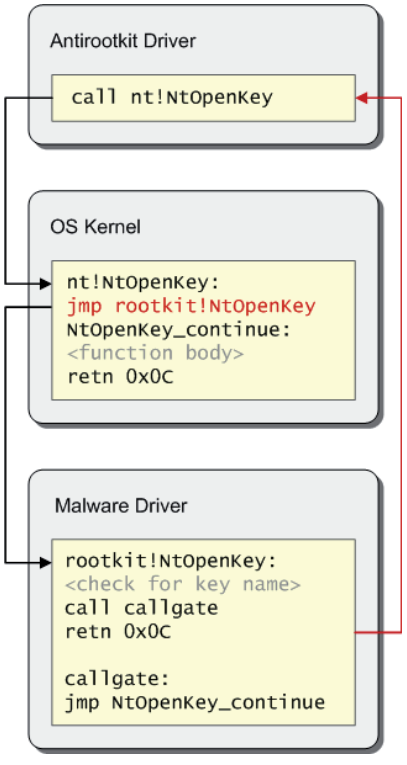


Figure 1: Rootkit modification of kernel.

2. Information is gathered from a lower level of system architecture than the assumed lowest level of a rootkit's residence.

GLOBAL UNHOOKING

Global unhooking is the way in which rootkit activity can be neutralized system-wide. Usually, this includes restoration of the SDT, of some code at the beginning of the kernel functions pointed to from the SDT, of IRP handlers, and generally, of any system structures suspected of having a modification that would cause output data forgery (see code displayed in red in Figure 1).

During system code restoration, a developer faces three difficult challenges:

1. Locating or calculating correct pointers to system calls, IRP handlers etc., which are necessary for the restoration of original execution paths. Likewise, locating the original system executables that are necessary for the restoration of possibly spliced[1] system code at specific locations.

[1] Splicing: inline modification of a function code causing execution flow redirection (usually a jmp or a call).

2. Identifying bad hooks that need to be removed, and distinguishing them from legitimate hooks installed by system applications such as firewalls.
3. Safe writing of data found at pt.1, to locations found at pt.2.

The problem here is that the writing of data to kernel executable regions which are constantly in use by the system can cause BSOD (the blue screen of death) under certain conditions.

The advantage of global unhooking is that, if performed safely and successfully, it allows complete neutralization of some rootkits, restoring to all applications their ability to obtain true information.

The global unhooking approach has a number of significant limitations:

- It is unsafe: global unhooking requires the manipulation of pointers in kernel code which is invoked system-wide. This is a risky operation.
- It is unreliable: a rootkit could reinstall its global hooks at any time.
- It is unsystematic: the specific code locations to be restored must be indicated. This enables a rootkit developer to exploit locations unforeseen by the anti-rootkit.
- It is laborious: finding the original pointers to functions, and distinguishing bad hooks from good hooks, are not simple tasks.

Given the limitations, we can say that global unhooking is more of a primitive reaction to known threats than a universal solution. This approach is not widely implemented in anti-virus solutions due to its insecurity.

GETTING DEEPER

Because the *Windows* architecture is layered, information can be gathered from multiple points of a call chain. Thus, an anti-rootkit that wants to request system information can avoid modified system structures, gathering information by invoking more profound system mechanisms than those that may be compromised.

This approach, which is much safer and far more universal than the previous one, is limited in other significant ways:

- It is labour-intensive: when going lower, it is necessary to implement all the data abstractions and conversions that are normally provided by higher-level mechanisms.
- It is strategically ineffective: because getting lower is more of an avoidance tactic than a solution, it only motivates rootkit developers to get lower too, which will then require even more labour-intensive solutions.

The following is an example of a typical arms race:

1. Rootkit hooks system calls to hide files.
2. Anti-rootkit invokes file system driver.
3. Rootkit hooks file system driver IRPs.
4. Anti-rootkit invokes disk driver.

And so on.

The result is that the protection developer needs to emulate the whole operating system to successfully skirt around a rootkit.

THE ALTERNATIVE

Among all the untrustworthy sources of information, oneself is probably the least untrustworthy. So we propose an anti-rootkit device that performs its own system calls, by providing it with its own clean kernel copy. This is a low-cost way in which genuine information can be obtained by avoiding possibly compromised system mechanisms without risking system safety.

Running your own kernel, if obtained and established properly, will enable reliable detection of the majority of modern kernel malware. More precisely, a lightweight implementation of the kernel copy (described in this article) will allow detection of hidden objects caused by SDT hooking and kernel code splicing rootkits, while a more complex implementation (maintaining copies of a file system and network driver stacks) may allow detection of almost any known kernel malware type.

DETAILS

While it sounds fearfully complex, the basic implementation of a working kernel copy in *Windows* is fairly easy. The basic steps to achieve this are as follows:

1. Find necessary executable files. For a minimal working kernel, take the main kernel file (ntoskrnl.exe in the majority of cases) and hal.dll. The most reliable way to locate kernel files is provided by hardware configuration analysis, as detailed below.
2. Load the files into kernel memory. Remember that the best practice for reading a kernel file is to read it directly from the disk, to ensure file authenticity.
3. Correctly relocate all the calls and data accessing code inside the kernel mapping. Normally, all global variables in the kernel copy should be reinitialized manually. However, for a minimal kernel copy

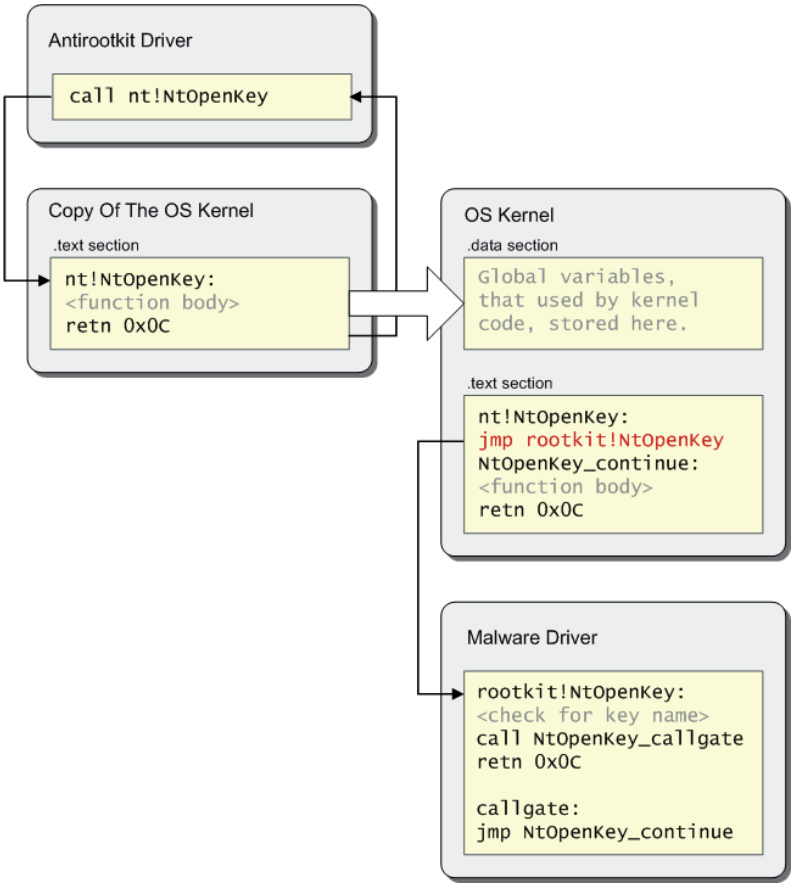


Figure 2: Duplicated kernel execution flow.

implementation, manual initialization is crucial only to certain variables, such as pIofCallDriver and pIofCompleteRequest, which are likely to be pointing to malicious code in the real kernel. The remaining variables can be retrieved from the real kernel.

4. Disable system notifications (both system-wide and locally) to ensure that no hidden data slips through via legitimate callback mechanisms. This can be done by temporary patching of ExReferenceCallBackBlock so that it returns 0 during the scanning process.

5. Redirect kernel calls from your own driver to the local kernel copy.

Because we should assume that straightforward sources for the main kernel file path/name (such as the boot.ini file or HKLM\System\CurrentControlSet\Control\SystemStartOptions 'KERNEL' registry key) could easily be spoofed by a rootkit, it is suggested that a smarter algorithm is used including hardware configuration analysis for locating the main kernel filename. The latter is defined by two system parameters: the number of processors installed, and PAE[2] support.

Kernel name	PAE support	Multiprocessor support
ntoskrnl.exe	No	No
ntkrnlpa.exe	Yes	No
ntkrnlmp.exe	No	Yes
ntkrpamp.exe	Yes	Yes

LIMITATIONS

1. Some hiding malware cannot be detected this way. The list includes malware that implements IRP hooks and filter drivers in order to conceal itself.

2. There is no trivial way in which the kernel copy can be removed immediately on process exit, because it may still be in use by some system threads.
   The suggested solution is to drop kernel code in memory after saving its address in the registry, so that if the anti-rootkit is loaded again, it will not litter the kernel memory.

3. Hidden files and registry keys cannot reliably be removed while the rootkit body and hooks are still present in memory, since hidden objects can be restored by a rootkit.
   The suggested solution is to initiate an immediate reboot (more exactly, a hard reset) after deleting hidden objects.

DEFEATING

Ways in which the suggested technique can be defeated boil down to either falsification or blocking of the external information sources upon which we rely. That is, of the files used to build a kernel copy. How could a rootkit do that?

- A rootkit might push a patched ntoskrnl.exe upon a file-reading request for this file.
  Solution: checking a kernel file's *Microsoft* signature will ensure code integrity.
- A rootkit might spoof filenames instead of content.

[2] PAE = Physical Address Extension.

Solution: retrieval of path/names via analysis of the hardware configuration, as described earlier.

- A rootkit might block access to kernel files.

  This is unlikely, because it would affect certain legitimate software.

ADVANTAGES

Advantages of the technique include the following:

- Safety: manipulating a kernel copy before it starts being used is as safe as performing manipulations on one's own driver, whereas manipulating a system kernel which is already in use is an extremely risky operation regardless of precautions.
- Reliability: a rootkit will never install/restore hooks in a local kernel, since it is not public.
- Purity: the integrity of kernel code which is retrieved manually from the disk and then installed and invoked locally with proper foresight can be guaranteed. Thus, any data retrieval performed via a kernel copy will output clean data unless the very data source is modified.

CONCLUSION

Without presenting another unsound panacea, the approach suggested in this article provides an inexpensive and safe way to detect kernel code modification caused by rootkit activity.

To demonstrate the usability of the suggested technique, we have developed a freeware anti-rootkit tool based on it. The tool is currently specialized for detection of the TDSS rootkit [1], though it is a generic anti-rootkit by design. The tool is named 'Rootkit.Win32.TDSS remover' and is available for download online [2].

In spite of the fact that effective realization of the suggested approach is quite easy, it has never (to our knowledge) been implemented in existing anti-malware solutions. We would be pleased to hear about any software using the technique described in this article.

REFERENCES

[1] Shevchenko, A. Case study: the TDSS rootkit. Virus Bulletin, May 2009, p.10. http://www.virusbtn.com/pdf/magazine/2009/200905.pdf.

[2] http://www.esagelab.com/projects/#tdss_remover.

FEATURE 2

AUTOMATED CLUSTERING OF UNKNOWN EXECUTABLES

Robert Sandilands
Authentium, USA

Why do we want to cluster samples?

We receive tens of thousands of executable samples every day, each of which a customer or another party suspects is malicious. This gives us a significant amount of data, but virtually no information.

What is the difference between data and information? In this case, data is a collection of one million files, each with a hash; information is the same collection of files, but clustered into families with known behaviours for each family including characteristics by which the family can be detected.

The first step in turning the massive amounts of data we receive into useful information is to classify the malware. Trying to classify millions of pieces of malware is either computationally extremely expensive or involves an impossible amount of manual labour. We need to be able to separate samples into large groups of samples that have a good probability of being similar. We can then select a smaller subset of each group to analyse, therefore saving time and responding more efficiently to malware. This is what we hope clustering will achieve.

We could decide to add every executable we receive by some hash – there are companies out there that do this. I don't think we need to go into the folly of that. It would be similar to trying to add detection for a metamorphic file infector using only the hash of the infected file. While we receive millions of samples in a year, I am convinced that this represents fewer than a few thousand different malware families.

The techniques and methods described here are not intended for classification, but there are significant similarities with classification methods and in theory these methods could be used for that purpose. However, I would not recommend it.

The steps that will be followed are:

1. Feature extraction
2. Clustering
3. Validation

STEP 1: FEATURE EXTRACTION

This is the process of extracting measurable information from unknown executables. The choice of features is the most important part of the whole process and can determine its success or failure.

Features can be anything that can be measured and that can be used to detect the samples. There is an art to choosing the right features and it might take a few attempts to find the right ones.

For the purposes of this article I will limit feature selection to physical characteristics only. Physical characteristics are those that can be deduced from simple measurements and do not include code analysis or emulation. This has some very obvious limitations but it will also allow a discussion of the process with few reservations and allows the test results to be reproduced easily.

The features used for this article are:

1. Size of the file
2. Size of section 1
3. Entropy of section 1
4. Size of section 2
5. Entropy of section 2
6. Size of section 3
7. Entropy of section 3
8. Number of sections
9. Offset of PE header
10. Size of appended data
11. Is it a DLL?
12. Entry point section number

Each of these measurements will be normalized to within a range of -1.0 to 1.0. If it is not possible to calculate a feature then it will default to zero. If it is a boolean feature then true will become 0.8 and false will become -0.8.

Obviously you could use every possible measurable feature, or even use something like a genetic algorithm to help optimize your choices. In general, you will find that this is an iterative process that will not only have to be repeated several times to get the initial implementation to work, but also will need to be repeated to fine-tune the behaviour of the algorithm over time.

STEP 2: CLUSTERING

What is clustering? Think of an *n*-dimensional space where *n* is the number of features you have. Consider every sample to be a point in that space with the location determined by its features. Clustering is the process of creating *n*-dimensional spheres in this space that encapsulate groups of samples.

In the simplistic example provided in Figure 1 you can see 16 files listed with their size and compression ratio. This data is completely artificial and was randomly generated to

	Compression ratio
10000	2
11000	2
10500	2
10230	2
10450	1.4
9854	1.3
11230	2
10345	2.3
10234	2.5
9400	1
8400	1
8900	0.7
8950	1
9300	0.8
9020	1
9023	0.9

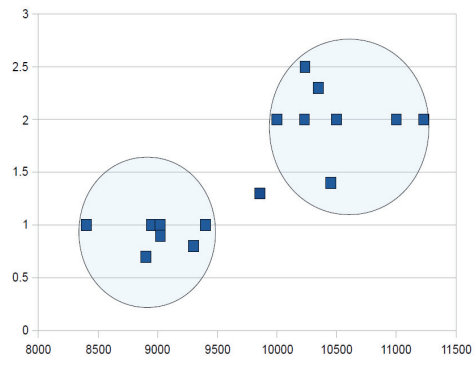


Figure 1: Artificial example of clustering of samples.

illustrate the technique. In this example it can be seen that there are three clusters of samples. Two of the clusters are highlighted using coloured circles and the third cluster is the single remaining point.

Method

Writing software to perform clustering is a relatively involved process and there are several commercial and open source packages available that implement the more important methods. The one I used for this article is Christopher Borgelt's implementation [1], which uses a fuzzy logic-based clustering algorithm. What this implies is that every sample has a probability of belonging to every cluster and can belong to multiple clusters with different probabilities.

I also used the excellent pefile Python module [2] to perform feature extraction. Additional scripts were written to generate and normalize the data [3]. This is a mix of Bash, Python and Perl.

The math

This clustering application is based on a fuzzy c-means algorithm.

Boolean logic is a class of logic whereby something belongs to one of two classes. True or false is an example of boolean logic.

In contrast, fuzzy logic and fuzzy membership is a field of logic whereby something has a degree of membership in any number of classes, and that degree can vary between 0 and 100%. It has a membership function that can be used to calculate the degree of membership for each class. For example, 'hot', 'very hot', 'mildly hot', 'cold' and 'very cold' can be classes in a fuzzy logic system.

If we take a temperature of 30°C then you can say it is most likely hot, a bit very hot and a bit mildly hot. It is

not cold or very cold. You can say it belongs to the class 'hot' with a degree of 80%, to the class 'very hot' with a degree of 10% and to the class 'mildly hot' with a degree of 10%. These are obviously only valid if you are talking about the temperature in a room. If you are talking about the temperature in a plant where steel is melted then the numerical values associated with the classes will be significantly different.

This makes fuzzy logic a very powerful tool for describing concepts that are a bit more complex than boolean logic allows for. It also makes it a very confusing field if you only believe in true and false.

The c-means algorithm is one whereby we iteratively minimize the cost of a fuzzy membership function using some method for optimizing the parameters of the algorithm. In this case the parameters are the location and size of the clusters.

The next question is: how do you optimize the parameters?

The method used to optimize the parameters is a variant of the back propagation algorithm also used to train neural networks. It is just a method where the parameters of the function being optimized are adjusted using the gradient of the error function. The error function is chosen to ensure optimal clustering.

Sample set

The sample set comprised 1,233 samples that varied between 2,346 and 293,760 bytes in size. All the samples were 32-bit *Windows* PE executables. Some of the samples were packed, others were not.

The results

One of the parameters for the clustering algorithm is the number of clusters it has to use. In this case 15 clusters were selected. The following results were obtained:

Cluster	Total
14	66
13	3
12	160
11	112
10	97
9	137
8	1
7	97

Cluster	Total
6	106
5	2
4	3
3	17
2	95
1	157
0	179

Let us assume that any cluster containing more than 50 samples is worth investigating. We assume that considering fewer than 50 samples for a generic signature is inefficient. We can look at the samples that were included in clusters 14, 12, 11, 10, 9, 7, 6, 2, 1 and 0. This allows us to look at a subset of samples from 10 different clusters which represents 1,207 of the group of 1,233 samples provided.

STEP 3: VALIDATION

The question is, how useful are these results? It has been stated that the features used in this article are very limited, so it would not be surprising if the results were not very useful.

The samples were selected from our malware archives. A random subset of samples were selected from files that were classified by our scan engine using 10 different names. They were:

W32/Allaple.C
W32/Allaple.J
W32/Backdoor.ALHF
W32/Downloader.ALJ
W32/Downloader.OJ
W32/EmailWorm.AMX
W32/Trojan2.SRR
W32/Trojan.AYPG
W32/Trojan.Inject.A
W32/Worm.MWD

Samples	Name	Cluster
179	W32/Trojan2.SRR	0
160	W32/Backdoor.ALHF	12
157	W32/Downloader.OJ	1
137	W32/Allaple.C	9
112	W32/Allaple.J	11
106	W32/Trojan.AYPG	6
97	W32/Trojan.Inject.A	7
97	W32/EmailWorm.AMX	10
95	W32/Downloader.ALJ	2
66	W32/Worm.MWD	14
11	W32/Allaple.J	3
4	W32/EmailWorm.AMX	3
3	W32/Allaple.J	4
3	W32/Allaple.C	13
2	W32/Allaple.C	3
1	W32/Worm.MWD	8
1	W32/EmailWorm.AMX	5
1	W32/Allaple.J	5

Table 1: Results and malware names together.

The fact that the clustering algorithm identified 10 clusters, matching the number of malware names used to select the samples, is encouraging.

Table 1 lists the results and the malware names together. The last eight items show a group of samples that were not clustered as would be expected. When investigating these samples they all seemed to be corrupted or not related, indicating a possible issue with the signature used to classify them.

CONCLUSION

Given the limitations in the features used for this demonstration, this technique showed surprisingly promising results. With more advanced feature selection much better results should be possible.

There is a relatively good match between the samples we already detect using the same name and the results of the clustering. This shows that the technique has some promise when used with a group of unknown samples. The intention of these techniques is to help focus analysis efforts and to simplify the process of selecting samples for generic detection.

The quality of the results is dependent on the quality of the feature extraction. A significant amount of time will have to be spent on verifying whether the feature selection is providing good clusters. This verification should be part of the analysis process. A subset of the samples must be analysed to determine their behaviour and the optimal detection. This should also provide feedback for the feature extraction process. As with any non-deterministic method it is not suggested that this method should be used as the only tool to solve a problem, but as part of a larger arsenal of tools.

I hope this article has instilled sufficient curiosity in the subject of clustering to convince readers to investigate it as a viable technology to use to help in the daily efforts of analysing very large numbers of samples.

REFERENCES & FURTHER READING

[1] Borgelt, C. Cluster – Fuzzy and Probabilistic Clustering. http://www.borgelt.net/cluster.html.

[2] Carrera, E. pefile Python module. http://code.google.com/p/pefile/.

[3] Sandilands, R. Other scripts and data. http://robert.rsa3.com/vbcluster09.zip.

[4] Matteucci, M. http://home.dei.polimi.it/matteucc/Clustering/tutorial_html/cmeans.html.

CONFERENCE REPORT

REFLECTIONS ON CEAS 2009

Gordon V. Cormack
University of Waterloo, Canada

Since its inception in 2004, CEAS (the Conference on Email and Anti-Spam) has been held in Silicon Valley. Perhaps the biggest news to come from the 2009 event, was that it is tentatively set to move north to Seattle next year, to collocate with SOUPS, the Symposium on Usable Privacy and Security (http://cups.cs.cmu.edu/soups/2009/). The proposed move reflects the importance of human, social and societal issues – in addition to technical ones – in facilitating electronic communication while mitigating abuse.

KEYNOTE PRESENTATIONS

The keynote speech on the first day of the event was given by Dave Dittrich, who explored possible ways in which spammers or spam service providers might be punished for their activities. Given the expansive international underground network that supports spam and related activities, the conclusion is unclear.

Lori Cranor, organizer of SOUPS, addressed delegates on the second day of the event, emphasizing the need to coordinate the detection of phishing with education, so that users can learn how to respond to phishing attacks and alerts. A demonstration of educational materials employing the animated character PhishGuru is available online at http://phishguru.org/.

CONTRIBUTED PAPERS

In theme, the 23 contributed papers selected for CEAS 2009 ranged from understanding spammers to understanding users, and from pure technical solutions to those designed to engage the spammer or user.

Spammer behaviour

The first session explored the dimension of spammer behaviour. The first paper observed that spam is generated through vast networks, and that pinpointing the original spam is difficult. Next, 'Spamology: a study of spam origins' explored the propagation of email addresses through spammers' mailing lists. 'Spamming botnets: are we losing the war?' observed that the distribution of spam IP addresses is becoming more diverse, indicating that there are ever fewer 'safe' subnets that can be assumed to be uncompromised by spambots. Finally, in 'How much did shutting down McColo help?', Richard Clayton observed that while the volume of spam decreased acutely as the result of shutting down the large spam service provider, the

decrease was temporary and consisted mainly of 'easy to filter' spam messages. The net effect was perhaps less than might be assumed from elementary measurements.

Personalization

The second session considered the role of user input in spam filtering. First in this session was a paper considering the contrasting models of server-side vs. personal spam filtering, which observed that a personal spam filter can be trained using the results of a commercial server-side filter, requiring no input from the user. Next, 'Going mini: extreme lightweight spam filters' considered the problem of providing personalized spam filters in a server environment where a very limited amount of memory is available per user. The final paper in this session addressed the same problem by hashing personal and community judgements into a common feature space. The results presented indicate that this approach improves filter performance for those users who train the system as well as for those who don't – a win-win situation.

Technical approaches – server side

The third session considered anti-spam techniques that might be employed by a large email service provider. The first paper, 'Router-level spam filtering using TCP fingerprints', presented an approach to identifying spam from the router's perspective, where packets rather than complete messages are handled. Next, 'An anti-spam filter combination framework for text-and-image emails' considered how to combine the results of image- and text-based filters to improve overall accuracy. A group from Texas A&M University presented a tool designed to translate *SpamAssassin* regular expression rules into POSIX. *SpamAssassin* is slow, in large part due to the fact that it uses patterns written in Perl, which is an interpretive language. When translated into POSIX regexp syntax, the patterns can be compiled and executed much more efficiently. The translation is inexact, but yields good results. The final paper in this section explored the idea of using new spam and old ham to train products – based on the premise that spam changes much more quickly than non-spam, but is also much easier to collect.

Engaging the user

In the next session, 'An empirical analysis of phishing blacklists' explored the impact of phishing page warning messages on the user – phishing detection is of little use unless the user heeds the warning. 'Anti-phishing landing page: turning a 404 into a teachable moment for end users' investigated a user interface design in which links from phishing pages lead to educational pages explaining why the user was duped, and how to be more wary. The final paper in this session examined the issue of inadvertently addressing email to the wrong user, and proposed a mechanism to warn the user in many such cases.

Statistical filtering

The paper 'Training SpamAssassin with active semi-supervised learning' considered the idea of asking the user to label a small subset of messages – selected by the filter – as spam or non-spam. The overall impact is to lessen the burden on the user, while providing better personalized filtering. The paper 'Feature weighting for improved classifier robustness' considered the problem of incorrect training examples: spam messages labelled as non-spam, and vice versa. Such examples may occur due to user error or due to a spammer being able to label messages (for example, in a collaborative filtering system).

Potpourri

In the final session, 'Extracting product information from email recipients using Markov logic' considered the problem of identifying electronic transactions. For example, a participant in CEAS may have subscribed to an information list, used a web system to submit a paper, and a different web system to register. How can an email system recognize and accumulate the various messages related to the conference? 'CentMail: rate limiting via certified micro-donations' considered an approach to engage both sender and recipient, excluding the spammer. Like all previous proposals for proof of payment, this paper generated controversy. Finally, 'A human factors approach to spam filtering' suggested that the user should be engaged differently, labelling rather than filtering spam.

OVERALL

In the wrap-up meeting, the organizers solicited suggestions for a new name for CEAS, while preserving the acronym. The issues and technologies underlying the use and abuse of email are converging with those for other forms of electronic communication and collaboration – including the web, social networks, text messaging and collaborative recommender systems. For example, 'C' could stand for 'collaboration' or 'communication'; 'E' could represent 'electronic'; 'A' could be 'adversarial' or 'abuse'; 'S' – 'symposium', perhaps?

From my perspective, the most interesting papers fell at the boundary between technology and human factors. Usability is as important as technology and it makes no sense to study the two separately. The future collocation of the event with SOUPS (and perhaps another yet-to-be-named workshop) will provide valuable cross-pollination of interests and expertise.

The papers from this year's conference are available at http://www.ceas.cc/.

COMPARATIVE REVIEW

WINDOWS VISTA BUSINESS EDITION SP2 X32

John Hawes

Windows Vista limps onto the test bench once more this month – perhaps not quite the lame duck it is reputed to be, but certainly far from a roaring success. As the release of its replacement (*Windows 7*) approaches fast, little nostalgia has accumulated for the platform, with the user base still barely troubling its aging predecessor *XP*. Most estimates put *Vista* on fewer than 30% of desktops, with *XP* holding onto more than 60% of the marketplace some eight years after its release and a year after the first stages of its withdrawal from sale. Popular opinion continues to belittle *Vista*'s accomplishments and most would-be upgraders seem content to wait for the new and improved version 7, due in just a few months' time.

Our own previous experiences with the platform have done little to endear it to us, and presumably the developers of most anti-malware solutions have similar feelings, given the oddities, instabilities and general bizarreness we've seen on the platform in previous tests. We expected to see more of the same this time around, and hope that the advent of a replacement will mean not too many more comparatives on *Vista* will be necessary. The arrival of a new service pack promised to bring a new level of unpredictability to the mix, with the added stability it was designed to provide counterbalanced by the likelihood of a whole new range of horrors.

PLATFORM AND TEST SETS

Installing and preparing the test systems was a little less unpleasant this time thanks to a little experience, with many of the pitfalls – such as the tendency to go into deep sleep in the middle of an overnight scan – circumvented at an early stage. Applying the new service pack proved unproblematic, if rather long-winded, and the systems did seem more stable than on previous occasions. As usual, our Luddite tendencies led us to disable most of the funky graphical stylings and revert settings to the 'classic' style where possible, but the UAC system was left intact to monitor how well various products were integrated with it, knowing full well that in some cases it would produce numerous intrusions and in a few it might need to be disabled completely.

Several of the products submitted were unable to comply with our request for offline updating, so in addition to snapshots of the bare test system several others were taken on the deadline date with installed and updated products in situ, thus allowing them to be tested on a level field with the others.

The deadline for product submission was set for 24 June, which proved a more than usually busy day thanks to the extra tasks of installing products, connecting them to the web for updates and taking snapshots. We were relieved that the field of entrants was not as enormous as it might have been, with several of the occasional entrants of recent tests failing to turn up and some prospective newcomers deciding at the last minute that they were not quite ready to dip their corporate toes into the often chilly waters of the VB100. In the end a total of 37 products were entered for the test, but as in previous tests we reserved the right to exclude any which proved intractable or uncooperative, to allow enough time to test as many products as possible.

A measure taken for the first time this month has been to impose a nominal charge for multiple entries from the same vendor. We have no intention of breaking with the VB100 tradition of being free and open to all comers, but in recent tests a number of vendors have opted to submit multiple products, which has added significantly to the growing burden of testing. To avoid passing on to our readers the additional costs (in terms of hardware, space and manpower) of the ever-increasing field of competitors, we have opted to impose a per-product fee on the third and subsequent submissions from any single vendor (any vendor may submit up to two products to each test free of charge, a nominal fee will be charged for each product that exceeds this number). This month just one vendor chose to enter three separate products and was duly requested to contribute to our running costs, but of course this was not allowed to influence our treatment of the product in any way, either in the opinions given in the write-up or in the results collected from it.

With the test systems prepared and the field of products gathered, the final stage of set-up was the compilation of the test sets, which as usual since the introduction of our RAP testing system was not completed until a week after the deadline for product submissions. The bulk of our test sets were already frozen, with the standard test set deadline set a few days prior to the product deadline, on 20 June. The May 2009 WildList was released a few days prior to this date, and was thus used as the basis for our core certification set. The list was remarkable for the large number of new items included, dominated as many recent lists have been by online gaming password-stealers. Of most note in the list were a handful of samples of Conficker (aka Downadup), whose headline-grabbing days seem well in the past now, along with some social network targeting items such as W32/Koobface. Of most interest to us, however, was the addition of a genuine and by all accounts highly tricky

file-infecting virus – one of many sub-strains of the W32/Virut family which have caused a number of problems for major products in the past. With the ongoing development of our automated systems, we were able to include fairly large numbers of replicated samples in the test set. This meant that a list containing 677 items was represented by over 3,000 unique samples. As usual, percentages presented in the results tables are based on per-variant detections, rather than per sample, with the 2,500-odd Virut samples counted as a group with the same weighting as a single sample of the other entries, hence the rather fine percentage margins in some cases.

The growth in size was also seen elsewhere, with similarly large numbers of Virut samples added to the polymorphic set to represent some of the other sub-strains emerging in recent months. The RAP sets were compiled in the weeks leading up to and the week following the product submission deadline, and as usual fluctuated in size somewhat thanks to the unpredictable flow of samples into our various feeds. The trojan set was compiled from similar sources in the month or so prior to the RAP start date.

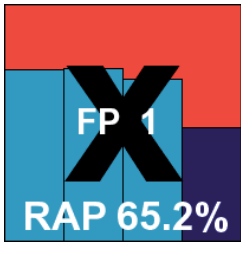
The greatest addition to the test sets this month was to the clean sets, with several hundred thousand new samples making their appearance this month after an ambitious period of sample gathering. The bulk of the samples came from well-known and widely used software brands and products, as part of a project to reorganize our clean sets by significance. While we expected few new false positives to emerge, it was of course impossible to rule out major and embarrassing slip-ups by some. We anticipated that the main impact of the enlargement of the set would be seen in scanning time and stability issues.

With all this squeezed onto the test systems, we prepared to shut ourselves away in the test lab, unlikely to see the sun for some time and with the prospect of a long and difficult month ahead.

Agnitum Outpost Security Suite Pro 6.5.5

ItW	100.00%	**Polymorphic**	89.99%
ItW (o/a)	100.00%	**Trojans**	87.48%
Worms & bots	99.71%	**False positives**	1

First on the roster, *Agnitum*'s suite product is nice and thorough, and as such has a rather slow installation process, which somewhat unusually creates a restore point before it gets underway. The interface is nicely designed and clear, but gives little space to the anti-malware component in amongst the various other modules and so provides fairly little by way of user configuration. Running tests proved fairly unproblematic, but at one point, during on-access scanning of clean files, a nasty crash complete with blue screen was observed. With care, the tests were completed however.

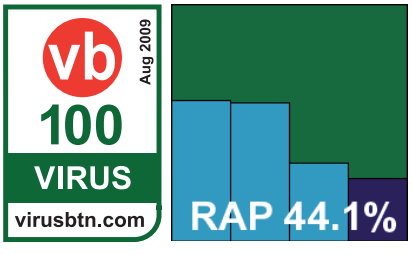


Detection rates proved pretty impressive, with a fairly steep drop in the +1 week of the RAP sets mitigated by some comfortingly even scores in the reactive portion, making for a strong overall average. Coverage of the large number of new Virut samples was impeccable, and the WildList was detected without issues, but in the clean sets a single file from the large swathe of new additions was alerted on as a trojan. The detection was recognizable to the practised eye as packer-based, but as the file is included with a recent version of *Microsoft*'s .NET framework – something which labs really should be tracking as part of their false positive mitigation regime – this was considered enough to deny *Agnitum* a VB100 this month.

AhnLab V3 Internet Security 8.0.0.2

ItW	100.00%	**Polymorphic**	99.58%
ItW (o/a)	100.00%	**Trojans**	87.49%
Worms & bots	99.89%	**False positives**	0

AhnLab's product has had something of an overhaul since we last looked at it, and presents a clean and appealing interface with a speedy installation process needing no reboot to complete. The interface has a few quirks of layout and also a few stability issues under heavy fire, suffering some lengthy freezes after longer scans and on-access runs. Logging also proved somewhat tricky, as the log viewer utility seemed unable to cope with large logs, spending some time trying to refresh its listings but eventually giving up. On a couple of occasions we also observed the test machine mysteriously shutting down during a long scan, which we attributed to overheating. To complete testing some of the test sets had to be broken up into smaller chunks to ensure they ran to the end and to enable accurate collection of data.

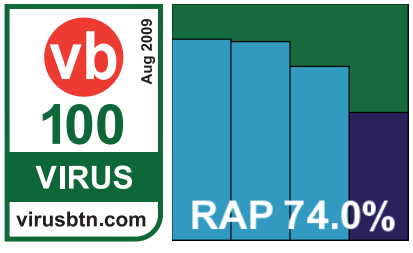


Scanning speeds were pretty decent though, and the interface generally proved simple to use and responsive, so testing completed in reasonable time despite the extra steps required. Although a fair number of samples of recent W32/Virut strains were missed, the specific variant included

in the WildList set was handled without difficulty, and with no other misses and no false positives, *AhnLab* earns the first VB100 award of this month's batch.

Alwil avast! Professional 4.8.1346

ItW	100.00%	**Polymorphic**	99.46%
ItW (o/a)	100.00%	**Trojans**	96.90%
Worms & bots	99.96%	**False positives**	0

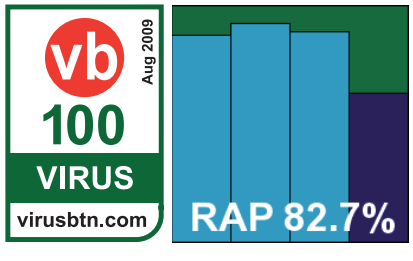


Alwil's *avast!* remains pretty much unchanged after some time in its present form, with its somewhat quirky design still resembling a media player in its standard 'basic' layout. A major new version is due sometime soon, and we look forward to the opportunity of taking a look at it in the coming months. For now, the installation process remains fast and simple, with a reboot not specifically required but recommended in case of problems. The advanced interface required for much of our testing still has a tree layout with some oddities of its own, which we found somewhat confusing despite much practice, and which continues to have a few issues during longer scans: a lack of refreshing leaves useful data invisible and inaccessible until the end of a scan.

Detection rates were pretty strong, not quite up to the excellent standards achieved in recent months, at least on the more recent samples in the RAP sets, but still good, with an overall average of 74% in the RAP test. The large number of new Virut samples presented no difficulty, and with no other issues in the WildList or extended clean sets, another VB100 award is granted to *Alwil*.

AVG Internet Security 8.5 build 375

ItW	100.00%	**Polymorphic**	99.03%
ItW (o/a)	100.00%	**Trojans**	97.83%
Worms & bots	99.99%	**False positives**	0

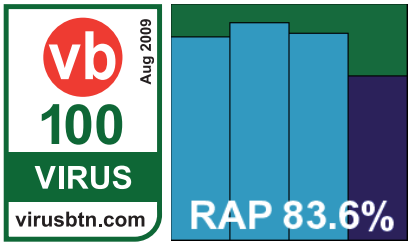


AVG's product remains attractive and well designed. The offer of a toolbar somewhat dampened our enthusiasm, but its recommended rather than enforced nature made up for this a little. At the end of the rather sluggish install, a 'first run wizard' leads through some initial set-up steps for the various components, and once finally through to the main interface with its multiple module/icon layout we found it fairly intuitive to use, if a little over complicated in places. Configuration options appeared a little limited for our tastes – for example lacking the option to scan archives on access, and the on-access mode also relies on file extensions to decide whether or not to scan things.

Speeds were a little below average, but detection rates more than made up for this, with superb levels across the board, the RAP average pushing close to 85% in a masterful display. With no issue in any of the new Virut strains, or anywhere else really, *AVG* comfortably earns our praise, and of course a VB100 award.

Avira AntiVir Professional 9.0.0.725

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.32%
Worms & bots	100.00%	**False positives**	0



Avira's *AntiVir* has a nice swift installation, with a requirements wizard which we found a pleasing touch. No reboot is required to get things going, and a swift check-up of the system ensures everything is up and running safely. The interface presents a sleek and easy-to-navigate layout, with an excellent level of configuration available without overwhelming the user. Again, file extensions are considered a reliable method of judging whether a file needs scanning.

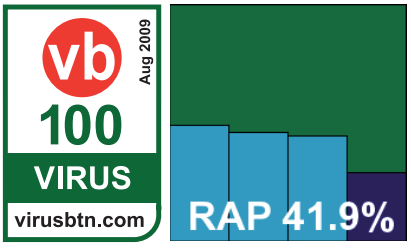
Perhaps aided by this shortcut, scanning speeds proved excellent, and detection rates once again highly impressive, very nearly catching the whole of our trojans set and also close to 85% average in the RAP sets. With no difficulties in the WildList set, and only a handful of suspicious alerts in the clean sets, *Avira* also walks away with a VB100 award.

CA eTrust ITM 8.1.655.0

ItW	100.00%	**Polymorphic**	92.79%
ItW (o/a)	100.00%	**Trojans**	77.97%
Worms & bots	100.00%	**False positives**	0

On-demand detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost Security Suite Pro	0	100.00%	8	99.71%	231	89.99%	1751	87.48%	1	0
AhnLab V3 Internet Security	0	100.00%	3	99.89%	58	99.58%	1748	87.49%	0	0
Alwil avast! Professional	0	100.00%	1	99.96%	7	99.46%	433	96.90%	0	0
AVG Internet Security	0	100.00%	1	99.99%	21	99.03%	304	97.83%	0	0
Avira AntiVir Professional	0	100.00%	0	100.00%	0	100.00%	95	99.32%	0	3
CA eTrust ITM	0	100.00%	0	100.00%	960	92.79%	3080	77.97%	0	0
CA Internet Security Suite	0	100.00%	0	100.00%	960	92.79%	3056	78.14%	N/A*	0
eEye Blink Professional	0	100.00%	0	100.00%	319	83.74%	1920	86.26%	0	1
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	419	97.00%	0	0
Filseclab Twister AntiTrojanVirus	2612	91.45%	363	84.02%	8789	28.93%	3119	77.69%	38	4
Finport Simple Anti-Virus	2897	49.41%	619	72.74%	11058	19.59%	5339	61.81%	2	0
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	4985	64.34%	0	2
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	12	99.89%	2728	80.49%	0	0
F-Secure Client Security	0	100.00%	0	100.00%	2	99.998%	710	94.92%	0	0
F-Secure PSB Workstation Security	0	100.00%	0	100.00%	2	99.998%	746	94.66%	0	0
G DATA AntiVirus 2010	0	100.00%	0	100.00%	0	100.00%	61	99.57%	0	0
K7 Total Security Desktop	0	100.00%	5	99.78%	585	87.45%	2475	82.29%	1	0
Kaspersky Anti-Virus 2009	0	100.00%	3	99.87%	2	99.998%	411	97.06%	0	0
Kingsoft Internet Security 2009 Std	228	99.99%	11	99.76%	4365	58.96%	5256	62.40%	0	0
Kingsoft Internet Security 2009 Adv	0	100.00%	10	99.77%	2386	60.74%	1801	87.12%	0	0
McAfee Total Security	0	100.00%	0	100.00%	0	100.00%	470	96.64%	0	0
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	602	95.69%	0	0
Microsoft Forefront Client Security	0	100.00%	0	100.00%	276	99.51%	566	95.95%	0	0
MWTI eScan Internet Security Suite	0	100.00%	0	100.00%	0	100.00%	475	96.60%	0	12
Nifty Corp. Security24	0	100.00%	0	100.00%	2	99.998%	670	95.21%	0	0
Norman Security Suite	0	100.00%	0	100.00%	319	83.74%	1919	86.28%	0	1
PC Tools AntiVirus 2009	1150	99.93%	7	99.85%	5179	69.77%	4545	67.49%	1	2
PC Tools Internet Security 2009	1134	99.93%	32	98.88%	5178	69.78%	4484	67.92%	1	2
PC Tools Spyware Doctor	1134	99.93%	0	100.00%	5178	69.78%	4484	67.92%	1	2
Quick Heal AntiVirus Lite 2009	0	100.00%	6	99.80%	149	98.23%	1468	89.50%	0	0
Rising Internet Security 2009	43	99.998%	2	99.91%	1169	72.98%	2807	79.92%	1	0
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	698	95.01%	0	0
Symantec Endpoint Protection	2	99.9999%	0	100.00%	8	99.99%	275	98.04%	0	0
Trustport Antivirus 2009	0	100.00%	0	100.00%	17	99.22%	347	97.52%	0	0
VirusBuster VirusBuster Professional	0	100.00%	2	99.97%	189	90.12%	1210	91.35%	1	0

*See p.18

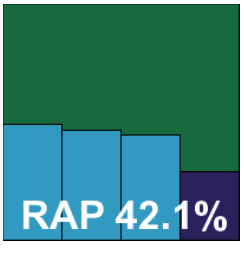


We have been begging for a new version of *CA*'s corporate product for some time, and have heard hints that a major overhaul may be on the horizon, so when this month's submission arrived labelled 'refresh' there was some excitement in the lab. However, after the install, with its usual long chain of EULAs and data gathering, we were treated to no major changes beyond a slight adjustment to the look and feel. As observed in some earlier tests on *Vista*, the browser-based interface is quite a lot less sluggish to respond than on other platforms, but remains rather awkward to use for any serious purposes. While settings appear to be present in some depth, some obvious items are missing, while some, such as the option to scan archives on access, fail to work once the option to enable them has been dug up.

Scanning speeds were as remarkable as ever, with the product powering through the test sets in incredible time, and detection rates in the older parts of the sets were decent. The RAP scores were somewhat disappointing, but in the core certification areas of the WildList and the clean sets no problems were encountered, and a VB100 award is duly granted to *CA*.

CA Internet Security Suite 10.0.0.177

ItW	100.00%	**Polymorphic**	92.79%
ItW (o/a)	100.00%	**Trojans**	78.14%
Worms & bots	100.00%	**False positives**	N/A



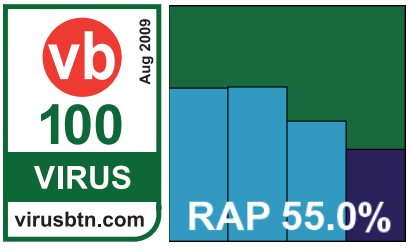
The latest version of *CA*'s home-user product is smooth and clean and generally very pleasing to look at, and setting up and running through the tests proved a fast and simple process. The on-access alert pop-ups had a tendency to recur rather more often than strictly necessary, but never caused any issues with the normal running of the system beyond their irritation value. In the standard set of tests, results were much the same as with the corporate version – remarkable speeds, reasonable to disappointing detection rates, but no major issues in any of the test sets, including the clean set.

However, the product submitted for this month's test was the full *Internet Security Suite*, rather than the simpler anti-virus solution entered for previous tests. The suite includes, among other modules, an anti-spyware component. This component is pre-programmed to run a spyware scan on a schedule, which seems to be set up for a first run not long after installation. At the end of the scan, *whether or not installed spyware is found on the machine* (and indeed on other occasions, such as when attempting to disable the anti-spyware component) a pop-up appears, informing the user that unidentified, non-specific 'threats' have been discovered on the machine, which can only be removed by a fully licensed version of the product. Our test machines, although laden with malware sitting harmlessly on the hard disks, are in fact quite pure and free from infection, with no malware installed or even present in the system drive. On further testing, we found that the same pop-up appears on machines freshly installed with a clean copy of *Windows* and with no whisper of a 'threat' present. The issue appeared only to arise on systems disconnected from the Internet, and thus not fully 'activated', but it is a scenario in which real-world users may find themsleves, for example when checking a suspect and quarantined machine for infections, in which case they may find themselves misled.

Although we fully accept the developers' insistence that the issue is a bug and that no deception is intended, the suggestion that these vague 'threats' are present is counted as an unspecified number of false positives, and *CA*'s home-user product is thus denied a VB100 award for this month.

eEye Digital Security Blink Professional 4.3.2

ItW	100.00%	**Polymorphic**	83.74%
ItW (o/a)	100.00%	**Trojans**	86.26%
Worms & bots	100.00%	**False positives**	0



Blink is a rather complex product with a range of components, and the installation process reflects this in its duration and complexity. The process is accompanied by the product's usual range of peach, sky blue and other delightful pastel tones, as is the main interface when it comes along. With many other modules to manage, including a firewall which appears to be entirely disabled by default, the anti-malware component (which is based on the *Norman* engine) is afforded few configuration options, but the basics are catered for and the defaults are pretty sensible.

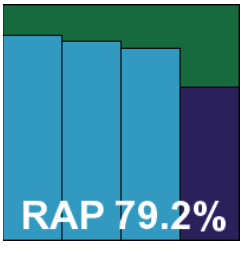
On-access detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost Security Suite Pro	0	100.00%	8	99.71%	231	89.99%	1427	89.80%	1	0
AhnLab V3 Internet Security	0	100.00%	3	99.89%	58	99.58%	1742	87.54%	0	0
Alwil avast! Professional	0	100.00%	1	99.96%	7	99.46%	2405	82.79%	0	0
AVG Internet Security	0	100.00%	1	99.99%	21	99.03%	469	96.65%	0	0
Avira AntiVir Professional	0	100.00%	0	100.00%	0	100.00%	101	99.28%	0	3
CA eTrust ITM	0	100.00%	0	100.00%	960	92.79%	3079	77.98%	0	0
CA Internet Security Suite	0	100.00%	0	100.00%	960	92.79%	3077	77.99%	N/A*	0
eEye Blink Professional	0	100.00%	0	100.00%	365	82.67%	2380	82.98%	0	1
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	654	95.32%	0	0
Filseclab Twister AntiTrojanVirus	2612	91.45%	395	82.61%	8789	28.93%	3378	75.83%	38	4
Finport Simple Anti-Virus	2897	49.41%	644	71.64%	11058	19.59%	5339	61.81%	2	0
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	4970	64.45%	0	2
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	12	99.89%	2786	80.07%	0	0
F-Secure Client Security	0	100.00%	0	100.00%	2	100.00%	924	93.39%	0	0
F-Secure PSB Workstation Security	0	100.00%	0	100.00%	2	100.00%	922	93.41%	0	0
G DATA AntiVirus 2010	0	100.00%	0	100.00%	0	100.00%	107	99.23%	0	0
K7 Total Security Desktop	0	100.00%	50	97.82%	774	84.20%	2507	82.07%	1	0
Kaspersky Anti-Virus 2009	0	100.00%	3	99.87%	2	100.00%	1010	92.78%	0	0
Kingsoft Internet Security 2009 Std	228	99.99%	11	99.76%	4365	58.96%	5287	62.18%	0	0
Kingsoft Internet Security 2009 Adv	0	100.00%	10	99.77%	2386	60.74%	1900	86.41%	0	0
McAfee Total Security	0	100.00%	0	100.00%	0	100.00%	3910	72.03%	0	0
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	602	95.69%	0	0
Microsoft Forefront Client Security	0	100.00%	0	100.00%	276	99.51%	1112	92.04%	0	0
MWTI eScan Internet Security Suite	0	100.00%	0	100.00%	0	100.00%	487	96.52%	0	12
Nifty Corp. Security24	0	100.00%	0	100.00%	2	100.00%	1048	92.50%	0	0
Norman Security Suite	0	100.00%	0	100.00%	365	82.67%	2380	82.98%	0	1
PC Tools AntiVirus 2009	1188	99.95%	19	99.30%	7347	64.18%	4565	67.34%	1	2
PC Tools Internet Security 2009	1355	99.95%	99	96.80%	5190	69.67%	5858	58.09%	1	2
PC Tools Spyware Doctor	1355	99.95%	2	99.91%	6697	66.27%	6246	55.32%	1	2
Quick Heal AntiVirus Lite 2009	0	100.00%	9	99.67%	178	95.98%	2519	81.98%	0	0
Rising Internet Security 2009	43	99.998%	2	99.91%	1169	72.98%	2816	79.86%	1	0
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1120	91.99%	0	0
Symantec Endpoint Protection	2	99.9999%	0	100.00%	8	99.99%	277	98.02%	0	0
Trustport Antivirus 2009	0	100.00%	0	100.00%	17	99.22%	2130	84.76%	0	0
VirusBuster VirusBuster Professional	0	100.00%	2	99.97%	189	90.12%	1350	90.34%	1	0

*See p.18

Scanning speeds were somewhat slow, most likely thanks to the implementation of the *Norman Sandbox* for extra protection. This provided a solid level of detection in the less recent parts of the test set, with a slight dip in coverage of the newer samples in the RAP sets and a small number of the new Virut samples not covered, but the strain included in the WildList set was fully detected. With no other issues in the rest of the WildList or the clean sets, *eEye* earns a VB100 award.

ESET NOD32 Antivirus 4.0.437.0

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



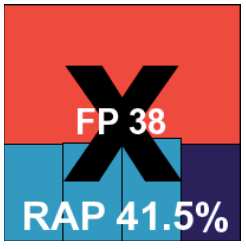
The latest iteration of *ESET*'s product has changed little on the surface. The usual fairly smooth installation process was interrupted only by a UAC prompt for an unfamiliarly titled installer program halfway through, and the usual attractive, excellently designed interface was present with its wealth of in-depth configuration. As in some previous tests, the stability of the interface was somewhat questionable under pressure, with a few wobbly moments evident especially after heavy bombardment in the on-access tests. On a couple of occasions we had to resort to the task manager to kill the product in order to get access to the GUI again.

These minor quibbles (unlikely to affect the bulk of everyday users) were more than made up for by some stellar detection rates, with the standard sets covered almost impeccably and the RAP sets handled with similar excellence. With some decent, if not outstanding scanning speeds, and no problems in either the WildList or clean sets, *ESET* easily earns another VB100 award.

Filseclab Twister AntiTrojanVirus 7.3.2.9971

ItW	91.45%	**Polymorphic**	28.93%
ItW (o/a)	91.45%	**Trojans**	77.69%
Worms & bots	84.02%	**False positives**	38

The somewhat oddly named *Filseclab*'s somewhat oddly named *Twister AntiTrojanVirus* makes its second appearance in the VB100, having impressed last time around with its slick presentation and stable operation if not with its detection rates. This time once again the install process was fast and smooth, although the UAC system presented some serious warnings about unknown and untrusted publishers. The main interface is clear and lucid, with a user-friendly and attractive design.

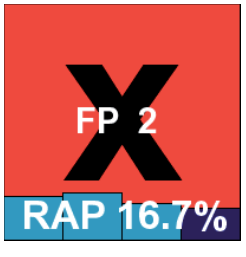


Once again the on-demand mode proved fast and stable, while the on-access mode presented something which we would later find to be a recurring issue in this test: the inability to block access to infected files. *Twister* is designed primarily as a behavioural and HIPS product, intended to monitor executing programs for malicious behaviour, with the standard anti-virus-style file access hooking added later than much of the product. In this case the on-access detection seems only to log attempts to access files, doing nothing to prevent them from being accessed. The logging proved reliable however, and speeds were decent in both modes, although as the on-access module was not actually preventing access, the speed measurement may not be strictly comparable with other products. Detection rates were also fairly decent, at least in the less recent items in the standard sets, although handling of polymorphic viruses was less than impressive. In the RAP sets detection rates were somewhat below par but at least even and regular. The WildList was not fully covered, with fairly minimal coverage of the Virut variant included there, and in the clean sets a number of false positives turned up, denying *Filseclab* a VB100 award this time, but still looking a promising prospect.

Finport Simple Anti-Virus 4.2.3.1

ItW	49.41%	**Polymorphic**	19.59%
ItW (o/a)	49.41%	**Trojans**	61.81%
Worms & bots	72.74%	**False positives**	2

Another product making its second appearance in our tests, *Finport* also had some issues with the UAC controls, requiring them to be turned off to allow the install process to complete successfully. While the main interface is pleasantly laid out and as simple as the title suggests, some aspects remain incomplete, with the EULA and some portions of the configuration and logging presented in the Cyrillic characters of the developers' native Ukraine.



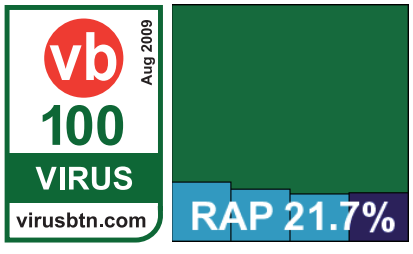
The controls are minimal but would be sufficient for many inexpert users, with a sensible set of defaults. Some areas

On-demand throughput (Time = s; Throughput = MB/s)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put
Agnitum	1108	2.71	1108	2.71	250	10.36	250	10.36	202	10.22	202	10.22	108	8.69	108	8.69
AhnLab	160	18.78	177	16.98	177	14.63	182	14.23	85	24.28	86	24.00	69	13.60	103	9.11
Alwil	282	10.66	1884	1.59	488	5.31	491	5.27	302	6.83	322	6.41	215	4.36	223	4.21
AVG	1849	1.63	1851	1.62	626	4.14	630	4.11	162	12.74	192	10.75	32	29.32	146	6.43
Avira	391	7.68	391	7.68	102	25.39	102	25.39	83	24.87	83	24.87	42	22.34	42	22.34
CA eTrust	360	8.35	360	8.35	76	34.07	76	34.07	56	36.86	56	36.86	37	25.35	37	25.35
CA ISS	753	3.99	753	3.99	91	28.45	91	28.45	71	29.07	71	29.07	66	14.21	66	14.21
eEye	954	3.15	954	3.15	1753	1.48	1753	1.48	123	16.78	123	16.78	207	4.53	207	4.53
ESET	1546	1.94	1546	1.94	478	5.42	478	5.42	117	17.64	117	17.64	142	6.61	142	6.61
Filseclab	846	3.55	846	3.55	109	23.76	109	23.76	141	14.64	141	14.64	142	6.61	142	6.61
Finport	619	4.85	619	4.85	657	3.94	657	3.94	106	19.47	106	19.47	162	5.79	162	5.79
Fortinet	348	8.63	348	8.63	390	6.64	390	6.64	137	15.07	137	15.07	170	5.52	170	5.52
Frisk	333	9.02	333	9.02	445	5.82	445	5.82	128	16.12	128	16.12	145	6.47	145	6.47
F-Secure Client	1369	2.19	1836	1.64	322	8.04	331	7.82	89	23.19	176	11.73	43	21.82	166	5.65
F-Secure PSB	1384	2.17	1875	1.60	331	7.82	338	7.66	92	22.43	175	11.79	48	19.54	147	6.38
G DATA	863	3.48	863	3.48	327	7.92	327	7.92	197	10.48	197	10.48	167	5.62	167	5.62
K7	170	17.68	NA	NA	245	10.57	245	10.57	35	58.97	35	58.97	40	23.45	40	23.45
Kaspersky	445	6.75	445	6.75	119	21.76	119	21.76	58	35.59	58	35.59	43	21.82	43	21.82
Kingsoft Std	44	68.29	NA	NA	353	7.34	353	7.34	148	13.95	148	13.95	144	6.51	144	6.51
Kingsoft Adv	44	68.29	NA	NA	157	16.49	157	16.49	53	38.94	53	38.94	43	21.82	43	21.82
McAfee Total Security	679	4.43	679	4.43	339	7.64	339	7.64	79	26.13	79	26.13	94	9.98	94	9.98
McAfee VirusScan	82	36.64	560	5.37	369	7.02	363	7.13	111	18.59	98	21.06	123	7.63	117	8.02
Microsoft	1369	2.19	1369	2.19	482	5.37	482	5.37	72	28.67	72	28.67	77	12.18	77	12.18
MWTI	1285	2.34	1285	2.34	1411	1.84	1411	1.84	2235	0.92	2235	0.92	1810	0.52	1810	0.52
Nifty Corp.	1859	1.62	1859	1.62	348	7.44	348	7.44	322	6.41	322	6.41	252	3.72	252	3.72
Norman	1042	2.88	1042	2.88	1687	1.53	1687	1.53	62	33.29	62	33.29	114	8.23	114	8.23
PC Tools AV	1623	1.85	1623	1.85	474	5.46	474	5.46	190	10.86	190	10.86	193	4.86	193	4.86
PC Tools IS	2775	1.08	2775	1.08	402	6.44	402	6.44	127	16.25	127	16.25	102	9.20	102	9.20
PC Tools SD	1472	2.04	1472	2.04	407	6.36	407	6.36	106	19.47	106	19.47	84	11.17	84	11.17
Quick Heal	323	9.30	618	4.86	94	27.55	91	28.45	106	19.47	291	7.09	61	15.38	77	12.18
Rising	1586	1.89	1586	1.89	453	5.72	453	5.72	79	26.13	79	26.13	76	12.34	76	12.34
Sophos	72	41.73	722	4.16	228	11.36	238	10.88	69	29.91	93	22.19	41	22.88	93	10.09
Symantec	488	6.16	512	5.87	210	12.33	263	9.85	156	13.23	151	13.67	97	9.67	97	9.67
Trustport	1018	2.95	1018	2.95	465	5.57	465	5.57	221	9.34	221	9.34	210	4.47	210	4.47
VirusBuster	712	4.22	812	3.70	181	14.31	181	14.31	113	18.27	113	18.27	53	17.70	53	17.70

of vital importance to us, such as stability and logging, seemed excellent, although some scans did present counts of 'warnings' at the end, with no details as to what we had been warned about. Detection remains pretty sketchy, particularly over the polymorphic sets, and there is much work to do to achieve full coverage of the WildList, but false positives were fairly few, and a VB100-worthy product could be achievable by *Finport* given some more work.

Fortinet FortiClient 4.0.1.54

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	64.34%
Worms & bots	100.00%	**False positives**	0

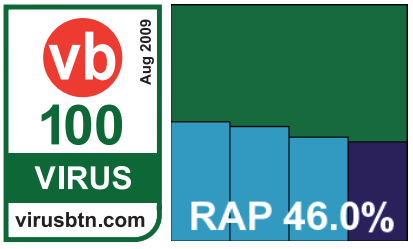


Fortinet presented a pleasantly redesigned interface in the previous test, and it returned this month. Warning messages about unsigned drivers during installation also returned with a vengeance thanks to the UAC system, which had to be disabled to allow the install to complete properly. The design is good though, with an excellent level of configuration and some very thorough default settings befitting its primarily business audience. Some other issues emerged with the UAC interaction, including the requirement to be running as admin to access some system files, which resulted in a standard scan of the C drive halting halfway through. Logging was also a bit of an issue, as what were nice clear records seemed to be compressed and encrypted without notice at one point.

With careful saving of logs the full set of tests were completed and results obtained, showing some mid-range scanning speeds and a considerable improvement in detection over the trojans set from the product's last few appearances. The RAP sets showed much work still to be done, and as in previous tests a quick recheck with the 'extended databases' enabled, along with heuristics and 'grayware' detection, showed a huge improvement but could not be counted for the official scores as all are disabled by default. In the core areas, however, no problems were encountered, with a clean run over the WildList and clean sets, and a VB100 award is duly granted.

Frisk F-PROT Antivirus 6.0.9.1

ItW	100.00%	**Polymorphic**	99.89%
ItW (o/a)	100.00%	**Trojans**	80.49%
Worms & bots	100.00%	**False positives**	0

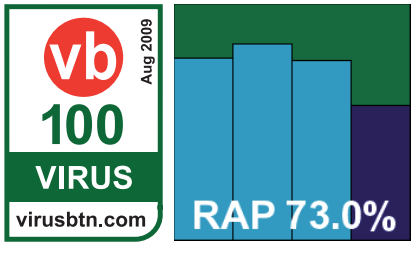


Frisk's nice simple product installs at a reasonable pace and appears to be carrying out a lot of activity after installation, with a lengthy pause observed before the requested reboot was allowed to take place. The simplicity and relative shortage of configuration allows the interface to be clean and easy to use, although in a few places the available options seem a little esoteric. Logging is also fairly sparse, with no obvious recording of on-access detections, and the scanner remains somewhat prone to hangs and crashes; several error messages appeared during bigger scans of both clean and infected sets, and while in some cases a 'continue' button allowed scanning to complete, in others a restart was necessary.

Scanning speeds were only reasonable, and on-access overheads a little on the heavy side. Detection rates were generally pretty decent in the standard sets, although the RAP sets once again left something to be desired, hinting at issues with keeping up with the vast numbers of new samples appearing. The WildList, including the many Virut samples, was handled without issue though, and no problems were encountered in the clean set either, thus earning *Frisk* another VB100 award.

F-Secure Client Security 8.01 build 133

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	94.92%
Worms & bots	100.00%	**False positives**	0



The first of two entries from *F-Secure* this month is the company's standard desktop solution, which seems pretty much unchanged since we first encountered it a few years back. The install is surprisingly quick considering the number of components included, and requires a reboot to complete. The layout is fairly simple to navigate, and has a nice quirky but unfussy look and feel. The thoroughness of the detection took rather a heavy toll on our test systems, which seemed to wear out quite quickly and on a few occasions shut themselves down unexpectedly. We also noted a few issues with the product

File access lag time (Time = s; Lag = s/MB)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag
Agnitum	82	0.03	NA	NA	289	0.10	289	0.10	194	0.08	194	0.08	128	0.11	128	0.11
AhnLab	82	0.03	NA	NA	221	0.08	221	0.08	116	0.04	116	0.04	95	0.07	95	0.07
Alwil	53	0.02	458	0.15	199	0.07	192	0.07	123	0.04	117	0.04	74	0.05	72	0.05
AVG	8	0.00	262	0.09	368	0.14	464	0.17	125	0.04	154	0.06	40	0.02	107	0.09
Avira	37	0.01	195	0.06	108	0.03	216	0.08	77	0.02	98	0.03	35	0.01	66	0.04
CA eTrust	42	0.01	NA	NA	92	0.03	92	0.03	85	0.03	85	0.03	57	0.03	57	0.03
CA ISS	46	0.01	NA	NA	107	0.03	107	0.03	105	0.03	105	0.03	173	0.16	173	0.16
eEye	80	0.03	287	0.09	335	0.12	331	0.12	162	0.06	163	0.06	195	0.18	212	NA
ESET	23	0.01	NA	NA	170	0.06	170	0.06	165	0.06	165	0.06	168	0.15	168	0.15
Filseclab	29	0.01	NA	NA	60	0.02	NA	NA	93	0.03	NA	NA	45	0.02	NA	NA
Finport	236	0.08	236	0.08	352	0.13	352	0.13	32	0.00	32	0.00	30	0.00	30	0.00
Fortinet	332	0.11	332	0.11	512	0.19	512	0.19	142	0.05	142	0.05	181	0.17	181	0.17
Frisk	99	0.03	NA	NA	485	0.18	485	0.18	153	0.06	153	0.06	163	0.15	163	0.15
F-Secure Client	55	0.02	1700	0.56	472	0.18	497	0.19	187	0.07	245	0.10	182	0.17	259	0.25
F-Secure PSB	41	0.01	1706	0.57	318	0.12	487	0.18	177	0.07	237	0.10	180	0.17	250	0.24
G DATA	4	0.00	1418	0.47	186	0.07	548	0.20	278	0.12	300	0.13	277	0.27	282	0.27
K7	93	0.03	NA	NA	255	0.09	255	0.09	57	0.01	57	0.01	53	0.03	53	0.03
Kaspersky	25	0.01	490	0.16	130	0.04	125	0.04	103	0.03	112	0.04	64	0.04	84	0.06
Kingsoft Std	42	0.01	NA	NA	380	0.14	380	0.14	179	0.07	179	0.07	178	0.16	178	0.16
Kingsoft Adv	14	0.00	NA	NA	169	0.06	169	0.06	81	0.02	81	0.02	55	0.03	55	0.03
McAfee Total Security	45	0.01	NA	NA	213	0.08	213	0.08	117	0.04	117	0.04	120	0.10	120	0.10
McAfee VirusScan	48	0.01	535	0.18	376	0.14	355	0.13	117	0.04	112	0.04	121	0.10	120	0.10
Microsoft	145	0.05	NA	NA	482	0.18	482	0.18	86	0.03	86	0.03	85	0.06	85	0.06
MWTI	350	0.12	580	0.19	271	0.10	297	0.11	69	0.02	81	0.02	61	0.04	92	0.07
Nifty Corp.	39	0.01	NA	NA	315	0.12	315	0.12	155	0.06	155	0.06	175	0.16	175	0.16
Norman	61	0.02	NA	NA	245	0.09	245	0.09	88	0.03	88	0.03	96	0.08	96	0.08
PC Tools AV	NA	NA	NA	NA	682	0.26	682	0.26	220	0.09	220	0.09	361	0.36	361	0.36
Quick Heal	24	0.01	NA	NA	73	0.02	NA	NA	98	0.03	NA	NA	35	0.01	NA	NA
Sophos	44	0.01	663	0.22	233	0.08	248	0.09	80	0.02	98	0.03	61	0.04	89	0.07
Symantec	38	0.01	NA	NA	178	0.06	178	0.06	116	0.04	116	0.04	63	0.04	63	0.04
Trustport	314	0.10	NA	NA	774	0.29	774	0.29	269	0.11	269	0.11	266	0.26	266	0.26
VirusBuster	30	0.01	NA	NA	193	0.07	199	0.07	61	0.01	109	0.04	36	0.01	73	0.05

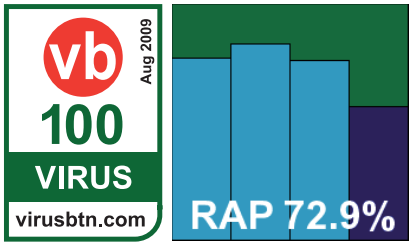
itself, which seemed to lose touch with its controls, the 'scan target' button regularly failing to bring up the required dialog if clicked on too soon after the completion of a scan. The thoroughness of the standard settings led to some rather slow scanning speeds, but on access, rather surprisingly, the product relies on file extensions to determine what to scan.

With the speed tests handled, the infected sets proved more difficult thanks to the rather shaky logging that has been mentioned in the past. This seemed less serious an issue this time though, and complete logs were obtained with only minimal moderation of scan sizes, with reboots in between scans used to circumvent the issue of the failing

scan button. The final results showed a handful of samples of recent Virut variants missed in the polymorphic set, but no problems with the WildList strain. Detection rates overall were excellent, with a pretty decent showing in the RAP sets, and with no false positives either *F-Secure* earns a VB100 award.

F-Secure PSB Workstation Security 8.00 build 245

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	94.66%
Worms & bots	100.00%	**False positives**	0

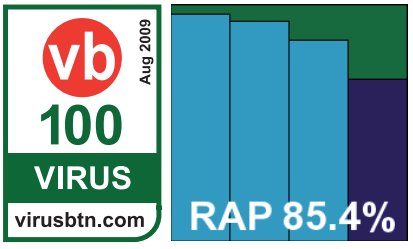


This is a more corporate-oriented version of the *F-Secure* product, '*PSB*' standing for '*Protection Services for Business*'. On the surface it seems much the same as the *Client Security* (*CS*) product, with a rather slower install process interrupted by a UAC warning about an unidentified publisher. Although we had to refuse its request to connect to the Internet to validate itself, all appeared to be running just fine, and pretty similar results to the *CS* version were found in the speed tests.

Running the product over the infected sets, perhaps overconfident after some luck with the *CS* version, we once again ran into the dreadful logging issues previously discussed. With a scan of any length producing more than a few hundred notable events, the log viewing process seems unable to cope and produces heavily truncated logs. In a business environment this would be unacceptable, and it made things pretty tricky for us – once again forcing us to carry out a time-consuming series of cautiously small scans. Eventually, after many frustrating reruns of tests in an attempt to find a viable set size, the data was gathered, and provided much the same results as the *Client* version – overall very thorough detection rates and no false positives, thus earning *F-Secure* a second VB100 award. The experience was not the most pleasant, however, and we will be looking closely at our rules on logging accuracy for future tests.

G DATA AntiVirus 2010 20.0.4.46

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.57%
Worms & bots	100.00%	**False positives**	0

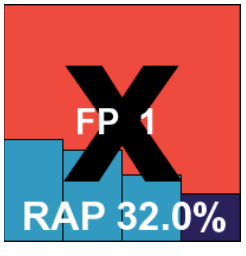


G DATA's installation was a little slow, and forced a restart on completion. The interface is sleek and stylish and provides a fair level of configuration, although more experienced users may wish for more control over the behaviour. The multi-engine product has some seriously thorough default settings and took some time plodding through the tests. It also took a heavy toll on system resources, on a couple of occasions causing unexpected shutdowns. Scanning speeds were thus rather slow, with some pretty hefty lag times on access too. Logging also proved a little fiddly.

Detection rates were impressive however, with virtually nothing missed in the standard sets and an overall average in the RAP sets of over 85%. With full detection of the WildList and no false positives, *G DATA* easily wins another VB100 award.

K7 Total Security Desktop 9.8.009

ItW	100.00%	**Polymorphic**	87.45%
ItW (o/a)	100.00%	**Trojans**	82.29%
Worms & bots	99.78%	**False positives**	1

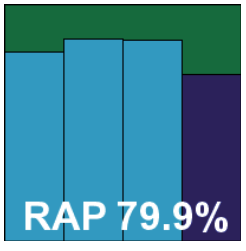


K7 has had a bit of a rollercoaster ride in the VB100 in the couple of years since it became a semi-regular entrant, with some excellent detection levels tempered by the odd unexpected drop and an occasional false positive. The product itself is hard to dislike, with a swift and simple install process requiring no reboot, and a colourful, easy-to-navigate interface with sensible defaults and a reasonable degree of configuration for a home-user product.

It zipped through the speed tests in pretty good time, and achieved some very good detection rates in the standard sets, although the RAP scores were a little down on previous performances. In the clean sets, a single file was misidentified as malware, a component of a suite of mobile phone software from *Sony Ericsson*. This is unfortunate for *K7*, as the sample in question is unlikely to trouble users in the company's key market of Japan, but under the strict rules of the VB100 any false positive is enough to spoil a product's chances of qualification, and *K7* will have to wait a while to earn another VB100 award.

Kaspersky Anti-Virus 2009 8.0.0.506

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	97.06%
Worms & bots	99.87%	**False positives**	0

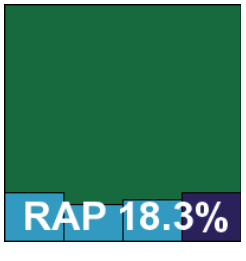


Kaspersky's current product is a stylish and attractive beast, with a lovely shiny interface that is a pleasure to explore and provides plenty of data on the activities of its various components in the form of eye-catching graphs and charts. Set-up is not too complex and configuration is ample without becoming overwhelming. Despite some pretty thorough defaults, scanning proceeded at a good pace and on-access overheads didn't seem too heavy. The intensity did show itself a few times however, with a number of unexpected shutdowns as experienced with a few other products this month.

With a little care taken not to overtax the product, these issues were soon overcome, and results were easily gathered. These showed things to be much as expected, with most scores a notch or two better than other products using the same engine – especially in the RAP week +1 set where a truly excellent level was attained. A couple of recent Viruts went undetected, but precious little else, and with the WildList and clean sets handled ably, a VB100 award is easily earned.

Kingsoft Internet Security 2009 Standard 2008.11.6.63

ItW	99.99%	**Polymorphic**	58.96%
ItW (o/a)	99.99%	**Trojans**	62.40%
Worms & bots	99.76%	**False positives**	0

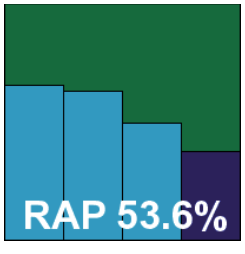


Kingsoft's 'Standard' product has appeared in our tests before. This time it looked much the same, with a fairly standard install process that is not too taxing on the user, and a simple set-up wizard for basic configuration. The interface is well designed with a tabbed set-up which keeps all the required controls in easy reach.

Scanning speeds were fairly mediocre, and results likewise; the standard sets were handled fairly well, with some work needed on polymorphic viruses. Perhaps the best that can be said of the RAP figures is that they are consistent. No false positives were observed in the clean sets, but the trouble with polymorphic viruses extended to the Virut variant in the WildList set, and thus no VB100 award is granted for this performance.

Kingsoft Internet Security 2009 Advanced 2008.11.6.63

ItW	100.00%	**Polymorphic**	60.74%
ItW (o/a)	100.00%	**Trojans**	87.12%
Worms & bots	99.77%	**False positives**	0

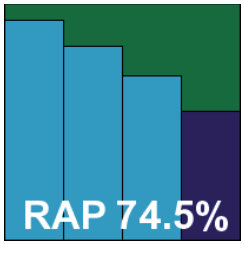


Kingsoft's advanced product has shown some slight superiority to the standard edition before, although on the surface it all seems much the same, with an identical appearance and no visible mention of its separate designation noted during install or use.

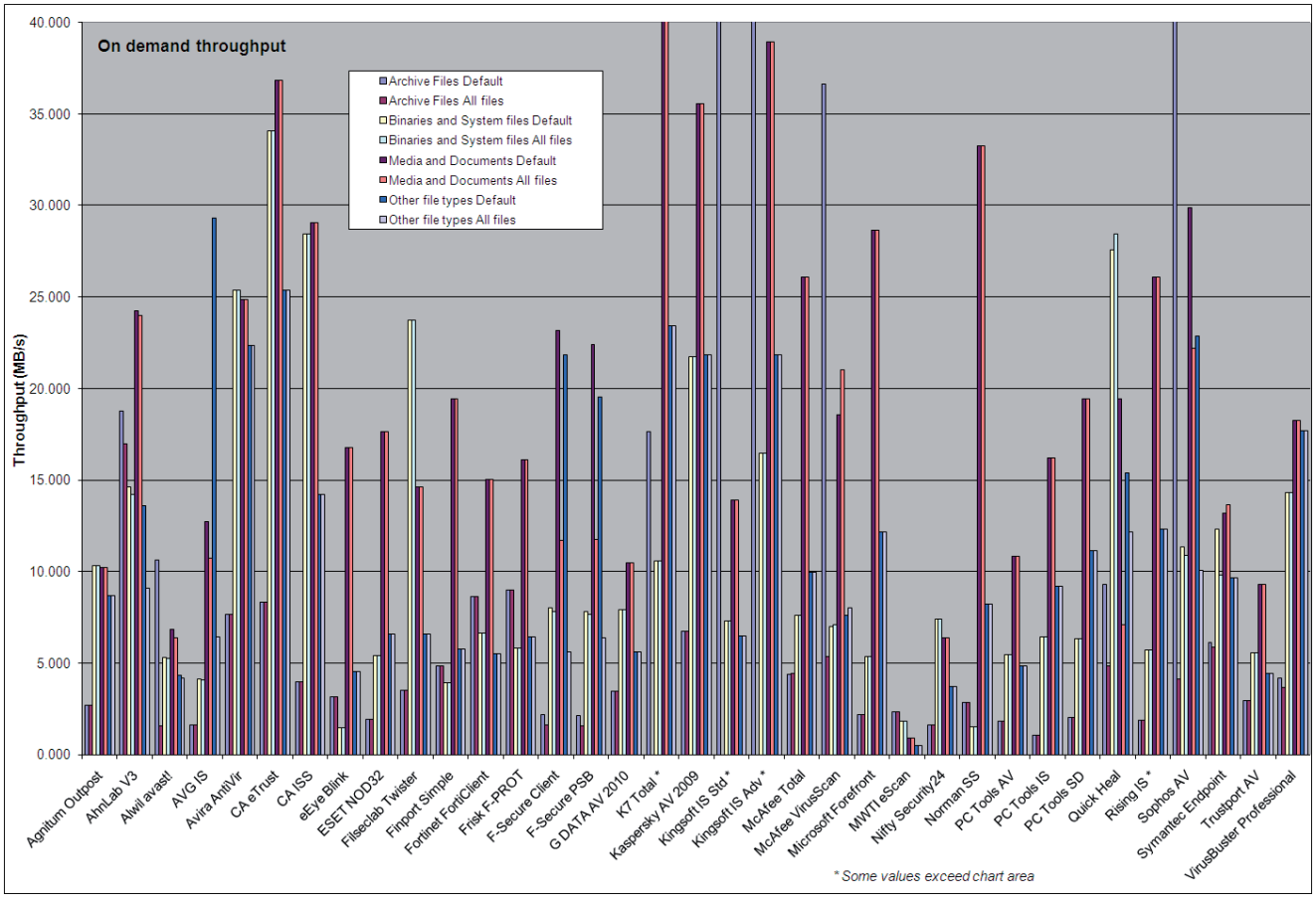
Once again, we quickly noticed that things were moving much faster this time, both in the install process as well as in both sections of the speed test, and when the detection results were processed we saw a considerable improvement here as well. Polymorphic detection rates were up, and a very creditable score was achieved in the trojans set. Even the RAP sets produced some decent figures, all without causing any new false alarms. The polymorphic improvement extended to full coverage of the Virut variant on the WildList, and for this edition *Kingsoft* earns a VB100 award.

McAfee Total Security 13.111.102

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.64%
Worms & bots	100.00%	**False positives**	0



This is the first appearance for the home-user version of *McAfee*'s product, but it is not entirely unfamiliar; having found it installed on a laptop received as a gift, I have spent some time wrestling with its Machiavellian removal process. For those not blessed

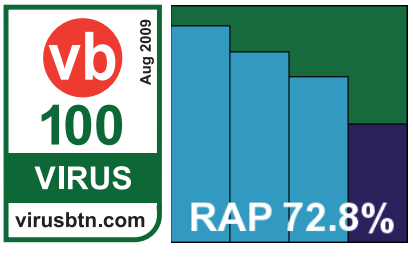


with a free trial copy on new hardware, the product installs entirely from the Internet, so may not be suitable for anyone who likes to have their system protected at all times when connected to the wild wild web. The interface is curvy and colourful and fairly appealing at first sight, but navigation through what appears to be a wealth of options proved to be extremely difficult and rather disappointing – many of the controls we would have liked were either absent or too well hidden for the likes of us to discover. Problems with the destruction of our samples as well as some quirky on-access behaviour were overcome by careful analysis, sneaky workarounds and appeals to the developers for assistance. We eventually managed to get to the end of testing, though hampered once again by a number of surprise halts of the test system, generally in the middle of a long scan.

Checking over the results also proved something of a chore, as logging – once we had removed the rather low default size limit – seemed rather flaky, producing mangled tests with lines crushed together, seemingly random use of case and other quirks. Satisfactory results were eventually obtained after multiple retests, and showed the expected very solid levels of detection, though with a fairly steady decline through the RAP sets as samples grew fresher. No problems were encountered with the WildList and no false positives emerged either, and a VB100 award is thus granted.

McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.69%
Worms & bots	100.00%	**False positives**	0

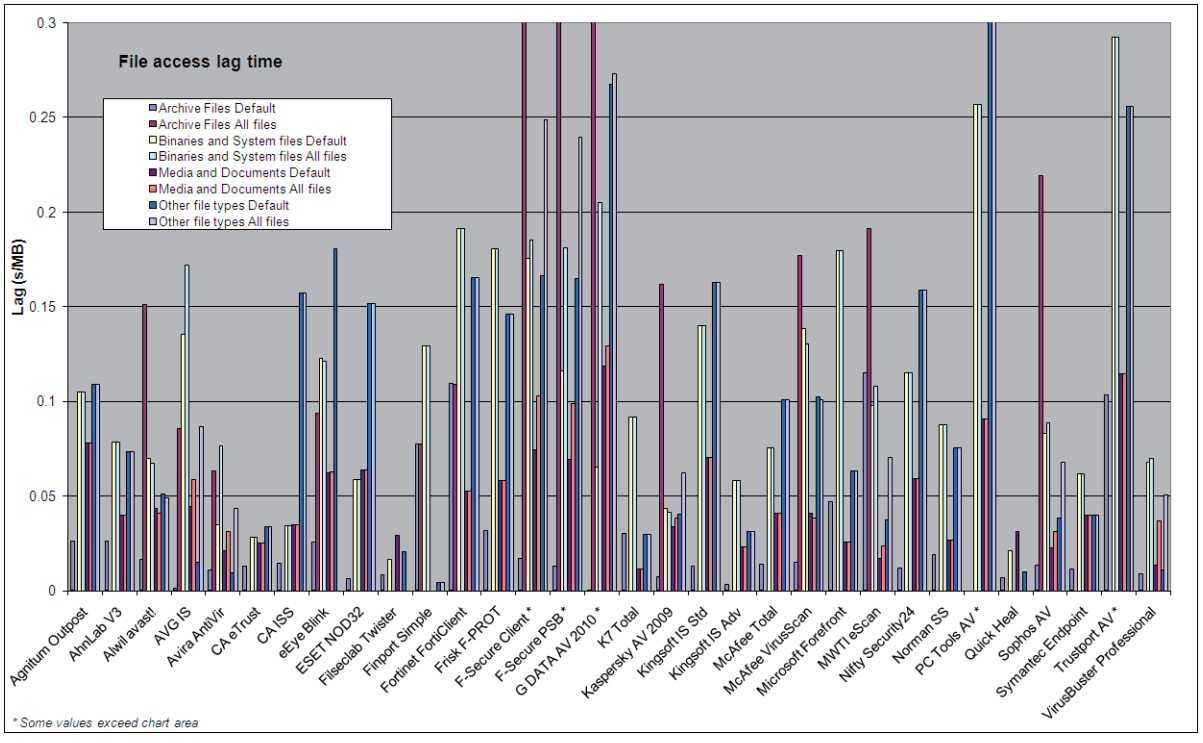


McAfee's corporate product is more familiar, and a welcome sight after its somewhat wayward sibling. Everything here is much more simple and businesslike, providing a much more satisfactory level of control, yet somehow making it more accessible and navigable. It has remained the same for many years

Archive scanning		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
Agnitum Outpost	Default	2	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
AhnLab V3 Internet Security	Default	X	√	X	X	√	√	X	√	√
	All	X	X	X	X	X	X	X	X	√
Alwil avast!	Default	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
	All	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
AVG Internet Security Edition	Default	X	√	6	√	√	√	√	√	X/√
	All	X	X	X	X	X	X	X	X	X/√
Avira AntiVir	Default	√	√	√	√	√	√	√	√	√
	All	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
CA eTrust ITM	Default	X	√	X	√	√	√	√	√	√
	All	X	X	X	1	X	X	X	1	√
CA Internet Security Suite	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	1	X	X	X	1	√
eEye Blink	Default	X	1	√	1	1	1	8	2	√
	All	X	X	X	X	X	X	X	X	√
ESET NOD32	Default	√	√	√	√	√	√	5	√	√
	All	X	X	X	X	X	X	X	X	√
Filseclab Twister AntiTrojanVirus	Default	5	3	3	4	1	4	X	5	√
	All	X	X	X	X	X	1	X	2	X
Finport Simple	Default	X	√	X	√	X	√	X	√	√
	All	X	√	X	X	X	√	X	√	√
Fortinet FortiClient	Default	X	√	√	√	√	√	√	4	√
	All	X	√	√	√	√	√	√	4	√
Frisk F-PROT Antivirus	Default	1	√	√	√	√	√	√	√	√
	All	X	X	2	2	X	X	X	2	√
F-Secure Client Security	Default	X/√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
F-Secure PSB Workstation Security	Default	X/√	√	√	√	√	√	√	√	X/√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
G DATA AntiVirus 2010	Default	√	√	√	√	√	√	√	√	√
	All	√	√	4/√	√	√	√	8/√	8/√	√
K7 Total Security	Default	X	X	X	1	1	1	X	1	√
	All	X	X	X	X	X	X	X	X	√
Kaspersky Anti-Virus 2009	Default	X	√	√	√	√	√	X	√	√
	All	X	4	1	4	4	5	X	2	√
Kingsoft Internet Security 2009 Standard	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Kingsoft Internet Security 2009 Advanced	Default	X	X	X	X	X	X	X	X	√
	All	X	X	X	X	X	X	X	X	√
McAfee Total Security	Default	2	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
McAfee VirusScan	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	X	1	X	X	X	1	√
MWTI eScan Internet Security Suite	Default	√	√	8	√	√	√	8	√	√
	All	X	X	8	√	X	X	X	X	√
Nifty Corp. Security24	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Norman Security Suite	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
PC Tools AntiVirus	Default	2	√	√	√	X	√	√	√	√
	All	2	√	√	√	X	√	5	√	X
PC Tools Internet Security 2009	Default	2	√	√	√	X	√	√	√	√
	All	2	√	√	√	X	√	5	√	X
PC Tools Spyware Doctor	Default	2	√	√	√	X	√	√	√	√
	All	2	√	√	√	X	√	5	√	√
Quick Heal AntiVirus Lite	Default	X/2	X/5	X	2/5	X	2/5	X/1	2/5	X/√
	All	X	X	X	X	X	X	X	X	X
Rising Internet Security 2009	Default	1	√	√	√	√	√	√	√	√
	All	X	√	√	√	√	√	√	√	√
Sophos Anti-Virus	Default	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	All	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	Default	3/√	3/√	3/√	3/√	3/√	3/√	1/5	3/√	√
	All	X	X	X	X	X	X	X	X	√
Trustport Antivirus 2009	Default	X	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
VirusBuster Professional	Default	2	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	X/√

Key:
X - Archive not scanned
√ - Archives scanned to depth of 10 or more levels
*Executable file with randomly chosen extension

X/√ - Default settings/thorough settings
[1-9] - Archives scanned to limited depth

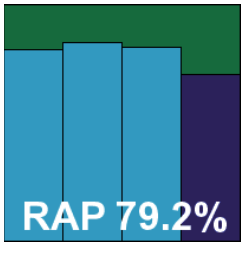


now, but the developers seem to be sticking to the principle 'if it ain't broke, don't fix it' (most sensibly in our opinion). The only minor issue we noted during testing was that the on-access protection seemed to shut down momentarily when the settings were changed, perhaps only for a few seconds but long enough for us to notice it by running our on-access test scripts too soon after an adjustment.

No problems were encountered with the stability of the product or the test system, and as would be expected from a serious business product all detection activity is faithfully and accurately recorded. Detection rates seemed closely comparable with the home-user product. A few fractionally lower scores could be attributed to the offline updater package provided for the test being a few hours older than the updates applied to the home-user product during its brief time connected to the Internet on the deadline day. Again no problems were encountered with the WildList, and no false positives were generated either, thus *McAfee* earns a second VB100 award this month.

Microsoft Forefront Client Security 1.5.1972.0

ItW	100.00%	**Polymorphic**	99.51%
ItW (o/a)	100.00%	**Trojans**	95.95%
Worms & bots	100.00%	**False positives**	0



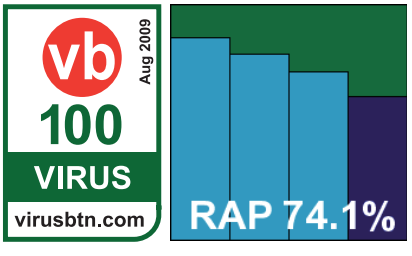
Microsoft's corporate product is here on its own this month, with *OneCare* on its way into retirement and the replacement, code named *Morro* but apparently now to be referred to as '*Security Essentials*', anticipated very soon. *Forefront*'s install process is rather different for us than for standard users thanks to the set-up of our lab. This made for a rather complex process with multiple reboots, but the standard set-up should, one hopes, be rather smoother and less laborious. The product has a pretty basic interface with extremely limited configuration, including the rather cryptic option to 'use the program', which apparently provides the option to shut it down completely if required. With response to clicks somewhat sluggish, and set-up of scans not as simple as some, we would normally have been tempted to resort to using the context menu scan (which has become something of a standard these days), but here for some reason it does not appear to be provided.

Nonetheless, we ploughed through testing without significant issues, although the 'History' option appears to be rather unreliable, on many occasions spending several

minutes pondering after a lengthy scan only to present a blank screen and a message implying no detections had been recorded from a scan discovering several tens of thousands of infected files. Thankfully, full and reliable logging is buried in the product's file structure, in a folder which *Vista* warned we should not be probing into but which was found thanks to some tips received from the developers. Parsing these showed some superb detection rates, continuing a long-term upward trend in the product's prowess, with the RAP week +1 detection particularly noteworthy as the highest of any product tested this month. The WildList was handled without problems, although once again a fair number of the additional Virut sub-strains added to our polymorphic set this month were missed. This does not affect certification though, and with no false positives encountered *Microsoft* more than deserves its VB100 award.

MWTI eScan Internet Security Suite 10.0.985.449

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



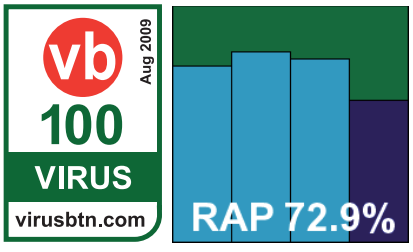
Microworld's *eScan* product has been settling in fairly well since the decision to rely entirely on the company's own detection technology. The current version has a nice simple install process, which somehow feels a little old-fashioned next to some of the super-slick products appearing of late, and produces a few unexpected pop-ups of unpredictable appearance during the process, as well as lingering for several minutes at the 'finishing' stage.

Once up and running though, things are nicely laid out and simple to navigate, with a decent level of options. On-demand scanning is remarkably slow, perhaps not helped by the default option to log details of every item scanned rather than only infected or otherwise troublesome files, but on-access overheads seemed fairly light by comparison and there were no issues with stability.

Detection rates were most commendable, with no issues at all in the WildList, worms and bots or polymorphic sets, and precious few misses in the trojans set either. The RAP test was handled with considerable style, and with no false positives uncovered in the rather bulky logs of the clean sets, a VB100 award is duly granted.

Nifty Corporation Security24 5.30

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	95.21%
Worms & bots	100.00%	**False positives**	0



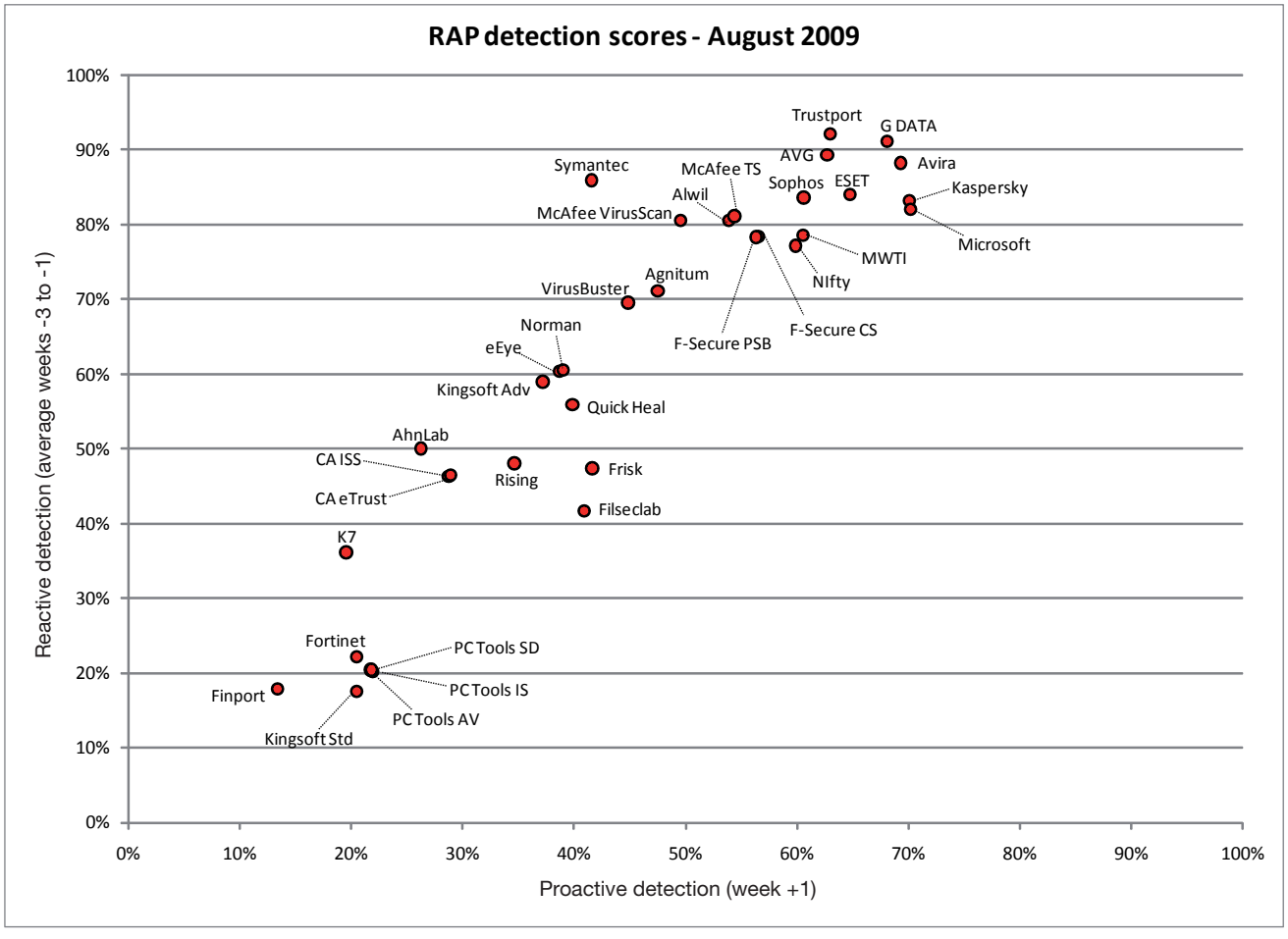
A newcomer to the VB100 this month, representatives of Japan's *Nifty Corporation* contacted us not long before the test deadline and bravely put their product on the line. With no English translation, we used the standard Japanese-language product – with a user guide kindly provided by the developers and a Kanji dictionary to hand to look up any troublesome words in the interface. Unable to provide an offline updater, we were forced to install the product on the deadline date, update and take a snapshot for later transfer to the test systems, but this proved no big deal, with a smooth and easy installation and a fast, straightforward update process.

The main interface is quite attractive, and is a little unusual compared to much of the rest of the market, but this is of little surprise. Even with the Japanese characters only partially rendered on our English-language systems it seemed fairly simple to navigate based on recognition of standard iconography and a basic if rather rusty understanding of the writing system. Logging is fairly minimal by default, but a simple registry tweak provides more detailed records to be passed to the event log, from where the required information was gathered without difficulty. The product is based on the *Kaspersky* engine, and thus, as one would expect, provides an excellent level of detection across the board, along with some impressive stability under pressure, although the thoroughness is naturally tempered by some rather slow scanning speeds and perhaps less than ideal on-access overheads. With no problems encountered in any of the test sets, the *Nifty Corporation* takes away a VB100 award at its first attempt, and we look forward to its return.

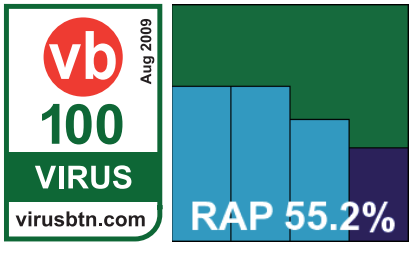
Norman Security Suite 7.10

ItW	100.00%	**Polymorphic**	83.74%
ItW (o/a)	100.00%	**Trojans**	86.28%
Worms & bots	100.00%	**False positives**	0

Norman's current suite installs rapidly and easily, with the only tricky question during the process being whether or



not to enable the 'Screen saver scanner', designed to run a scan when the system is idle. Although on by default, we opted to disable this in case it interrupted our normal testing. The end of the process suggests that a reboot may be necessary once the attempt to update has completed. This was indeed the case, with a small and rather subtle pop-up prompting for the restart a minute or two after the install proper was done.



The interface itself greatly resembles that of the *Norman* appliance product reviewed in these pages last month (see *VB*, July 2009, p.21), making for a nice consistency across products. However, it seemed a little sluggish to respond at times, perhaps in part thanks to the general slowness observed in the browser rendering on which it relies. Navigation could not be simpler though, and with a fairly minimal set of controls little time was spent using the interface.

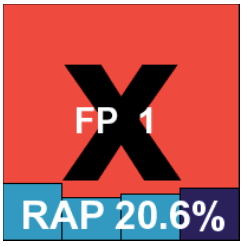
With no obvious option to set up scans of specific areas from within the GUI, context-menu scans were used for all on-demand tests. On a few occasions, returning to the GUI to check settings after a hefty scan found it whited-out and failing to respond, and in most cases a reboot was required to regain control, but protection seemed stable throughout. Rather amusingly, even while the main GUI is in this state, the licensing wizard – which has long been a regular feature during tests of *Norman* offerings, popping up every so often to pester the user into fully licensing the product – is blocked by the UAC system and requires user confirmation to commence its nagging.

Scanning speeds were generally pretty good, and detection rates decent, with a notable dip in coverage in the most recent parts of the RAP sets. Although a handful of the new Virut samples in the polymorphic set were missed even with the *Sandbox* system enabled, none of the WildList samples went undetected, and without false positives either, *Norman* earns a VB100 award.

Reactive And Proactive (RAP) detection scores	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1		week +1	
Agnitum Outpost Security Suite Pro	72.29%	72.88%	68.31%	71.16%	47.51%	65.24%
AhnLab V3 Internet Security	59.12%	58.47%	32.55%	50.05%	26.27%	44.10%
Alwil avast! Professional	84.77%	83.79%	73.39%	80.65%	53.91%	73.97%
AVG Internet Security	87.27%	92.05%	88.69%	89.34%	62.72%	82.68%
Avira AntiVir Professional	85.63%	91.95%	87.33%	88.30%	69.34%	83.56%
CA eTrust ITM	48.89%	45.91%	44.05%	46.28%	28.78%	41.91%
CA Internet Security Suite	48.89%	46.12%	44.43%	46.48%	28.93%	42.09%
eEye Blink Professional	64.94%	65.42%	50.97%	60.44%	38.67%	55.00%
ESET NOD32 Antivirus	86.88%	84.29%	81.07%	84.08%	64.76%	79.25%
Filseclab Twister AntiTrojanVirus	40.60%	41.40%	43.03%	41.68%	40.92%	41.49%
Finport Simple Anti-Virus	18.32%	19.98%	15.24%	17.85%	13.43%	16.75%
Fortinet FortiClient	24.85%	21.81%	19.69%	22.12%	20.49%	21.71%
Frisk F-PROT Antivirus	50.24%	48.38%	43.61%	47.41%	41.64%	45.97%
F-Secure Client Security	76.93%	82.62%	75.77%	78.44%	56.55%	72.97%
F-Secure PSB Workstation Security	76.83%	82.60%	75.71%	78.38%	56.32%	72.86%
G DATA AntiVirus 2010	95.89%	92.78%	84.82%	91.17%	68.12%	85.40%
K7 Total Security Desktop	42.77%	38.07%	27.56%	36.13%	19.56%	31.99%
Kaspersky Anti-Virus 2009	79.71%	85.12%	84.82%	83.22%	70.09%	79.94%
Kingsoft Internet Security 2009 Standard	20.06%	15.37%	17.21%	17.55%	20.49%	18.28%
Kingsoft Internet Security 2009 Advanced	65.30%	62.69%	49.09%	59.03%	37.23%	53.58%
McAfee Total Security	92.78%	81.71%	69.13%	81.21%	54.40%	74.51%
McAfee VirusScan Enterprise	91.45%	80.38%	69.96%	80.60%	49.55%	72.83%
Microsoft Forefront Client Security	80.91%	83.56%	81.96%	82.15%	70.19%	79.16%
MWTI eScan Internet Security Suite	85.81%	78.82%	71.13%	78.59%	60.55%	74.08%
Nifty Corp. Security24	74.25%	80.12%	77.29%	77.22%	59.88%	72.89%
Norman Security Suite	65.07%	65.50%	51.10%	60.56%	39.03%	55.17%
PC Tools AntiVirus 2009	23.63%	17.74%	19.21%	20.19%	21.96%	20.64%
PC Tools Internet Security 2009	23.78%	18.11%	19.31%	20.40%	21.70%	20.72%
PC Tools Spyware Doctor	23.83%	18.16%	19.34%	20.44%	21.85%	20.80%
Quick Heal AntiVirus Lite 2009	61.62%	62.01%	44.08%	55.90%	39.86%	51.89%
Rising Internet Security 2009	55.60%	55.13%	33.44%	48.06%	34.67%	44.71%
Sophos Anti-Virus	83.59%	88.38%	79.01%	83.66%	60.63%	77.90%
Symantec Endpoint Protection	92.06%	87.91%	78.02%	86.00%	41.59%	74.90%
Trustport Antivirus 2009	93.88%	95.10%	87.55%	92.18%	63.03%	84.89%
VirusBuster VirusBuster Professional	70.45%	71.37%	67.01%	69.61%	44.87%	63.42%

PC Tools AntiVirus 2009 6.0.0.19

ItW	99.93%	**Polymorphic**	69.77%
ItW (o/a)	99.95%	**Trojans**	67.49%
Worms & bots	99.85%	**False positives**	1



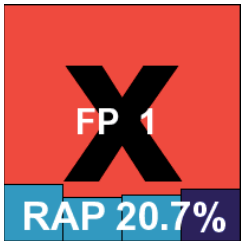
The first of three entries this month from *PC Tools*, the plain vanilla AV product has long been the favourite of the range with us, mostly thanks to its relative ease of use and adherence to standard anti-malware functionality. The install is fairly quick, although there is a rather worrying pause at the end before the product finally appears. It has a pretty simple layout, and very little by way of configuration, which is always somewhat worrying to us. The on-access tests proceeded with ease, however, trundling through the speed tests in fairly sluggish time and showing quite some slowdown in the general responsiveness of the test system. Once we reached the infected sets, things got rather worse, with the on-access scan holding up for a few dozen samples before shutting itself down with a rather limp error message (perhaps overwhelmed by the cascade of alert messages it insisted on flooding down one side of the screen). This happened on numerous occasions, requiring at least one and occasionally several reboots to get the engine to reload and resume protection.

With much care though, we managed to get through the on-access tests with reasonable success, and the on-demand tests proved much smoother and more straightforward. On final analysis, detection levels were mediocre, with the RAP scores particularly low (but at least consistently so) across the weeks. The WildList was mostly handled well, but with a little under half of the samples of the new Virut variant missed, and a single false positive in the clean sets too, no VB100 award is forthcoming despite all our testing efforts.

PC Tools Internet Security 2009 6.0.1.441

ItW	99.93%	**Polymorphic**	69.78%
ItW (o/a)	99.95%	**Trojans**	67.92%
Worms & bots	98.88%	**False positives**	1

The second *PC Tools* offering is the company's complete suite, combining the anti-malware protection of the preceding product with additional anti-spyware and firewalling. The install is fairly similar, with a reminder to remove any competing products and the offer of a 'browser defender' toolbar. The interface looks much the same but is even shorter on controls for the anti-malware component, perhaps in part thanks to the additional modules taking up valuable space. This time we opted to run the on-demand tests first and these proved much as expected, with some slight improvements over the plain AV product in some areas but, rather surprisingly, some areas less well covered. We had a few moments of worry when we found that the log was fixed at a maximum size, but alternative logging was shown to be available as part of the 'community' program, designed to record data more accurately for the developers' use.



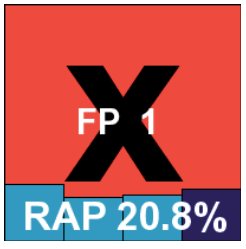
Approaching the on-access scan with some caution, we soon found that although the process clearly states that it 'monitors and blocks' the launching, accessing, copying or moving of malicious items, it actually appears to do none of these. Our standard on-access tool, which performs a simple open on the test files, provoked no response, and copying around the system seemed similarly ineffective. We eventually noted some pop-ups and logged items, and the occasional denial of read or write privileges, and in the end resorted to a combination of copying around the local system, and copying to the system across the network. The VB100 rules do not require blocking, only evidence that a malicious file has been noticed, so we were able to cobble results together from a combination of the product's internal logs, and by counting the files successfully written to, denied access to, disinfected etc. This was by no means simple, as pop-ups and log entries continued to appear – claiming to have intercepted and blocked something – up to three hours after the supposed blocking had taken place. The results gathered may thus be somewhat inaccurate, but only to the extent that the product was, and they tallied at least reasonably closely with those of the plain AV product, with again the missed Virut in the WildList and a single false positive being more than enough to deny the product a VB100 award.

PC Tools Spyware Doctor 6.0.1.441

ItW	99.93%	**Polymorphic**	69.78%
ItW (o/a)	99.95%	**Trojans**	67.92%
Worms & bots	100.00%	**False positives**	1

Testing *PC Tools*' mid-level product, a combination of the plain anti-virus with the company's longer-standing anti-spyware solution, was much the same fiddly, frustrating and occasionally frightening experience as testing the suite (from which it seems to differ only in the provision of a firewall). This time, a *Google* toolbar is offered during installation, for those who feel their browser does not have enough gadgets and gizmos. Otherwise, the interface,

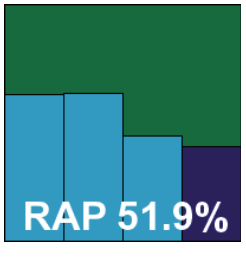
controls and layout are much the same.



Again, on-demand testing proved reasonably straightforward and reliable, and on-access scanning rather confusing and short of that all-important sense of security. Scores were once again gathered using multiple moving around of test sets and botched together from untrustworthy logs and analysis of file sets for changes, and should again be treated as unreliable thanks to the extreme difficulty of obtaining repeatable results. Extra care was taken with the WildList samples to ensure complete accuracy, and eventually we achieved a score directly matching the suite – fairly large numbers of the Virut strain not detected. Coupled with the same false positive as the other two offerings, none of *PC Tools*' trio of entries manages to win a VB100 award this month.

Quick Heal AntiVirus Lite 2009 10.00 SP1

ItW	100.00%	**Polymorphic**	98.23%
ItW (o/a)	100.00%	**Trojans**	89.50%
Worms & bots	99.80%	**False positives**	0

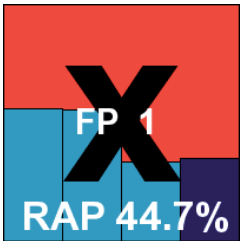


Quick Heal's installer is pretty unusual in providing a little scan of the core system even before installation commences, and runs through its set-up in good time. The interface is unchanged from the last few tests, being fairly plain and simple to navigate but with a few quirks rendering some useful items rather obscure, and the whole is generally slightly sluggish to respond.

Scanning itself is lightning-fast as usual, more notably so over infected files than in the clean sets used for the official speed measurements, which come out as no more than good. Detection rates have lagged behind somewhat in recent tests but here were pretty good, with a fairly sharp drop in the last few weeks of the RAP sets. No problems were encountered with any Virut samples, and with no false alarms either *Quick Heal* earns a VB100 award.

Rising Internet Security 2009 21.43.41

ItW	99.99%	**Polymorphic**	72.98%
ItW (o/a)	99.99%	**Trojans**	79.92%
Worms & bots	99.91%	**False positives**	1

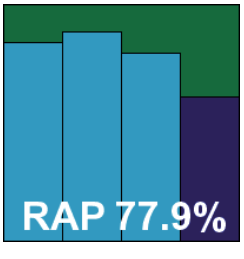


Rising's suite product has quite an involved and lengthy installation process, starting off with some serious warnings from the UAC system and a choice of languages, followed by complex licensing, a selection of installation options, a momentary disconnection from the LAN and a reboot. Once up, with the trademark cartoon lion prancing around in the corner of the screen, the main interface is fairly clear and usable, with the unusual but sensible precaution of a CAPTCHA being presented when important settings are changed, to ensure the action is intentional and not caused by a malevolent presence.

Unlike most other products, on-access protection is not sparked by simple file access, so detection was measured by copying files to the system, which meant that standard on-access overhead measurement was not possible. Logging was also rather odd, taking the form of databases rather than easily read and parsed plain text, but a fairly reliable log processor helped skirt around this even with large amounts of data to handle. In the end, fairly decent scores were observed in the standard sets, dropping in steps through the more recent samples in the RAP sets. Thanks to incomplete coverage of the latest Virut samples in the WildList and a single false positive in the clean sets, however, *Rising* does not quite make the grade for a VB100 award this month.

Sophos Anti-Virus 7.68

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.01%
Worms & bots	100.00%	**False positives**	0



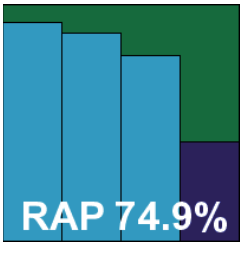
The main component of *Sophos*'s *Endpoint Security and Control* product, *Sophos Anti-Virus* continues to stick to the tried and trusted interface design which has graced many a VB100 in recent years. The installation is somewhat long-winded, offering removal of third-party software and the option of a firewall among its many stages. Once up and running, confirmation of a UAC pop-up is required before the main GUI can be accessed – and also, perhaps more surprisingly, before a context-menu scan is carried out. As ever, configuration is available in extreme depth for those seeking it, and options are generally easy to find and apply, and no issues with stability were

encountered. We have previously mentioned issues with the progress bar as our main gripe about this product, but this time, in line with a general theme developing this month, we thought we should mention the rather awkward logging set-up. While it seems somewhat petty to complain about excessive detail, the product does produce a large, rather confusing log, with no option to record results of a particular scan to a particular location, and no option to purge existing data. This may only be of interest to testers, of course.

Scanning speeds were excellent and overheads quite acceptable on access, and detection rates very impressive across all the sets. With no problems handling the WildList and an absence of false positives, *Sophos* is a worthy winner of a VB100 award.

Symantec Endpoint Protection 11.0.4202.75

ItW	99.99%	**Polymorphic**	99.99%
ItW (o/a)	99.99%	**Trojans**	98.04%
Worms & bots	100.00%	**False positives**	0



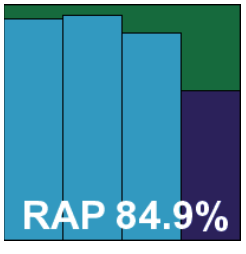
Symantec's corporate desktop product had a facelift not so long ago, and now more closely resembles a home-user product than a business tool, with its bright colours and curvy shapes. The install is simple, if a little slow, but once up and running things are fairly responsive and easy to use – the serious configuration areas eschew the slick and shiny stylings of the main interface in favour of more traditional, solid, serious greys and right angles.

Zipping through the speed tests proved something of a breeze, and on-access tests were also pretty speedy, but the on-demand scanner took some time, particularly over infected sets, taking several days to complete the biggest scan and causing some worries as the end of the test period approached fast. The poor test machine also grew increasingly hot as the scan proceeded. Logging is recorded in extreme depth, to such an extent that the log viewing utility within the product is barely usable for our purposes, taking hours at a time to convert all the information for display. Fortunately, the bare logs were easily parsed and showed some pretty superb detection levels in most areas, with only the proactive week of the RAP sets showing any decline from the heights of excellence – something which should be addressed by the various additional proactive technologies included with the product.

In the WildList however, a tiny number of the new Virut samples were not detected; further analysis from *Symantec* has shown that a minor adjustment to the detection routines for this item, in place only for a short time around the submission deadline, led to the possibility of a fraction of infected samples not being detected – as few as one in 100,000 by the developers' reckoning. It is extremely unlucky, therefore, that our set of 2,500 contained two such samples, but our rules are clear and our sets are designed to test completeness of detection. After putting together a quite magnificent unbroken run of 44 VB100 passes stretching back to the last century, this month *Symantec* is denied an award by a whisker.

Trustport Antivirus 2009 2.8.0.3016

ItW	100.00%	**Polymorphic**	99.22%
ItW (o/a)	100.00%	**Trojans**	97.52%
Worms & bots	100.00%	**False positives**	0



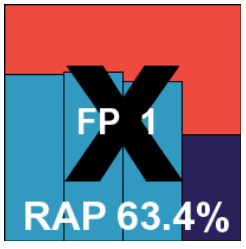
Trustport's installation procedure manages to be swift and straightforward despite some unusual steps, which include some initial configuration for the duo of engines used to provide protection. After the required reboot a registration wizard is presented, and the various control facilities can be accessed from a menu placed in the system tray. The main configuration tool has both simple and advanced modes, which provide a reasonable level of configuration options with all the main areas covered.

The dual engine approach as usual resulted in some fairly lacklustre scanning speeds in both modes, and the added strain on our tired old test systems saw more of those unexpected shutdowns – quite frequently during lengthy scans of infected sets. With some careful management of strings of small scans and saving of logs, plenty of data was acquired however. On processing, the results showed the expected outstanding detection rates, taking pride of place at the top of the table for the reactive part of the RAP sets and a close second in the overall averages. With no problems encountered in the WildList or clean sets, *Trustport* comfortably earns another VB100 award.

VirusBuster VirusBuster Professional 6.1.148

ItW	100.00%	**Polymorphic**	90.12%
ItW (o/a)	100.00%	**Trojans**	91.35%
Worms & bots	99.97%	**False positives**	1

VirusBuster takes its accustomed place at the end of the comparative roster, with its familiar product presenting the same old outlook to the world. Its install process is enlivened only by the customary UAC pop-up at the beginning, and runs slick and smooth to completion.



The rather quirky design no longer presents much difficulty, mainly thanks to experience, but some of its oddities can still take the unwary tester by surprise. Not least of these was the lack of an option to simply run a scan and log results; opting for the 'interactive' method rather than the automatic cleaning/removal mode, we left a long scan of the clean set to run overnight, only to find, on arrival the next morning, that it had spent most of the night sitting waiting for a response to an alert. Fortunately, once this was given it provided an option to suppress further alerts, and could safely be left to run for another night. This set-up could be slightly frustrating for those who wish to leave their massive external hard drive to be scanned overnight but for whom the risk of false positives is too much of a concern to trust the product to automatically delete items detected.

Apart from this minor glitch everything else went smoothly, with some decidedly impressive results in the standard sets and some strong signs of improvement in the RAP sets too. The product had no problem handling the gamut of new Virut samples added to various sets either. The alert discovered after the abortive overnight scan presents the only hiccup in an otherwise excellent run – as with *Agnitum* at the very beginning of this long journey, that single suspect file from *Microsoft*'s .NET package is wrongly described as a trojan, and a VB100 award is therefore denied this time around despite a very good performance.

CONCLUSIONS

A remarkable feeling of calm descends over the test lab as we reach the end of a long, tough month of testing. This has been a more than usually arduous comparative for many reasons, the most obvious of which being the sheer size of the field of submissions. Though not quite a record, it was still a lot of products to get through, actually larger than shown here thanks to a couple of additional products which were eventually excluded from the test but still took up precious testing time. One of these was excluded thanks to limitations on logging which, even with our usual willingness to make the effort and plod through our tests in smaller chunks, would simply have taken too long, and the other rendered the test machine completely unresponsive on reboot.

Many of the products in this test did prove stable, speedy and well behaved, but many others had issues far too serious to be classed as mere quirks and oddities. We experienced a large number of freezes, crashes and hangs, not just of the product interfaces or of specific scans but in many cases seeing the whole machine shutting down. At first we suspected this was simply some incompatibility between *Vista* and our standard test hardware, but as the test progressed it became clear that it was happening frequently with a small group of products and not at all with the rest, implying that the activities of those specific products were the main factor in the incidents. We continue to investigate some new test procedures which will focus on product stability and proper interaction with the operating system.

Another major issue this time has been logging difficulties, whether it be unreliable, unnecessarily truncated, bizarrely mangled or strangely formatted log files, encrypted log files only accessible via untrustworthy display systems, or downright peculiar layout and content. We are considering imposing some rules on logging requirements which must be satisfied by any product before it will be accepted into our tests as we feel that, while it may be a rare thing for the average home-user to encounter large logs with high numbers of detections listed, it is a simple requirement of any product that it be able to account for its behaviour and record its own history.

The bulk of this month's products made the VB100 grade – some just scraping across the line and some galloping home with plenty to spare. A handful of false positives caused problems for a few, most of which came from the sizeable new additions to the clean sets. There were also a few products that didn't quite cover the highly complex polymorphic file infector that found its way onto the WildList for this test. As always seems to be the case with these items, whenever they appear on the list there are a few casualties. This month has also seen another interesting batch of figures from our RAP testing, which will be added into the aggregate graphs displayed at http://www.virusbtn.com/vb100/rap-index.xml.

With nothing more to be tested, the lab team is set to begin the process of clearing up and beginning preparations for the next test. We can only hope that some of the more troublesome vendors will be paying attention, and will provide better products next time, not just for our sakes, but for those of all their users.

Technical details:

Test environment: All products were tested on identical systems with *AMD Athlon64 X2* Dual Core 5200+ processors, 2GB RAM, dual 80GB and 400GB hard drives, running *Microsoft Windows Vista Business Edition, Service Pack 2, 32 bit.*

END NOTES & NEWS

The 18th USENIX Security Symposium will take place 12–14 August 2009 in Montreal, Canada. The 4th USENIX Workshop on Hot Topics in Security (HotSec '09) will be co-located with USENIX Security '09, taking place on 11 August. For more information see http://www.usenix.org/events/sec09/.

The International Cyber Conflict Legal & Policy Conference 2009 will take place 9–10 September 2009 in Tallinn, Estonia. The conference will focus on the legal and policy aspects of cyber conflict. For details see http://www.ccdcoe.org/126.html.

The 7th German Anti-Spam Summit takes place 14–16 September 2009 in Wiesbaden, Germany (the event language will be English). For details see http://www.eco.de/veranstaltungen/7dask.htm.

IMF 2009, the 5th International Conference on IT Security Incident Management & IT Forensics takes place 15–17 September 2009 in Stuttgart, Germany. Experts will present and discuss recent technical and methodical advances in the fields of IT security incident response and management and IT forensics. For more information see http://www.imf-conference.org/.

SOURCE Barcelona will take place 21–22 September 2009 in Barcelona, Spain. The conference will be run in two tracks: Security and Technology, covering security software, application security, secure coding practices, engineering, new tool releases and technology demonstrations; and Business of Security, covering critical decision-making, entrepreneurship, issues of compliance, regulation, privacy laws, disclosure and economics. For full details and registration see http://www.sourceconference.com/.

Hacker Halted 2009 takes place in Miami, FL, USA, 23–24 September 2009. See http://www.hackerhalted.com/.

VB2009 will take place 23–25 September 2009 in Geneva, Switzerland. For the full conference programme including abstracts for all papers and online registration, see http://www.virusbtn.com/conference/vb2009/.

Hack in the Box Security Conference 2009 takes place 5–8 October 2009 in Kuala Lumpur, Malaysia. Technical training will take place on 5 and 6 October, with conference sessions on 7 and 8 October. For full details see http://conference.hackinthebox.org/.

The third APWG eCrime Researchers Summit will be held 13 October 2009 in Tacoma, WA, USA in conjunction with the 2009 APWG General Meeting. eCrime '09 will bring together academic researchers, security practitioners and law enforcement to discuss all aspects of electronic crime and ways to combat it. For more details see http://www.ecrimeresearch.org/.

Malware 2009, the 4th International Conference on Malicious and Unwanted Software, will take place 13–14 October 2009 in Montreal, Quebec, Canada. For more information see http://www.malware2009.org/.

The SecureLondon Workshop on Information Security Audits, Assessments and Compliance will be held on 13 October 2009 in London, UK. See http://www.isc2.org/EventDetails.aspx?id=3812.

RSA Europe will take place 20–22 October 2009 in London, UK. For full details see http://www.rsaconference.com/2009/europe/.

CSI 2009 takes place 24–30 October 2009 in National Harbour, MD, USA. For information and online registration see http://www.csiannual.com/.

The 17th general meeting of the Messaging Anti-Abuse Working Group (MAAWG) will be held 26–28 October 2009 in Philadelphia, PA, USA. Meetings are open to members and invited participants only. See http://www.maawg.org/.

AVAR2009 will be held 4–6 November 2009 in Kyoto, Japan. For more details see http://www.aavar.org/avar2009/.

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

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/