OCTOBER 2009

# virus BULLETIN

Fighting malware and spam

## CONTENTS



ISSN 1749-7027

## IN THIS ISSUE


### LEAVING ON A JET PLANE

Ears still ringing from the sound of yodelling and (to a lesser degree) jet planes, Helen Martin reflects on VB2009 – one of *VB*'s biggest conferences to date.
**page 6**

### LANDING SITE

Ponnurangam Kumaraguru and colleagues describe a collaborative project between the Anti-Phishing Working Group and Carnegie Mellon University that aims to educate users about the dangers of phishing by displaying an informational message in place of phishing sites that have been taken down.
**page 10**

### VB100 ON WINDOWS SERVER 2008

VB's test team put 26 products to the test on Windows Server 2008. John Hawes has the details.
**page 17**

*'Just when we thought things couldn't get any more volatile, along came social networking.'*

**Jeff Aboud**
**In-Focus Marketing, USA**

## SOCIAL NETWORKING MEETS SOCIAL ENGINEERING

We all know that the Internet cuts both ways – particularly in today's Web 2.0 world. Users enjoy continuous connectivity and the power to communicate in new and unique ways, whilst malware authors enjoy an endless supply of victims and the power to wreak havoc in new and unique ways. Just when we thought things couldn't get any more volatile, along came social networking.

For years, security experts have warned users about the dangers of Internet-based threats and attempted to educate them on an array of techniques used by malware authors to trick them into opening their wares. Time and again we told users 'don't open attachments from anybody you do not know', 'don't open suspicious attachments from anybody you do know', 'don't click on embedded links' and 'be wary of downloading content from unfamiliar, untrusted websites'. But just as end-users were beginning to heed our warnings (albeit slowly and far from universally), along came social networking sites and reversed our teachings. *Facebook*, *MySpace*, *YouTube* and others taught users that embedded links were something to be followed; to download content from unknown websites was normal; and that strangers were really just friends we had not yet met – so it was OK to open their attachments, to get to know them!

Then, in December 2008, the inevitable occurred. Koobface surfaced and quickly became the most successful piece of malware to propagate via a social network. Though Koobface was a complex worm powered by a substantial bot network, its social engineering strategy was simple: infect one user and send messages from his social networking account to everybody in his network. The only difference was that the legitimate link to the social networking site would be replaced with a rogue link, redirecting to a spoofed site containing the malware's executable. Social networks routinely send messages with embedded links, so it was natural that users would click on the link without question. Likewise, due to extraordinary levels of trust with these communications, users gladly downloaded what they were told was a required *Flash* update – seemingly without the slightest hesitation. Though the most prolific variant has been on *Facebook*, other variants have made their way through *Twitter*, *YouTube* and others.

Despite the relative success of Koobface, other malware authors have proven that its complexity was in many ways unnecessary. Due to the routine behaviours users exhibit on social networking sites, a simple comment with an embedded link posted to a popular thread can be enough to propagate malware to thousands of users. Similarly, a fraudulent account can be used to harvest email addresses and other sensitive user information, proliferate spam, or harbour malware. Though neither of these techniques possess the engine required for mass distribution as Koobface does, they also require more time to detect and eradicate than the more visible Koobface.

In each of these cases, as with traditional threats such as spam and phishing, social engineering has proven to be the most essential element to the propagation strategy. The reason is twofold: first, social networking sites rely on 'interesting' content. Blogs, photos, videos, even pages themselves, should be interesting. If they are, they will attract many users. Second, users exhibit an exceptional level of trust with social networking sites – meaning that a user will willingly follow links and download content from people he does not know, with the assumption that the unknown user must somehow be in his extended network. This combination adds unimaginable joy to the life of a malware author.

Malware authors will assuredly continue to develop new social engineering techniques to spread their wares via social networking sites, since end-users make themselves easy targets through their illogical behaviour. The question is, how do we reverse this behaviour? We were only marginally successful the first time around, but now there is a powerful force, with more mindshare than we will ever have, teaching users the diametric opposite. Perhaps our most promising recourse is to embrace this situation as a means to educate our business owners, once again, on the overwhelming need for endpoint security, in addition to their gateway and cloud-based solutions.

# NEWS

## MORE PHISH

Phishing attacks are still on the rise according to two recent reports. A study by brand protection firm *MarkMonitor* indicated that phishing attacks reached a new high in the second quarter of 2009, with more than 151,000 unique attacks, while the average number of phishing attacks per organization also increased to record levels, with an average of 351 attacks per organization.

Meanwhile, the Anti-Phishing Working Group (APWG) released its latest report last month, showing that the volume of phishing threats reported in May this year was around 7% higher than last year's high. The report also showed that online payment services such as *PayPal* became the most targeted industry sector – knocking financial services from the top spot for the first time since the APWG began its studies. Much as expected, the US was recorded as the country hosting the largest number of phishing sites with the exception of June 2009, when Sweden overtook the US.

## DHS TO RECRUIT SECURITY PROFESSIONALS

October is National Cybersecurity Awareness Month in the USA – the sixth annual National Cybersecurity Awareness Month to be sponsored by the Department of Homeland Security (DHS). The theme of this year's awareness month is 'our shared responsibility', and a range of activities and events have been organized to inform the public about cybersecurity issues – including conferences and seminars, awareness days aimed at children from kindergarten to higher education, exhibitions and a media tour.

At the launch of the activities, DHS Secretary Janet Napolitano announced that the agency has received approval to hire 1,000 new cybersecurity professionals over the next three years to fill various roles within DHS agencies. Napolitano said the department is primarily looking for analysts, programmers and systems engineers, and that the hiring plan will focus on strengthening the security of federal civilian networks, as well as supporting the Secret Service in combating cybercrime.

## SECURITY ESSENTIALS CAUSES STIR

The much anticipated release of *Microsoft*'s free *Security Essentials* product at the end of last month sparked a barrage of views and opinions from industry members and commentators – from those claiming that the release signalled the end of the AV industry, to those slating the free product as inadequate and pointless. *VB*'s testing team are already preparing an in-depth review of *Microsoft Security Essentials* – watch this space.

### Prevalence Table – August 2009

| Malware | Type | % |
|---|---|---|
| Agent | Trojan | 28.27% |
| OnlineGames | Trojan | 20.50% |
| Kryptik | Trojan | 15.36% |
| Heuristic/generic | Misc | 5.74% |
| NetSky | Worm | 4.70% |
| Mytob | Worm | 3.86% |
| Virut | Virus | 3.66% |
| Zbot | Trojan | 2.56% |
| Mydoom | Worm | 2.33% |
| Encrypted/Obfuscated | Misc | 2.25% |
| Bredolab | Trojan | 1.54% |
| Iframe | Exploit | 1.47% |
| Clicker-misc | Trojan | 0.89% |
| Stration/Warezov | Worm | 0.74% |
| Basine | Trojan | 0.70% |
| Lineage/Magania | Trojan | 0.44% |
| Bagle | Worm | 0.43% |
| Zlob/Tibs | Trojan | 0.42% |
| Buzus | Trojan | 0.39% |
| Small | Trojan | 0.35% |
| Backdoor-misc | Trojan | 0.33% |
| VB | Worm | 0.31% |
| Dropper-misc | Trojan | 0.28% |
| Alman | Worm | 0.23% |
| Sality | Virus | 0.19% |
| Downloader-misc | Trojan | 0.18% |
| Mywife/Nyxem | Worm | 0.15% |
| FunLove/Flcss | Worm | 0.15% |
| FakeAV | Trojan | 0.14% |
| Fujacks | Worm | 0.12% |
| Murlo | Trojan | 0.09% |
| Autorun | Worm | 0.09% |
| Delf | Trojan | 0.08% |
| Others[1] | | 1.05% |
| Total | | 100.00% |

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

# MALWARE ANALYSIS

## FLYING SOLO

*Peter Ferrie*
Microsoft, USA

*Continuing his series of analyses of viruses contained in the EOF-rRlf-DoomRiderz virus zine, Peter Ferrie looks at a virus named 'Pilot'.*

The term 'pilot' in the sense of a television programme can be likened to a proof-of-concept for a proposed series. A 'pilot' in the sense of computer viruses might be an appropriate term for a technique that could become common in the future. At least, that's one conclusion that might be drawn from the virus whose author named it 'Pilot'. (In fact, the virus author named it 'PiLoT', intending to refer to the PLT, as explained below.)

### RESOLVE TO WORK HARDER

In the case of viruses for the *Intel* x86-based *Linux* platform, it is common to see the use of 'int 0x80' instructions to call the system functions. However, in this virus there are no 'int 0x80' instructions. Instead, the virus resolves the function addresses dynamically, in much the same way as most viruses for the *Windows* platform do.

The general principle of address resolution is to find the base address of the interesting external file (for example, kernel32.dll in *Windows* and libc in *Linux*). On the *Windows* platform, it is a trivial matter to walk a series of in-memory structures to find the one that refers to the kernel32.dll file (though the current most common method relies on an undocumented field in one of those structures, and thanks to a minor change related to that field, the technique does not work on the most recent version of *Windows*). On the *Linux* platform, some searching is required, since there is no equivalent direct pointer to the libc file.

### GET IT. 'GOT' IT? GOOD.

The virus begins by examining the Procedure Linkage Table (PLT). Specifically, the virus examines the value at PLT+8. The PLT is ultimately an array of jumps to imported functions, however it contains additional instructions that are used by the linker to resolve the addresses dynamically. It begins with a push of an absolute indirect address, followed by a jump through another absolute indirect address (subsequent entries have a different format – a jump through another absolute indirect address, followed by a push of an immediate value, and ending with a relative jump to the first entry in the PLT). The first entry in the PLT jumps to the dynamic linker if its presence is required. Subsequent entries jump to the other functions used by the host process.

The source of the address for the jump is the Global Offset Table (GOT)+8. The size of the push instruction is six bytes and the address for the jump is two bytes into the jump instruction. Thus, the value at PLT+8 is an address within the GOT. The GOT is a table of pointers, and the value at GOT+8 is a pointer to the _resolve symbol, which points to the dynamic linker. If the dynamic linker is not required (because the symbols were all resolved before the process started) then the value at this location will be zero.

### ELVES VS TROLLS

The virus retrieves the value at GOT+8. If the value is zero, then the virus retrieves the value at GOT+16 and trusts that this value is a pointer within the libc file. If the value at GOT+8 is not zero, then the virus page-aligns this value, and uses it as a starting point for a search within memory. The virus searches backwards in memory, page by page, looking for the dynamic linker's ELF header. The virus recognizes the header when it finds the 'ELF' signature at the start of a page, and a value that describes the file as 32-bit class, data in LSB format, and version 1 header format.

The virus contains no exception handling, so there is a risk that, depending on the section layout, a gap exists in memory between the starting location of the search and the ELF header. If such a gap exists, then the virus will cause a segmentation fault, which will cause the process to be terminated.

Once the dynamic linker's ELF header has been found, the virus searches within the Program Header Table entries for the PT_LOAD entry with the lowest virtual address and the PT_DYNAMIC entry, which the virus assumes will always exist. If the PT_DYNAMIC entry is found, then the virus is interested in its virtual address.

The virus converts the virtual address of the PT_DYNAMIC entry into a file offset, and then searches within the dynamic linking array for an entry which has the DT_PLTGOT tag. It is also assumed that this search will always be successful. The associated pointer references the GOT of another file. The virus retrieves this pointer, and then retrieves a value from within that GOT, at offset 16. This value is assumed to point into libc.

At this point, the virus performs the routine again, beginning with the search for the ELF header, and ending with the search for the DT_PLTGOT tag. The result is

that the virus recovers the required values for the libc file: a pointer to the dynamic linking array, the adjustment to convert a virtual address to a file offset, and a pointer to the GOT.

## STRING THEORY

Given these values, the virus searches the dynamic linking array for the entries whose tags are DT_STRTAB, DT_SYMTAB, and DT_HASH. At last, the virus has all that it needs to resolve arbitrary symbols. The virus retrieves the addresses of the open, lseek, mmap, close, munmap, mprotect, readdir, opendir and closedir APIs, which are needed to infect files, and places the addresses on the stack. The resolution is achieved by hashing the name of the API, indexing through the bucket list (see *VB*, August 2009, p.4) to find the starting point in the list, and then comparing the names in the list until a match is found.

The virus allocates two pages of memory for itself using read/write attributes, copies itself to the first page, then changes the attributes of that page to read/execute. This allows the virus to work on systems that enforce the write^exec exclusion. That is, any given page can be writable or executable, but not both at the same time. The virus copies the API addresses from the stack into the second page, then transfers control to the first page.

## I LIKE TO MOVE IT MOVE IT

In order to restore the PLT (see below), the virus changes the attributes for the page in which it exists to read/write, and does the same for the following page. By always marking two pages, despite the fact that the virus is smaller than a page, the virus does not need to worry about the offset of the PLT. Since the paging API requires an aligned base as a starting address, the virus must either place itself at exactly such an aligned address (which might require moving the PLT, and thus everything around it, too – a very complicated operation, though the virus author demonstrated that a similar thing can be done, in his Crimea virus [see *VB*, February 2008, p.4]), or the size of the marking must be increased appropriately (which is the case here) in case the PLT spans two pages. However, there is an implicit assumption here – that the PLT is no larger than 8KB, which is equivalent to 512 functions. While the vast majority of files will not import nearly as many functions, we have seen such extreme examples on the *Windows* platform. It is certainly possible that such files could exist on the *Linux* platform, too. In that case, the virus will cause a segmentation fault while rebuilding the PLT, which will cause the process to be terminated.

The virus then builds a new PLT, beginning with the second entry, by placing the indirect absolute jump, the push and the relative jump once for each of the symbols. The appropriate values for each are filled in as the PLT is constructed. After the PLT has been restored, the virus changes the attributes for the two pages to read/execute. This is a potential bug, since if the PLT did not span two pages, then the attributes for the next page might originally have been something other than read/execute. Thus, by changing the attribute to read/execute, an incompatibility might be introduced that will cause the process eventually to crash.

Finally, the virus is ready to search for files to infect.

## THE MAKER'S MARK

The virus is interested in files that are at least 84 bytes long, in ELF format for the *Intel* x86-based CPU, and not infected already. The infection marker 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.

For each such file that is found, the virus searches within the Section Header Table entries for an entry that is named '.plt'. If the .plt entry is found, then the virus checks if the section is large enough to contain the first entry and the virus body. If the section is too small, then the file will not be infected, however the infection marker is not added, so such a file could be examined repeatedly in the future.

If the section is large enough, then the virus examines each of the entries in the PLT, to ensure that the addresses are arranged in increasing order. This is required because an out-of-order table cannot be reconstructed by the routine described above. If all goes well, then the virus overwrites the PLT with the virus body, and saves some important values in the code (the GOT pointer, the PLT-specific relocation-table pointer, the number of PLT entries and the original entrypoint). The virus changes the host entrypoint to point directly to the virus code, and then sets the infection marker.

## CONCLUSION

As we can see, the PLT is another cavity, but not *just* another cavity. Unlike others, the contents of the PLT must be restored before the host can run. This benefits us, too – a virus cannot be heavily entrypoint-obscuring if it uses the PLT as a cavity, because the host cannot call any external functions until the PLT is restored.

# CONFERENCE REPORT 1

## GENEVA CONVENTION

*Helen Martin*

This year the *VB* conference landed on the shores of Lake Geneva – or, perhaps more accurately, at the end of the runway of Geneva International Airport. The Crowne Plaza hotel, a mere 0.5km from the airport terminal, is a haven for plane spotters, boasting uninterrupted views of the runway from one end of the building, yet internally free from the slightest sound of a jet engine thanks to the wonders of modern glazing technology.

A free tourist bus pass made the venue's distance from the centre of town seem significantly shorter, with the 10-minute ride into the city taking in such sites of international significance as the UN European HQ and the High Commission for Refugees before arriving in the centre of Geneva, where the crystal waters of Lake Geneva sparkled against their backdrop of majestic mountains (when they appeared from the mist that is).

The run-up to this year's event was surrounded by a certain amount of uncertainty – as will have been the case for many businesses, we waited anxiously to see what the effects of the global economic downturn would be. Having heard rumours of travel budgets having been slashed in this company and that, we braced ourselves for a slightly more modest turnout than in recent years. However, we were thrilled by an even stronger turnout than last year, with the final number of attendees just a handful short of *VB*'s largest conference to date. The number of delegates in attendance this year and the level of support from sponsoring organizations are, I think, a testament to the industry's recognition of the importance of sharing insight and knowledge, debating and challenging ideas, and encouraging coordinated global efforts to combat cybercrime.

### IN THE BEGINNING

The conference kicked off on Wednesday morning with a presentation by Eric Davis, head of *Google*'s Anti-Malvertizing team, who called for industry-wide cooperation in an effort to help combat malicious web advertising – a serious problem not only for *Google* and other search sites but also for the sites that rely on ad syndication networks, and for users of the web in general.

The conference then split into its usual two-stream format, with Pascal Lointier looking at incident response from a financial perspective, while *Microsoft* trio Elda Dimakiling, Scott Wu and Francis Allan Tan Seng unravelled the various malware attacks linked to the MS08-067 vulnerability – looking not only at Conficker but at a number of other malware families that use the MS08-067 exploit to spread.

Next, Juraj Malcho asked 'Is there a lawyer in the lab?' as he explored the boundaries between legitimate and illegitimate applications and the minefield that exists for vendors in making a decision regarding an executable's intentions (and thus whether or not to include detection for it). He highlighted the increasing frequency with which labs are forced to consult with legal teams regarding applications that are sufficiently dubious to warrant detection, yet which proclaim just enough legitimacy to potentially cause problems for a vendor that detects them.

Later in the afternoon another *Microsoft* researcher, Chun Feng, provided a fascinating look at five generations of Dogrobot – a family of malware that has caused more than $1.2 billion in losses from Chinese Internet cafés using a novel rootkit technique to hijack System Restore on *Windows*. Meanwhile, Guillaume Lovet gave a comprehensive overview of the technical, juridical and ethical challenges of fighting cybercrime.

### EAR PLUGS ANYONE?

Wednesday evening saw the first of the main networking events of the conference – the VB2009 drinks reception. Delegates were greeted at the entrance to the reception by two magnificent St Bernards. Each weighing in at around 65kg, both Beetoo and Caspar proved to be gentle giants and took the hustle and bustle of the crowd and the non-stop paparazzi-style photography in their (very large) stride. Of course, for Beetoo (formal name Beethoven), the glitz and glamour lifestyle is in the genes as his owners proudly revealed that he is a direct descendant of the canine star of the 1992 film *Beethoven*.

*Some VB delegates brought their own supplies in case the free drinks ran out...*

At the opposite end of the bar from our canine guests an altogether more raucous form of entertainment was on offer (if I'm honest, it was a little difficult to ignore). Yodeller extraordinaire Barbara Klossner and her group of musicians, Les Amies du Lac Léman, began by providing a rousing demonstration of

*...while for others, the drinks reception was too much to handle.*

traditional Swiss yodelling. The mantle was then passed over to the audience for *VB*'s first (and hopefully last) yodelling competition.

Compère Jan Hruska started proceedings with a quick demonstration of his own yodelling skills (or lack thereof) to the tune of 'Happy Birthday' and then threw the competition open to the floor. A steady stream of would-be yodellers lined up to take the mic. At one point concern was expressed for the distinct possibility that all the wine glasses in the room might shatter around us, but mercifully 'Happy Birthday' proved to be just brief enough to save the glassware. A three-strong judging panel awarded marks out of five for each contestant, eventually declaring Björg Olafsdottir the undisputed winner.

## IN THE MIDDLE

Thursday morning kicked off with a presentation by Raoul Chiesa, a former hacker who is now Technical Liaison Officer on Cybercrime Issues at the United Nations Interregional Crime and Justice Research Institute (UNICRI). Raoul provided a fascinating insight into the Hackers Profiling Project, the first project to be dedicated to the criminal profiling of hackers. Meanwhile, Maik Morgenstern and Andreas Marx of *AV-Test.org* discussed the limitations of current in-the-cloud security solutions, highlighting privacy, security, reliability and fault tolerance issues.

Next to take to the podium was *Sophos* researcher Dmitry Samosseiko who took a detailed look at the Russian partnerka – the hundreds of well-organized affiliate networks and webmasters that make millions of dollars

*VB delegates show off their yodelling skills while the judging panel keep smiling through the pain.*

of profit each year through the online sales of unlicensed prescription medicine, fake designer goods, fake anti-virus, and so on. Dmitry exposed their economic model, revealing statistics and information including the typical amount of money a partnerka webmaster could expect to earn each day, as well as highlighting some of the tools and techniques of the 'trade'.

After a break for mid-morning coffee and pastries, Bryan Lu took to the stage for a look at the different ways in which security companies display threat levels. He called for standardization of the way in which computer and Internet threat levels are assigned in order for these to be useful and have any meaning.

Righard Zwienenberg followed, with an update on the current state of the Anti-Malware Testing Standards Organization (AMTSO) and on the progress the group has made since its early beginnings in 2007.

The first of this year's anti-spam papers came after lunch on Thursday, with *Kaspersky* team Darya Bronnikova and Anna Volodina presenting a detailed look at SMS fraud – a criminal activity that is common in Russia and the former Soviet countries but rare in Western countries, the discrepancy largely being due to the fact that Russian mobile network providers do little to prevent fraudulent activities, while in the West the risks of being caught are significantly greater. *Microsoft*'s Terry Zink was next up with an interesting look at how *Microsoft*'s *Exchange Hosted Services* mitigated the problem of outbound spam – not only that, but the multi-talented Terry also delighted the audience with a card trick and by making a coin vanish into thin air (although on reflection, given the astronomical bar prices at the venue, the crowd might have been more impressed had he made coins appear out of thin air). Finally, another *Kaspersky* duo, Darya Gudkova and Andrey Nikishin, presented a round-up of different anti-spam legislation across the world, looking at where it is effective and what additional legislation is needed to help the global fight against spammers.

Later in the afternoon Methusela Ferrer highlighted the issue of Mac security, looking at malware threats on *Mac OS X*. Methusela outlined the underlying motives and methods used by a number of Mac threats. Despite a small technical hitch, the presentation was one of the most popular of the conference – demonstrating that Mac security is very much being taken seriously by the industry's top researchers.

Thursday also saw this year's selection of last-minute presentations – eight shorter papers that were submitted and selected just three weeks prior to the conference in order to allow more up-to-date material than the rest of the papers which take several months to produce.

Dmitry Bestuzhev kicked off the last-minute papers with a colourful presentation on the thriving Brazilian banking trojan scene. With close to 23 million users of the major online banks in Brazil, combined with the fact that the country is the largest source of banking trojans in the world, banks have a tough challenge in fighting the problem. If nothing else, most delegates came away from the presentation with a sense of relief that they don't bank in Brazil.

Researchers from *Trend Micro* and *Kaspersky* focused on social-network-aware threats. Ivan Macalintal from *Trend* presented research carried out by his colleagues on the Koobface worm – the first piece of malware to successfully and continuously propagate through social networks. Ivan described what Koobface does, what makes it successful and how cybercriminals are monetizing it – concluding that the worm is still a work in progress and more developments are likely. Afterwards, *Kaspersky*'s Costin Raiu and *Trend Micro*'s Morton Swimmer collaborated on a presentation that focused on *Twitter* attacks – both researchers are working on separate projects analysing the volume and nature of *Twitter*-related threats and exploring patterns of abuse. The pair revealed that AV firms currently scan around half a million unique URLs posted to *Twitter* every day in their search for malicious code.

Other last-minute highlights included Igor Muttik discussing the Industry Connection Security Group's XML schema for sharing samples and information among vendors and testers and Erik Wu's presentation of the results of a three-month case study of more than 600 real-world botnets.

## FUN AND FROLICS

Of course, no *VB* conference would be complete without the traditional gala dinner evening. As usual, members of the AV industry turned out in all their finery and elegance – I have to say that, as a crowd, the AV industry scrubs up pretty well!

The dinner was accompanied initially by the mellow and melodious tones of a trio of alphorns, and towards the end of the meal we were treated to a charming performance by Swiss mime trio Due piu Uno. Their repertoire was witty, touching, energetic and delightfully entertaining, with a mixture of slapstick comedy, music and acrobatic feats, all timed to perfection.

## IN THE END

The final morning started off bright and early at 9am with a presentation by *Kaspersky*'s Stefan Tanase taking a look at the evolution of Web 2.0 threats and at the likely direction in which they will develop in the future, while *BitDefender*'s Claudiu Musat described a system for extracting novelty from an unsorted spam flow. *VB*'s own Martijn Grooten followed with a presentation outlining the essentials of anti-spam testing, while another *BitDefender* researcher, Catalin Cosoi, returned once again to the topic of Web 2.0 as he described a fractal approach to the detection of social network spam.

*Fun and frolics with Due piu Uno.*

The most popular presentation of the conference took place later on Friday as John Graham-Cumming described JavaScript security as 'the elephant in your browser', pointing out that the security situation with JavaScript is so poor that the only solution is to kill it.

The conference concluded with a panel discussion led by Paul Ducklin, in which two 'teams' (*Sophos*'s Graham Cluley and *West Coast Labs*' Lysa Myers, facing *McAfee*'s Greg Day and *Lockheed Martin*'s John Alexander) debated the virtues of free anti-virus versus paid for anti-virus and the issue of rogue anti-virus products. Aside from the entertaining debate, the award for the best moment of the conference must surely go to Mikko Hyppönen, who was called upon to ask a question in the style of Vesselin Bontchev – all I can say is that it was as if the great man himself was in the room.

## AND FINALLY...

There has not been enough space to mention more than a small selection of the speakers and presentations here, but I would like to extend my warmest thanks to all of the VB2009 speakers for their contributions, as well as to sponsors *CA*, *ESET*, *K7 Computing*, *IKARUS Software*, *Kaspersky Lab*, *Kingsoft*, *Lavasoft*, *eScan*, *OPSWAT*, *Sunbelt Software*, *TrustPort* and *Beijing Rising* for their support.

Next year the *VB* conference makes a return visit to the stunning city of Vancouver for its 20th birthday, with the conference taking place 29 September to 1 October 2010 at the Westin Bayshore, Vancouver, Canada. I very much look forward to welcoming you all there.

*Photographs courtesy of: Pavel Baudis, Jeannette Jarvis and Tjark Auerbach. More photographs will be available soon at http://www.virusbtn.com/conference/vb2009/photos.*

# CONFERENCE REPORT 2

## 7TH GERMAN ANTI SPAM SUMMIT 2009

*Sorin Mustaca*
Avira, Germany

The 7th German Anti Spam Summit, hosted by the *eco* organization (http://www.eco.de/veranstaltungen/7dask.htm), took place last month at the beautiful Biebrich castle in Wiesbaden, Germany.

The theme of this year's summit was 'Spam – advertising and compromising (unsolicited emails as cause and effect of botnets)'. Despite the fact that most of the participants were German, the official language of the summit was English. In general, the event was angled towards those in technical and legal management. A stream of presentations ran alongside a series of sponsor workshops.

### DAY 1

On the first day, the presentation stream was split into two parts: one dedicated to the role of registries and registrars and the second to digital brand management.

The speakers in the first part were representatives of the .INFO and .ORG registries and the Austrian and German ccTLDs. The content of their presentations could be summed up by a single sentence: 'The registries are not allowed to interfere with the registrars'. I must confess that these presentations left me with a bitter taste in my mouth. It confirmed why we see so many fake domains being registered with the sort of names that even a non tech-savvy user would recognize as suspicious. While on the one hand attempting to hunt down online fraudsters, the authorities are blocking the very organizations which could enforce some guidelines in this field. I appreciated the fact that the speakers were very honest and open to discussion and suggestions. However, all my ideas for slowing down or preventing the fake domains from being registered proved unrealistic due to the same legal issues which force the registries to step aside.

The presentations on digital brand management covered standards related to online security, domain name and trademark misuse, domain monitoring and reputation management (checking where and how your brand and domain name are used).

A podium discussion attempted to determine what registries and registrars should do in the future, but failed to reach any real conclusions.

### DAYS 2 & 3

The second day of the conference was a lot busier and more interesting than the first – there were around 150 delegates in attendance.

The day started with some warm-up speeches from the German authorities from Hessen-IT (the region in which the conference took place) and from the BSI (the Federal Office for Information Security). The highlight of the day was a presentation by two students from the University of Bonn who took the Conficker worm apart and suggested a smart way to immunize computers by fighting the worm with its own weapons. Whether or not this is ethical was not addressed and remains to be decided.

A very interesting presentation, for which the press was requested to leave the room, was about abuse and fraud management at the ISP *1and1* (www.1und1.de). It was nice to see a big ISP caring about what its customers are doing to the Internet for a change, rather than merely the other way around.

The other presentations discussed how to cooperate in combating spam, how different European countries combat spam (and fail to do so), and discussed SURBL.

The last day of the conference was reserved for a workshop run by the same students that took Conficker apart. They presented different techniques to fight and eventually control complex botnets, as well as showing how to get more information from honeypots.

### CONCLUSIONS

I was pleasantly surprised to see delegates at this event from the major ISPs in Germany (although unfortunately I didn't see anybody from *T-Online*, the biggest ISP in Germany) – which suggests that, at least in Germany, security on the Internet is an issue that is being taken seriously.

I also noticed that a couple of European email marketing companies were present at the event. I have to admit that I consider their activity to be one of the main reasons why spam is so hard to catch nowadays. I asked two of the representatives why they were attending. The answer? They were trying to learn how to send 'cleaner' emails. Applause, please.

*The opinions expressed in this report are those of the author and do not represent those of the author's employer or of Virus Bulletin.*

# FEATURE 1

## ANTI-PHISHING LANDING PAGE: TURNING A 404 INTO A TEACHABLE MOMENT

*Ponnurangam Kumaraguru*
Institute of Information Technology, Delhi, India

*Lorrie Faith Cranor*
Carnegie Mellon University, USA

*Laura Mather*
Anti-Phishing Working Group, USA

The Anti-Phishing Working Group (APWG) anti-phishing landing page[1] is a web page designed to be displayed in place of a phishing website that has been taken down. The page carries a succinct anti-phishing training message. The landing page is currently being used by financial institutions, ISPs, phishing site take-down vendors, government organizations and online merchants. When would-be phishing victims attempt to visit a phishing website that has been taken down, they are redirected to the landing page, hosted on the APWG website.

In this article, we describe the development of the landing page and present our analysis of the data we collected from its log files during the first six months of the landing page programme. Our analysis suggests that approximately 70,000 users were educated by the landing page during this period. We identified 3,917 unique phishing URLs that had been redirected to the landing page. We found 81 URLs in our log files that also appeared in email messages archived in the APWG phishing email repository. We present our analysis of the features of these emails.

### HOW THE LANDING PAGE WORKS

In the past, when ISPs and registrars were asked to disable a phishing site, they would remove the site from the Internet. This meant that a user would see a 404 error when they tried to access the site. These 404 errors would often confuse users who believed they were visiting a legitimate website. Because of this, APWG and Carnegie Mellon decided to create an educational landing page.

The landing page is a web page containing an educational message to help consumers protect themselves from phishing. The page is hosted by the APWG. When ISPs and registrars are contacted about disabling phishing sites they are now asked to redirect all traffic attempting to access the phishing site to the landing page. This way, when users attempt to access the phishing site, instead of encountering a 404 error, they are taken to a page that educates them on how to protect themselves against phishing (See Figure 1).

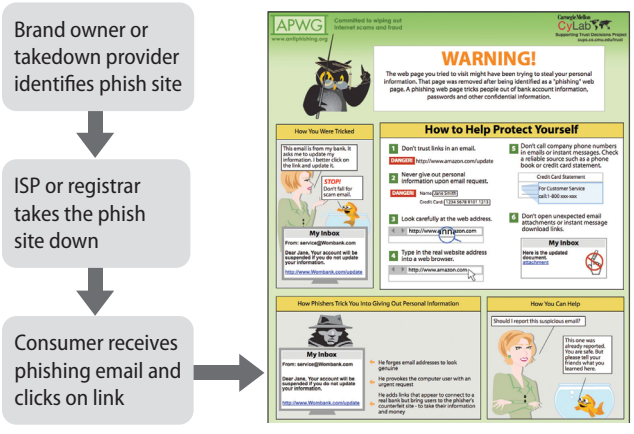



*Figure 1: APWG landing page. Users are presented with a version of the PhishGuru intervention when they click on a link to a phishing site that has been taken down.*

### ADVANTAGES OF THE LANDING PAGE

The landing page approach is compelling for several reasons. First, it takes advantage of an ideal 'teachable moment' in that it directs training to the users who need it most – those who have 'fallen' for a phishing scam. In addition, the landing page enables users to be trained without taking time out of their busy schedules, and it motivates them to pay attention to the training. The landing page makes use of research results from *PhishGuru*, another programme aimed at educating users about the perils of phishing[2]. Finally, use of the landing page creates a repository of data that can be analysed to gain a better understanding of phishing.

### EVOLUTION OF THE LANDING PAGE

The APWG landing page is based on the *PhishGuru* embedded training approach developed at Carnegie Mellon University. *PhishGuru* is an embedded training system that teaches users to avoid falling for phishing attacks by sending them simulated phishing emails. Figure 2 presents one version of the *PhishGuru* intervention. People access these training emails in their inbox when they check their regular email. The training emails look just like phishing emails, urging people to go to some website and log in. If users fall for the training email – that is, if they click on a link in that email – we provide an intervention message that

[1] http://education.apwg.org/r/en/.

[2] http://phishguru.org/.

explains that they are at risk of falling victim to phishing attacks and which offers tips they can follow to protect themselves. The training materials present the user with a comic strip that defines phishing, offers steps the user can follow to avoid falling for phishing attacks, and illustrates how easy it is for criminals to perpetrate such attacks. Our previous user studies in the laboratory and in the real world have validated the effectiveness of the *PhishGuru* approach [1, 2].

We designed the landing page using a user-centred iterative design process. Our goal was to design a succinct and engaging training intervention that could be translated into multiple languages and formatted for a variety of devices, including handheld devices. We began by compiling suggestions for training content from members of the APWG IPC (Internet Policy Committee). While this design incorporated all of the content committee members wanted to include, there were concerns that it was too long and not clear enough for non-experts to understand. We developed a second condensed version that omitted some of the content that was not directly related to phishing and which shortened the phishing-related content. We then conducted two focus group studies to evaluate both the short and long versions of the proposed landing page and compare them with one of our *PhishGuru* cartoons.

The first focus group was a two-hour session at Carnegie Mellon University with nine participants of varying ages and educational backgrounds. Using a wall projector, we began by demonstrating how someone might click on a link in a phishing email and arrive at the landing page. We then showed them what they might see on a landing page. We discussed details of three versions of the intervention: (1) the committee draft; (2) a condensed draft; and (3) the *PhishGuru* cartoon. We provided participants with a colour printout of the designs and asked them to provide feedback. Participants said the committee draft and the condensed draft were both too long, and that they would not read the entire content of either. However, they were more positive about the *PhishGuru* version and said that they would be more likely to read its entire content. After listening to participants make many comments about how their grandparents would react to the landing page, we decided to determine how the landing pages would appeal to older people. To that end, we conducted a second focus group study.

The second focus group study was a 2.5-hour session with six participants at The Jewish Community Center of Greater Pittsburgh. We worked with AgeWell's Independent Adult Services Department to recruit participants who were over 65 years old. Once again, participants came from a variety of backgrounds and none of them knew what phishing was. The process for conducting the study was similar to the first one. Using feedback from the first focus group, we revised the condensed and *PhishGuru* versions of the landing page. This time we discussed details of three versions of the intervention: (1) the committee draft; (2) the revised condensed draft; and (3) the revised *PhishGuru*.

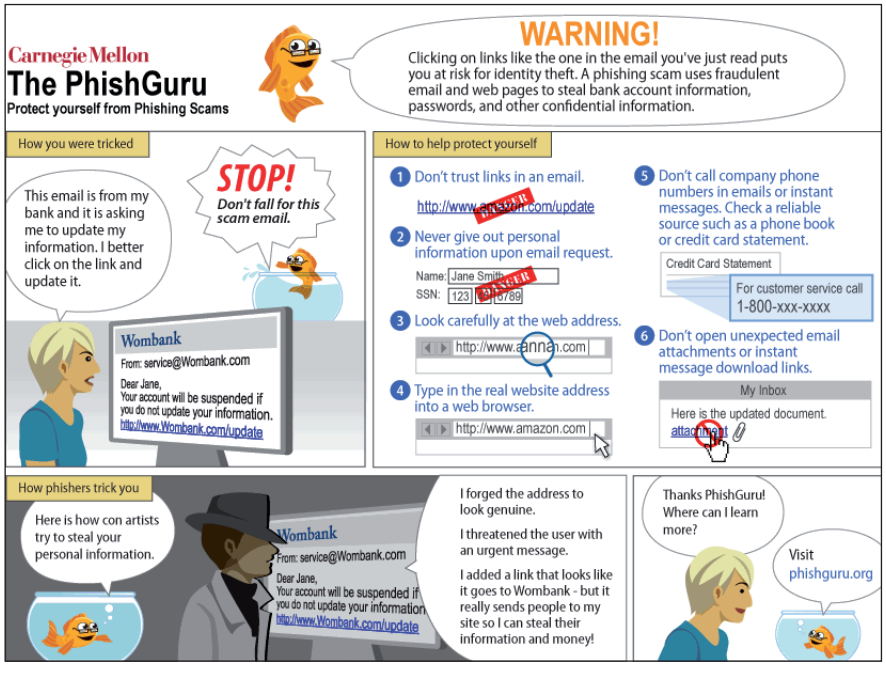



*Figure 2: The final intervention design that we used in a large-scale real-world study [2].*

Participants in this study, like those in the first, responded negatively to the committee draft. Most of the participants said they would not read the complete page. Participants liked the fact that the revised condensed version was short and had less text, but some participants mentioned that, even though it was shorter than the committee version, it was still too long for them to read in its entirety. Participants were attracted to the *PhishGuru* version, stating that it was fun to read and that people of all ages would read it. Participants were interested in the cartoon format and characters and said that they would read the complete intervention. All participants agreed that having cartoon characters is likely to attract readers' attention.

## LOG DATA

In order to make this an industry-wide initiative that any organization could use, a publicly available sub-domain was set up on the APWG website. Information about the project was posted on this website. The English version of the landing page was hosted on the same website. Since this page was intended to be translated into many other languages, it was decided that users would be redirected to a specific language depending on the default language of their web browser. As of March 2009, volunteers had come forward to translate the landing page into Arabic, Bulgarian, Catalan, Danish, Dutch, French, German, Hebrew, Japanese, Korean, Romanian, Spanish and Swedish. The French landing page is already live[3].

The APWG's server access log records all requests in *Apache*'s combined log format. By mining the landing page log files, we can create a list of phishing URLs that are redirected to the landing page. We correlated the log data with the APWG's feed of reported phishing emails[4] to find out which emails led most users to visit the landing page. This provided us with an insight into which phishing emails users are most likely to fall for. In the following sections we present an analysis of the logs we collected and results of feature analysis performed on the emails retrieved from the feed.

## LOG ANALYSIS

The data that we collect in the log files does not represent the entire population of users who click on the links in the phishing emails. If a user clicks on a link in the email and that link is already in the blacklist of the user's browser, then access will be blocked and the user will not be redirected to the landing page. Also, ISPs and registrars eventually stop redirecting users to the landing page some time after a site has been taken down. If users click on such a link after the redirection has been removed, the user will be presented with a 404 error page. Thus, our data is a good lower bound for people who click on links in phishing emails.

We believe the landing page has created many teachable moments in which users have been trained to avoid falling for future phishing attacks. From the entire data, there were 78,541 total hits on the page; among these hits, 3,917 unique phishing URLs were redirected to the landing page. These statistics suggest that the landing page has been responsible for at least 71,504 'teachable moments', in which a user has had the opportunity to learn from the intervention.

We observed that most hits (85.9%) came from the United States. This may be due to the fact that, at least for the time being, the brands that are requesting redirection to the landing page are mainly from the US. It also may be because the organizations being phished are mostly from the US. This may change as more brands around the world start using the landing page.

## EMAIL FEATURE ANALYSIS

To study the emails that correspond to the phishing URLs being redirected to the landing page, we compared the unique URLs from the landing page logs to the URLs in the APWG email feed. We found 81 matches for the period from 1 October 2008 to 31 March 2009. We examined the 81 emails manually and analysed the features in these emails. Around 95% of the messages masqueraded as

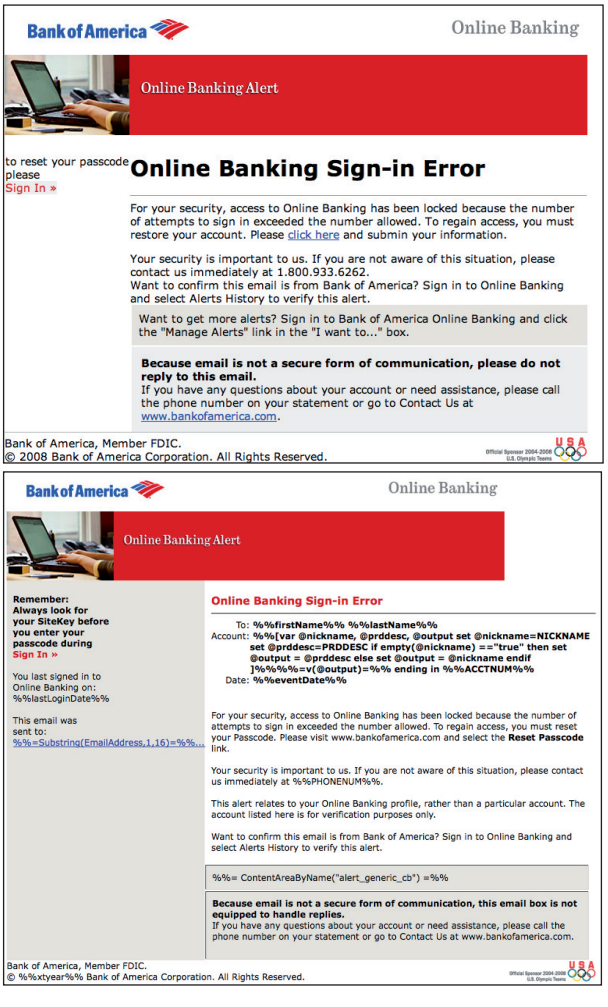



*Figure 3: Top: Phishing email from the APWG email dump that claims to come from Bank of America. Bottom: A real email from Bank of America to its customers. (All information with '%' is used to customize the emails with personal information).*

[3] http://education.apwg.org/r/fr/.

[4] Emails sent to reportphishing@antiphishing.org.

emails from one particular financial institution. The rest were made to look as if they were from other popular financial institutions and government agencies.

Most of the emails had features similar to legitimate messages. Ninety-one per cent of them had some form of logo or banner at the top. As researchers have shown, the fact that these logos and banners look legitimate is one of the main reasons people fall for phishing emails. Seventy-three per cent of the emails had some sort of footer containing logos; in particular, Bank of America emails had an Olympics logo in the bottom right-hand corner (see Figure 3). In some cases, phishers used an exact replica of a legitimate email. Figure 3 presents a legitimate email and a similar phishing email found in the AWPG feed.

## CONCLUSION

In this article, we discussed a real-world implementation of a landing page, based on *PhishGuru*, that educates consumers on how to avoid phishing attacks at the most teachable moment. Many users were educated by seeing the landing page instead of a 404 error page.

Since most phishing emails replicate legitimate emails, we believe that researchers and industry could reap substantial benefits by creating a corpus of legitimate emails, studying their features, and incorporating these features into email filters. Phishing emails haven't changed much over time, remaining relatively unsophisticated and containing a great number of errors in grammar and formatting. Most of the emails in the log analysis asked users to click on a link in the message to update their account details.

Going forward, we plan to study the changes to the data as the landing page is deployed in additional languages and as more brands request redirection to the page.

A more detailed description of this research can be found at http://www.ceas.cc/papers-2009/ceas2009-paper-37.pdf. The authors can be reached at pk@iiitd.ac.in, lorrie@cs.cmu.edu and laura.mather@antiphishing.org.

## REFERENCES

[1] Kumaraguru, P.; Rhee, Y.; Acquisti, A.; Cranor, L. F.; Hong, J.; Nunge, E. Protecting people from phishing: the design and evaluation of an embedded training email system. CHI '07: Proceedings of the SIGCHI conference on Human Factors in Computing Systems (New York, NY, USA, 2007), pp.905–914.

[2] Kumaraguru, P.; Cranshaw, J.; Acquisti, A.; Cranor, L.; Hong, J.; Blair, M. A.; Pham, T. School of phish: A real-world evaluation of anti-phishing training. Symposium On Usable Privacy and Security (2009).

# FEATURE 2

## AN UPDATE ON SPAMMING BOTNETS: ARE WE LOSING THE WAR?

*Marios Kokkodis, Michalis Faloutsos*
University of California Riverside, USA

Over the last few years, there has been an ongoing battle between botmasters and security administrators regarding the proliferation of bots. The former are constantly recruiting new members to their army, while the latter keep trying to improve their defences.

Intuitively, the larger a botnet becomes, the more harmful it can be. Since spamming is one of a botnet's major activities, the proliferation of bots results in an increase in the volume of spam messages that travel across the Internet. Because of this, many studies have been conducted on the behaviour of spamming botnets. Even though the contribution of these studies is significant, it is also important to remain up to date, since spamming botnets evolve rapidly (e.g. by modifying their spamming tactics, expanding their army of compromised machines, updating the techniques they use to obfuscate their identities etc.). As a result of this constant evolution, empirical studies that deal with questions such as 'who is sending all these unsolicited messages?' become very important for both the evaluation and improvement of the currently available mitigation techniques.

In this article, we present the results of an empirical study that we conducted regarding spamming activity. In more detail, we discuss the temporal spreading of spammers across the IP space. Our study analyses spam messages received in the last four years and illustrates the evolution of high-activity spamming IP spaces. Our findings can be summarized into two main observations:

- A previously unreported IP space has become a major source of spamming activity during the last two years.
- There is a spreading trend of spamming activity across the IP space.

These two observations have grave significance since they can compromise the effectiveness of IP-filtering-based mitigation techniques. In the rest of this article we describe the analysis that led to our findings, and discuss some of the ensuing implications.

## SPAMMING BOTNETS

Before outlining our analysis, it is important to have a basic understanding of the functionalities of a botnet. A botnet is a collection of compromised machines (i.e. bots) that

are controlled centrally by a botmaster. Their size varies between a few thousand to a few million compromised machines (e.g. the Conficker botnet has more than ten million bots in its army), while the amount of spam that a botnet can send varies between hundreds of millions to a few billion messages per day. In addition to spamming, botnets often engage in other malicious activities (e.g. DoS attacks). However, in this study, we concentrate only on spamming.

Figure 1 shows an abstract view of a spamming botnet. From this, we can identify three major groups of participants in the spamming process:

1. The botmaster. This is the person (or persons) that control(s) everything that has to do with the botnet. The botmaster is in charge of:
   - Recruiting new members (bots) by crawling the Internet and attacking unprotected machines.
   - Managing his current resources to maximize his profit (e.g. splitting them into groups and assigning a different spam campaign[1] to each group).
   - Managing the victim mailing lists (e.g. commanding bots to crawl the Internet and harvest new user accounts or to try randomly to guess some valid ones [e.g. from *Google*, *Yahoo!* etc.]).
2. The bots. These are compromised machines that blindly obey their masters' commands. The bots are the origin of the spam messages received by Internet users.
3. The victims (represented by the 'Internet' cloud in Figure 1). These are listed user-accounts that receive spam.

Figure 1 provides a blueprint of the botnet spamming procedure: the botmaster assigns specific lists of users to each bot, and then commands them to begin sending spam messages.

## KNOWN FACTS

Spam is a major problem that all network administrators have to overcome. The bad guys (spammers) are constantly improving their techniques, and so are the good ones (network administrators). As a result, a lot of work has been carried out in this field. Below are some fundamental findings that we already know about the origin of spam:

- The vast majority of spam messages come from bots (i.e. spamming botnets) [1–3].

[1] A spam campaign is a group of spam messages that have the same (or very similar) subject (e.g. a drugstore advertisement).

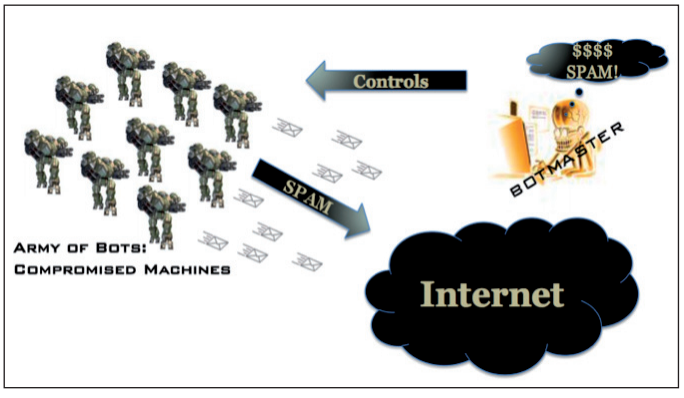



*Figure 1: An abstract view of a spamming botnet.*

- Two IP spaces[2] are responsible for the majority of the observed spam [2, 4].
- Spam activity seems quite 'concentrated' and follows the Pareto principle (the 80-20 rule[3]) [4].

These findings are implicitly optimistic, as they suggest that by focusing on a few highly active IP prefixes, we may be able to fight spam at the IP level (e.g. block traffic from specific subnets). However, our study unveils a worrying trend: bots seem to be spreading widely across the IP space.

## DATA

For our study, we used a publicly available dataset [5], which consisted of 2,046,520 spam messages (both email header and content). These messages were collected by various user accounts from three different domains over a four-year period (January 2006 – May 2009). The majority of these emails were flagged as spam by *SpamAssassin*, a well-known email filtering application. To increase our confidence in the dataset, we manually verified as spam a randomly chosen subset of the emails.

## PARSING DETAILS

Extracting useful information from an email header is not trivial, since spammers usually bypass the SMTP protocol in order to obfuscate their identities. Therefore, we believe that it is important to clarify the parsing procedure we follow in our study.

Our ultimate goal here is to find a valid source IP for each message in the dataset. According to the SMTP protocol, each server that receives a message appends a Received

[2] These are the /8-subnets between 60.* and 90.*, and between 190.* and 220.*.

[3] The 80-20 rule in our case indicates that 80% of the received volume of spam originates from 20% of the IP space.

record (e.g. Received : from example.com [77.49.119.108]) to the top of the email header. Hence, the earliest Received record should include the IP of the first SMTP server that forwarded the email (i.e. the source IP). However, as mentioned above, in the case of spam messages the protocol is often violated since spammers have developed techniques to hide (or obfuscate) their identities. An example of such a technique is to falsify the header information either by modifying it or by appending invalid Received headers. Therefore, the only relay from which we can identify the true IP address is the one that established the SMTP connection to our mail server. In our study, we used this as the source IP for conducting our analysis.

## DATA STATISTICS

In order to provide better insight into our dataset we present some statistics in Tables 1 and 2. In Table 1, we show the high-activity IP spaces for each of the four years of our dataset. In Table 2, we give the percentage of the IP space that is covered by these spaces, along with their respective contribution to the total volume of spam.

More specifically, in the data from 2006, we can identify three high-activity spamming chunks of IPs (the first row in Table 1), which constitute 22.6% of the total IP address space[4], and are the origin of 92% of the total amount of spam that was received in 2006. This result barely follows the Pareto principle that we mentioned before. In addition, it indicates that, by applying some kind of traffic control on those three IP spaces, we could significantly reduce the volume of spam received.

In the 2007 data, the percentage covered by high-activity areas (presented in the second row in Table 1) rises to 29.3% of the total IP space, and is responsible for 95% of the total volume of received spam. Furthermore, the high-activity chunks of 2006 are only a subset of the respective spamming chunks of 2007 – an observation that shows a spreading of spammers over the IP space. In the data from 2008, we again identify three high-activity areas (third row in Table 1), which are the cause of 91.5% of the total volume of spam, and constitute 32.4% of the total IP address space. A similar argument can be made for the high-activity spamming IPs of 2009 (fourth row in Table 1): these chunks are responsible for 93.4% of the total amount of spam, while they cover 34.4% of the IP space.

## NEW FINDINGS

In Figure 2 we present the spam Cumulative Distribution Function (CDF) for each of the last four years. In

[4] In our study we considered all the valid IP addresses (i.e. allocated, unallocated and reserved) as IP space.

| Year | Space A | Space B | Space C |
|---|---|---|---|
| 2006 | 58.* – 73.*<br>80.* – 90.* | – | 190.* – 222.* |
| 2007 | 57.* – 92.* | 121.* – 126.* | 188.* – 222.* |
| 2008 | 57.* – 96.* | 116.* – 126.* | 188.* – 222.* |
| 2009 | 57.* – 97.* | 113.* – 126.* | 188.* – 222.* |

*Table 1: Active IP chunks between 2006 and 2009.*

| Year | Active IP space (% of the total IP space) | Volume of spam (% of the total volume) |
|---|---|---|
| 2006 | 22.6 | 92.0 |
| 2007 | 29.3 | 95.0 |
| 2008 | 32.4 | 91.5 |
| 2009 | 34.4 | 93.4 |

*Table 2: Contribution in total received volume of spam of the active spamming IP spaces between 2006 and 2009.*

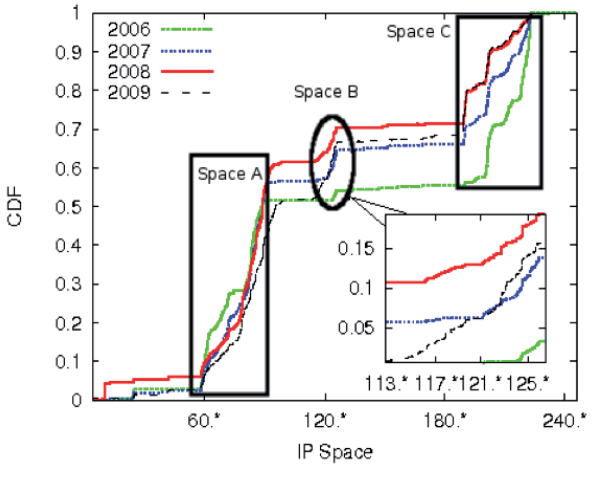



*Figure 2: The cumulative distribution of spamming activity across the IP space over the last four years. We show the two high-activity areas (left and right boxes) and an emerging high-activity area (middle box) not reported so far.*

Table 1, we list the high-activity IP spaces with respect to spamming. The first unexpected observation is the intense spamming activity of the IP space between 113.* and 126.*. To the best of our knowledge, no one so far has observed high spam activity in this area (shown as an inset in Figure 2). Note that spaces A and C were reported by previous studies [2], which increases the confidence in our dataset. This new space shows low spam intensity in 2007 but by 2009, it has become one of the three major spamming IP areas, serving as the origin of 15% of the received volume

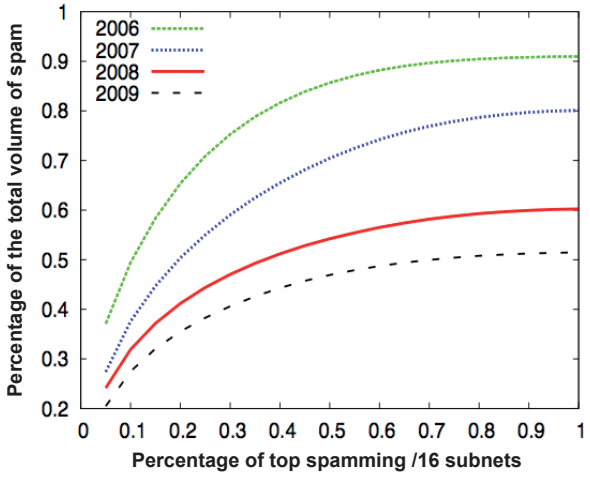



*Figure 3: The cumulative percentage of spamming contribution of the common /16 prefixes for the last four years. The activity becomes less concentrated from 2006 to 2009, which indicates that more spam is distributed among new /16 subnets across the IP space.*

of spam in 2009 while constituting only 5% of the total IP space.

The next important observation has to do with the 'spreading' trend of spamming activity across the IP space between 2006 and 2009. This 'spreading' observation is supported by two facts: (a) a new active area has emerged (2007–2009, as described before), and (b) the known major spamming areas became wider as of 2006 (shown in both Table 1 and Figure 2).

There are several different ways to quantify this trend. For example, in 2006, the high-activity spaces covered 22.6% of the total IP space. This percentage increased every year and peaked at 34.4% in 2009, illustrating the spreading trend of the spamming areas.

Another way to show this 'spreading' is to focus on the spam activity of the /16 subnets that were active throughout the period covered by the data. In Figure 3, we plot the cumulative percentage of the spam activity of these /16 prefixes as a percentage of the total received spam in each year. Note that the total on the y-axis does not add up to 100%, as there is contribution from subnets that were not part of the group we examined. The x-axis presents the active /16 prefixes, in order of decreasing activity. Conceptually, the closer the line is to the upper left corner, the more concentrated the spamming activity. In 2006, almost 90% of the total volume of received spam originated from these subnets. In the following years, the contribution of these subnets steadily decreased, dropping down to 52% in 2009. This indicates that over time, new IPs become responsible for an increasing portion of the total volume of received spam.

## DISCUSSION

The implications of the two observations that we made from our analysis need to be discussed further. The spreading trend indicates that IP-filtering can barely keep up with bots. This is due to the fact that spammers seem to exploit the entire active IP space[5], by constantly crawling[6] the Internet and recruiting new members.

Another important point is the rapid expansion of botnets to newly allocated IP spaces. According to IANA[7], the /8 subnets 121.* to 123.* were allocated for the first time in 2006 and by 2007, they were already part of the high-activity spamming subnets. The same happened for /8 subnets 114.* to 120.* a year later.

## CONCLUSION

We have described an empirical study of a publicly available archive of spam messages gathered during the last four years. Our analysis has revealed a worrying trend: spamming bots seem to have spread wider across the IP space since 2006. This spreading has major implications since IP-based filtering for bots and spam is becoming more challenging. At the moment, it seems like security administrators may be losing the war against botmasters.

## REFERENCES

[1] Husain, H.; Phithakkitnukoon, S.; Palla, S.; Dantu, R. Behavior analysis of spam botnets. COMSWARE. 2008.

[2] Ramachandran, A.; Feamster, N. Understanding the network-level behavior of spammers. SIGCOMM. 2006.

[3] Yinglian, X.; Yu, F.; Achan, K.; Panigrahy, R.; Hulten, G.; Osipkov, I. Spamming botnets: Signatures and characteristics. SIGCOMM. 2008.

[4] Zesheng, C.; Ji, C.; Barford, P. Spatial-temporal characteristics of internet malicious sources. INFOCOM. 2008.

[5] Spam. Archive. http://untroubled.org/spam/.

[5] Active IP space: subnets that are both allocated and active.

[6] Crawling the Internet means that some bots which are already members of the army find new unprotected machines across the active IP space and compromise them.

[7] The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of IP addressing.

# COMPARATIVE REVIEW

## WINDOWS SERVER 2008 STANDARD EDITION SP2 X86

*John Hawes*

Our second visit to *Microsoft*'s *Server 2008* platform could also be our last in its current incarnation, with the imminent and much anticipated release of *Windows 7* now just a few weeks away. While *Vista*, which seems doomed to fade into history with the early arrival of a replacement, will not be missed by most users (even those who have got around to adopting it), the server edition that accompanied it has proved a much finer package, easily eclipsing the earlier *2003 Server* in terms of speed, stability and general likeability. Looking forward, we hope the R2 edition will produce more of the same, and we will monitor its uptake among users before deciding whether to cease testing on the original version.

With the annual *VB* conference taking the whole team out of the lab for a full week in the middle of testing this month, we knew in advance that timing would be a major issue, and with the ever-growing numbers of products entering our desktop tests it was clear that running a less well-subscribed server test would be the only way to survive the month. As it was, the test still proved popular, with some 26 products making the final cut on the deadline day.

### PLATFORM AND TEST SETS

Setting up the test systems is by now fairly routine, with the application of a service pack to existing images not taking too much time or effort. As mentioned, the platform offers a much less frustrating user experience than its desktop sibling *Vista*, with all the required tools fairly close at hand. One step we did take to simplify matters was to disable the UAC system, assuming that an administrator operating his own server would know his business and would not want to be interrupted by intrusive pop-ups during software set-up. After having experienced some serious problems with system crashes in the recent *Vista* test (see *VB*, August 2009, p.14), we ran a few tests on the hardware to ensure there were no problems, and planned to watch out for any repetition of the worrying trend during the weeks ahead.

The deadline for product submissions was set for 26 August. Test sets were aligned with the July issue of the WildList and standard sets, including the clean sets, were frozen on 22 August. Of course, we continued collecting samples for a further week after the product submission deadline to complete our RAP sets.

In the WildList set there were few items of interest – a smattering of the usual suspects mostly targeting online gamers and social networkers – but a couple of variants of W32/Virut, both added more recently than the one which caused some upsets in the last comparative, looked likely to produce some difficulties of their own. Voraciously infectious and demonstrating highly complex polymorphism, they seemed certain to provide a stiff challenge to the detection capabilities of the products under test, and were added to our set in large numbers to provide a good measure of how thoroughly detection had been implemented.

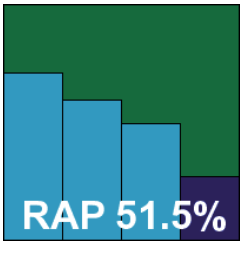
Elsewhere there were few changes beyond some further expansion of some of the other Virut strains recently relegated to the polymorphic test set. A minor update was made to our clean sets, with no obscure or unusual samples likely to trip any heuristics. The speed sets did see something of an overhaul, following up on some of the housecleaning done on the clean sets in recent months, with a fair number of older and rarer samples removed and replaced with more recent samples from major software providers. As this set is designed to measure speed only, we do our best to avoid including any files which are likely to cause false alarms, but nevertheless the occasional product will skew its speed figures by alerting on something in here and the set is officially included as part of our false positive test. Further updates to the speed testing system, along with ongoing overhauls of other areas, should, we hope, be in place in time for the next comparative.

With everything set up for the test, we got to work ploughing through the field of products with only a couple of weeks in which to get the bulk of testing out of the way, putting a great deal of trust in the stability of the platform to minimize the impact of any bad behaviour on the part of the products.

### AhnLab V3Net for Windows Servers 7.0.2.2 build 963

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 99.56% |
| **ItW (o/a)** | 99.99% | **Trojans** | 75.83% |
| **Worms & bots** | 99.79% | **False positives** | 0 |

*AhnLab*'s server-oriented product seems fairly similar to the desktop range commented on in the last review (see *VB*, August 2009, p.14), with a nice speedy installation and a fairly pleasant-looking interface. This similarity extended to a relative shortage of configuration options,

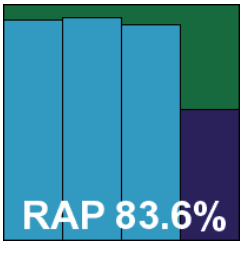


which many server administrators may find inadequate for their needs. We also found the splitting of scanning and detections into separate sections headed 'virus' and 'spyware' not only rather senseless in this modern age of boundary-stretching threats, but also somewhat confusing and on occasion dangerous. As noted before, while the on-access protection blocked most items on our list, some seemed to be spotted first by the spyware side, which meant that blocking was not implemented. With the spyware module disabled, protection from more serious threats actually seems to improve.

With these initial frustrations worked out, running through the tests went fairly smoothly with no repeat of the problems with logging and crashes noted in the last comparative. Scanning speeds were fairly reasonable, looking better on access thanks to the highly limited selection of files actually scannable, and detection rates seemed fairly decent too, with levels dropping in fairly steep steps throughout the RAP sets. Despite all looking good in the clean sets, a fair number of samples of one of the W32/Virut strains on the WildList were not detected, and *AhnLab* thus misses out on a VB100 this month.

## Alwil avast! Professional 4.8.1099

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 99.32% |
| **ItW (o/a)** | 100.00% | **Trojans** | 94.99% |
| **Worms & bots** | 99.96% | **False positives** | 0 |

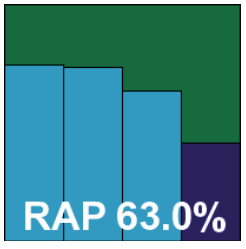




*Alwil*'s product is another that looks and feels identical to the desktop edition, and again comes with its own selection of oddities and idiosyncrasies of design and layout; a new version, believed to be on the verge of release, is hotly anticipated. Navigating the rather complex process of designing scan tasks, and monitoring them through a system which seems to refresh irregularly and not always very cleanly, is not a great problem though, and a full set of configuration should allow even the most demanding of admins to protect their servers in any manner desired.

Scanning speeds were excellent, even with more thorough settings selected, and detection rates pretty superb too, with a very commendable average achieved in the RAP test despite a fair sized drop in the week +1 set. False positives were entirely absent, and misses absent from the WildList set, thus setting *Alwil* on course to take the first VB100 award of this month's comparative.

## Authentium Command Anti-Malware 5.0.8

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 99.65% |
| **ItW (o/a)** | 99.99% | **Trojans** | 66.42% |
| **Worms & bots** | 100.00% | **False positives** | 0 |



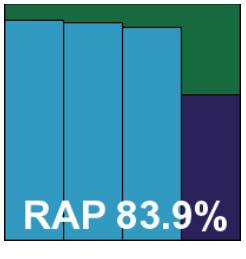

*Authentium*'s *Command* product is a semi-regular entrant in our comparatives, and only decided at the last minute to join this one, but is always welcome thanks to simple design and stable behaviour. The interface, unchanged from its last appearance, is pared down in the extreme, but still provides a few basic options, most of which require the 'advanced' option to be selected before they can be accessed. A couple of items which did slow down the test this month were a lack of information on the logging and archive handling, which is all in place but a little vague, and the apparent failure of the scheduler to fire up the scans we diligently prepared to run overnight.

Nevertheless, the tests were soon completed. Scanning speeds were around the mid range, with on-access overheads perhaps a little heavier than expected. Detection rates were decent too, somewhat improved over recent performances and surprisingly doing slightly better in the reactive part of the RAP sets than in the older samples in the trojans set. All looked pretty good, but in the WildList set those large collections of W32/Virut variants took another victim, with around 10% of samples of the most recent strain missed. *Authentium* thus does not quite make the cut for a VB100 award this time.

## AVG Internet Security Network Edition 8.5.409

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 99.06% |
| **ItW (o/a)** | 100.00% | **Trojans** | 93.57% |
| **Worms & bots** | 99.96% | **False positives** | 0 |

*AVG* opted to enter a standard desktop suite, although this time it was a business-oriented version compatible with remote administration tools. Installation was simple, fast and easy, with no reboot required, and on the surface the control centre looks much as

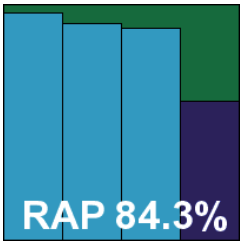
| On-demand detection | WildList | | Worms & bots | | Polymorphic viruses | | Trojans | | Clean sets |
|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | Missed | % | Missed | % | FP |
| AhnLab V3Net | 171 | 99.99% | 5 | 99.79% | 24 | 99.56% | 3167 | 75.83% | 0 |
| Alwil avast! | 0 | 100.00% | 1 | 99.96% | 7 | 99.32% | 656 | 94.99% | 0 |
| Authentium Command | 159 | 99.99% | 0 | 100.00% | 15 | 99.65% | 4400 | 66.42% | 0 |
| AVG I.S. Network Edition | 0 | 100.00% | 1 | 99.96% | 25 | 99.06% | 843 | 93.57% | 0 |
| Avira AntiVir Server | 1 | 99.99997% | 0 | 100.00% | 0 | 100.00% | 162 | 98.76% | 0 |
| BitDefender Security | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 2244 | 82.87% | 0 |
| CA eTrust | 0 | 100.00% | 0 | 100.00% | 1750 | 92.34% | 8079 | 38.35% | 0 |
| eScan Internet Security | 0 | 100.00% | 1 | 99.96% | 0 | 100.00% | 2202 | 83.19% | 0 |
| ESET NOD32 | 0 | 100.00% | 0 | 100.00% | 2 | 99.998% | 968 | 92.61% | 0 |
| Filseclab Twister | 5655 | 95.54% | 354 | 85.29% | 10001 | 33.69% | 5213 | 60.22% | 1 |
| Fortinet FortiClient | 38 | 99.999% | 0 | 100.00% | 4 | 99.70% | 2403 | 81.66% | 0 |
| Frisk F-PROT | 159 | 99.99% | 0 | 100.00% | 12 | 99.78% | 4291 | 67.25% | 0 |
| F-Secure Anti-Virus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1165 | 91.11% | 0 |
| G Data AntiVirus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 228 | 98.25% | 0 |
| Ikarus virus.utilities | 3759 | 99.87% | 3 | 99.88% | 5754 | 73.93% | 191 | 98.54% | 4 |
| K7 Total Security | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1822 | 86.09% | 0 |
| Kaspersky Anti-Virus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1278 | 90.24% | 0 |
| Kingsoft I.S. 2009 Advanced | 98 | 99.996% | 10 | 99.58% | 3282 | 61.94% | 10327 | 21.20% | 0 |
| Kingsoft I.S. 2009 Standard | 2461 | 99.91% | 11 | 99.54% | 4572 | 59.94% | 12161 | 7.20% | 0 |
| McAfee VirusScan Enterprise | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1229 | 90.62% | 0 |
| Microsoft Forefront | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 973 | 92.57% | 0 |
| Quick Heal AntiVirus Lite | 0 | 100.00% | 3 | 99.88% | 150 | 98.28% | 2436 | 81.41% | 0 |
| Sophos Anti-Virus | 1 | 99.99997% | 0 | 100.00% | 0 | 100.00% | 1231 | 90.60% | 0 |
| Symantec Endpoint Protection | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1031 | 92.13% | 0 |
| Trustport Antivirus 2009 | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 265 | 97.97% | 0 |
| VirusBuster for Servers | 5 | 99.9998% | 2 | 99.92% | 193 | 90.43% | 2631 | 79.92% | 0 |

we have come to expect lately: smooth and professional, with an abundance of icons leading to various protective modules. The layout is easy to navigate and provides a reasonable if not quite exhaustive level of configuration, and testing ran smoothly and without issues.

Scanning speeds were reasonable in both modes across the speed sets, although our heavily enlarged clean set with many multi-layered archives did take some time to trawl through, and in the infected sets detection rates were pretty excellent across the board, with a superb showing in the RAP sets. With no issues with false alarms or in the WildList, *AVG* comfortably takes home a VB100 award.

## Avira AntiVir Server 9.00.00.25

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 99.99% | **Trojans** | 98.76% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

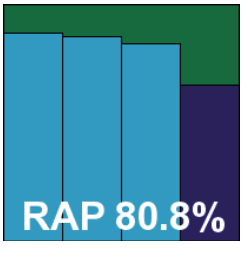



The first proper server version on offer this month, *Avira*'s product uses the standard MMC system to provide access to its controls, which seem fairly thorough once the layout has been deciphered. Options to exclude handling of selected *Windows* services seemed an especially appropriate addition for a server product. The setting up and running of scans required a little further investigation into the GUI design, and the monitoring of progress even more exploring, but scanning speeds made up for lost time with some decent speeds, perhaps not up to the usual excellent levels but quite acceptable. Some initial runs over the infected sets turned up a malformed file which seemed to cause the scanner some problems, shutting down the scan on several occasions and at one point apparently disabling the on-access scanner, although this effect could not be reproduced.

As in many recent tests, detection rates were quite remarkable throughout, with no false alarms despite the high detection rate. In the WildList however, a single item from one of the large sets of Virut samples was not detected. We retried the product over an even larger set generated during testing, and were able to find a further small handful of such samples to provide to the vendor for analysis. The incidence of missed samples was so low that we have had to expand the score table to fit in the required number of decimal places. Nevertheless, the rules of the VB100 are strict and this single miss is enough to deny *Avira* a VB100 award this month despite an otherwise superb performance.

## BitDefender Security for Windows Servers 3.3.54

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 82.87% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

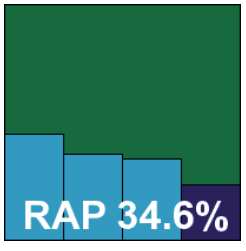




*BitDefender*'s offering is another proper server product, again using the MMC system and again finding it difficult to squeeze all the required controls and displays in without compromising usability somewhat. After a simple but rather sluggish installation, the interface presents a few challenges in navigation, lacking the smooth slickness of the desktop range, but once a few familiar paths have been uncovered it responds well and the whole solution runs in a stable, well-behaved manner.

Scanning speeds and overheads were fairly average, but detection levels were strong, with a solid showing in the proactive part of the RAP sets pushing the product's score up to a very respectable level. With no issues with any of the nasty polymorphic samples in the WildList or elsewhere, and no false alarms, *BitDefender* earns a VB100 award.

## CA eTrust 8.1.655.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 92.34% |
| **ItW (o/a)** | 100.00% | **Trojans** | 38.35% |
| **Worms & bots** | 100.00% | **False positives** | 0 |


*CA*'s business line continues with the same product as seen in many previous tests – however, some early peeks at an updated range point to a few changes yet to come as the company's partnership with *HCL* begins to show some signs of blossoming. The install is as ever lengthy, with a plethora of EULAs to agree to and a full page of personal data to fill in. Once up and running, response times were much better than they tend to be on *XP*, which made navigating the interface somewhat more pleasant, but as usual results are better ripped from raw logging data than viewed in the interface.

Scanning speeds remain hard to beat, although full measurements were not taken as the option to enable archive scanning on access, although present in the interface, remains non-functional. Detection rates seemed perhaps slightly improved compared to recent showings. This leaves a fair way to go, but the WildList and clean sets were handled ably and *CA* thus earns another VB100 award.

## eScan Internet Security 10.0.997.514

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 83.19% |
| **Worms & bots** | 99.96% | **False positives** | 0 |

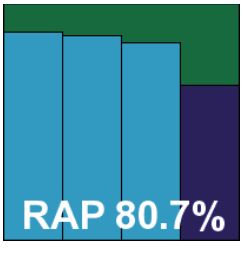
The people behind *eScan* have opted to remove their company name from promotion, so the results formerly listed under *MicroWorld* (and occasionally *MWTI*) will henceforth be referred to, more simply and more memorably, as *eScan*. The product is unchanged however,

| On-access detection | WildList | | Worms & bots | | Polymorphic viruses | | Trojans | | Clean sets |
|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | Missed | % | Missed | % | FP |
| AhnLab V3Net | 171 | 99.99% | 9 | 99.63% | 24 | 99.56% | 3356 | 74.39% | 0 |
| Alwil avast! | 0 | 100.00% | 1 | 99.96% | 7 | 99.32% | 656 | 94.99% | 0 |
| Authentium Command | 159 | 99.99% | 0 | 100.00% | 15 | 99.65% | 4587 | 65.00% | 0 |
| AVG I.S. Network Edition | 0 | 100.00% | 1 | 99.96% | 25 | 99.06% | 1084 | 91.72% | 0 |
| Avira AntiVir Server | 1 | 99.99997% | 0 | 100.00% | 0 | 100.00% | 162 | 98.76% | 0 |
| BitDefender Security | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 2335 | 82.18% | 0 |
| CA eTrust | 0 | 100.00% | 0 | 100.00% | 1750 | 92.34% | 8079 | 38.35% | 0 |
| eScan Internet Security | 0 | 100.00% | 4 | 99.83% | 0 | 100.00% | 2207 | 83.16% | 0 |
| ESET NOD32 | 0 | 100.00% | 0 | 100.00% | 4 | 99.995% | 840 | 93.58% | 0 |
| Filseclab Twister | 5655 | 95.54% | 384 | 84.05% | 10001 | 33.69% | 5526 | 57.83% | 1 |
| Fortinet FortiClient | 38 | 99.999% | 0 | 100.00% | 4 | 99.70% | 2404 | 81.65% | 0 |
| Frisk F-PROT | 159 | 99.99% | 0 | 100.00% | 12 | 99.78% | 4468 | 65.90% | 0 |
| F-Secure Anti-Virus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1677 | 87.20% | 0 |
| G Data AntiVirus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 228 | 98.25% | 0 |
| Ikarus virus.utilities | 3759 | 99.87% | 3 | 99.88% | 5754 | 73.93% | 191 | 98.54% | 4 |
| K7 Total Security | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 2013 | 84.63% | 0 |
| Kaspersky Anti-Virus | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1386 | 89.42% | 0 |
| Kingsoft I.S. 2009 Advanced | 98 | 99.996% | 10 | 99.58% | 3282 | 61.94% | 10397 | 20.66% | 0 |
| Kingsoft I.S. 2009 Standard | 2461 | 99.91% | 11 | 99.54% | 4572 | 59.94% | 12216 | 6.79% | 0 |
| McAfee VirusScan Enterprise | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1231 | 90.60% | 0 |
| Microsoft Forefront | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 973 | 92.57% | 0 |
| Quick Heal AntiVirus Lite | 0 | 100.00% | 6 | 99.75% | 179 | 96.10% | 5412 | 58.70% | 0 |
| Sophos Anti-Virus | 1 | 99.99997% | 0 | 100.00% | 0 | 100.00% | 1231 | 90.60% | 0 |
| Symantec Endpoint Protection | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1068 | 91.85% | 0 |
| Trustport Antivirus 2009 | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 418 | 96.81% | 0 |
| VirusBuster for Servers | 5 | 99.9998% | 2 | 99.92% | 193 | 90.43% | 2631 | 79.92% | 0 |

and has its usual simple and straightforward install and set-up process. Towards the end of installation we received a warning that a component had crashed, but this seemed to affect neither the install process nor the operation of the product. The interface is clean and unfussy, providing all the controls required.

The default setting limits scanning to files under 5MB, which helped us get through our large clean sets containing a number of big, deep archives and installer packages which can slow down more thorough scanners such as this.

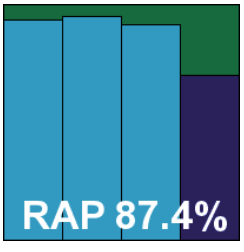
Nevertheless, the clean set took some time to get through, and the standard speed tests showed some fairly sluggish

speeds and hefty overheads. On a more positive note, detection rates continued to impress. The WildList, and indeed all the polymorphic samples tested, were handled without difficulty and no false alarms were raised in the clean set, thus earning *eScan* another VB100 award for its efforts.

## ESET NOD32 Antivirus 4.0.437.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 99.99% |
| **ItW (o/a)** | 100.00% | **Trojans** | 92.61% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

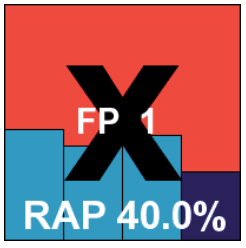

*ESET*'s product has a rapid and simple install process which comes to a halt on the question of handling 'potentially unwanted' items, a selection which has no default and requires some actual consideration from the user – reminding us that our procedures may need some adjustment to cope with such advanced thinking. With that minor hurdle quickly overcome, we soon had access to the interface, which remains extremely slick, stylish and attractive, and manages to combine ease of use with pretty thorough levels of configurability. A few features may require a little familiarity to find, while others, such as on-access archive handling, are absent, but in general all seems to be on hand.

Scanning speeds over the clean sets were no more than a slow average, and with several levels of on-access scanning affecting different access methods we were obliged to run the test by copying sets to the system, which took quite some time and on one occasion was interrupted by the system halting unexpectedly during the night.

When we finally got some figures down they showed some excellent detection rates, with commendably even scores across the trojans and the reactive parts of the RAP set indicating steady handling of new samples, and a splendid showing in the proactive set making for a very high overall average. A tiny number of samples from some older Virut variants were missed in the polymorphic set, but the newer ones on the official WildList were handled without issues. With no false positives *ESET* is the worthy winner of yet another VB100 award, thus maintaining *NOD32*'s position as the product with the largest number of VB100 awards.

## Filseclab Twister AntiVirus 7.3.2.9971

| | | | |
|---|---|---|---|
| **ItW** | 95.54% | **Polymorphic** | 33.69% |
| **ItW (o/a)** | 95.54% | **Trojans** | 60.22% |
| **Worms & bots** | 85.29% | **False positives** | 1 |




*Filseclab* bravely returns for another run in the VB100, having shown gradual improvements over its first few attempts. The install process remains simple and very speedy, although it does require a reboot to complete. The main interface is quite appealing, and a decent degree of configuration is tucked away underneath, albeit in slightly less stylish settings. The product also includes a range of other features beyond standard anti-malware, including a HIPS set-up, which is really its main strength, and also a 'Fix Windows' area which tweaks and adjusts a number of settings, putting the system into a safer state either after an infection or simply on spotting some of the notoriously insecure defaults in most *Windows* versions.

On-demand scanning speeds were fairly modest, and on-access protection is implemented in a rather unconventional manner, with no instant blocking of files but alerts, actions and log entries appearing soon after an infected file is accessed. This makes our standard on-access speed measurement somewhat unreliable, but as some slowdown was observed despite the lack of file access interception we opted to record it out of interest. Detection rates still lag behind somewhat, but seem to be improving, with only a single false alert generated in the much-expanded clean set. In the WildList, a fair number of recent items were not properly handled, with fairly large swathes of both Virut strains missed too, and *Filseclab* will have to keep working its way towards a VB100 award.

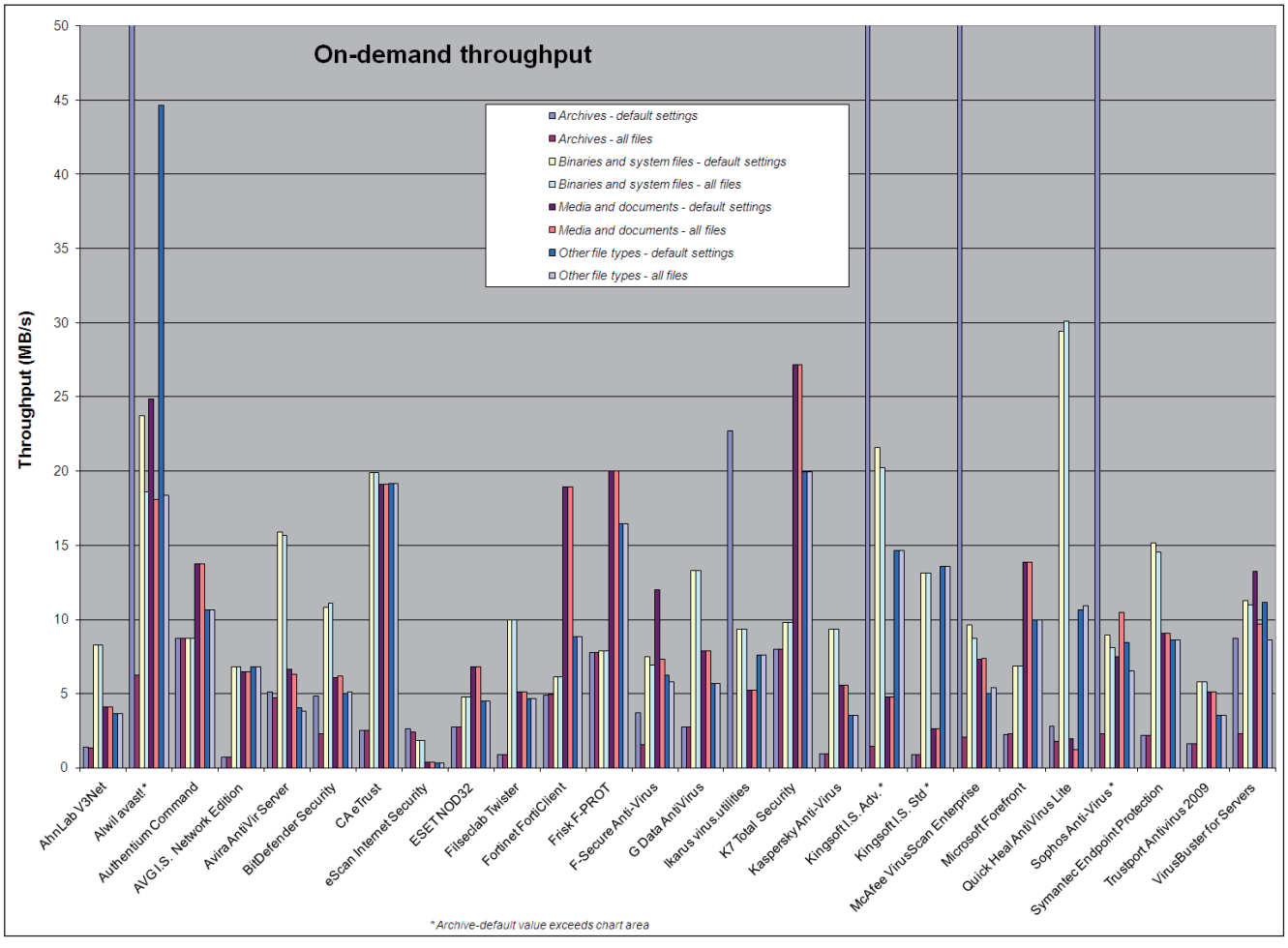
## Fortinet FortiClient Endpoint Security 4.0.1.54

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 99.70% |
| **ItW (o/a)** | 99.99% | **Trojans** | 81.66% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

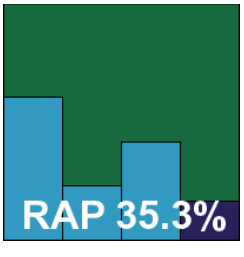
*Fortinet*'s install process is slowed by some warning pop-ups from *Windows*, most of which can be suppressed by instructing the system to 'always trust' *Fortinet* as a software provider; it seems likely that more pop-ups would be evident were the UAC system active. Once up and running though, the product looks good and runs well.

| Archive scanning | | ACE | CAB | EXE-ZIP | JAR | LZH | RAR | TGZ | ZIP | EXT* |
|---|---|---|---|---|---|---|---|---|---|---|
| AhnLab V3Net I.S. | Default | 9/√ | 9/√ | 9/√ | 9/√ | 9/√ | 9/√ | X | 9/√ | √ |
| | All | X | X | X | X | X | X | X | X | X |
| Alwil avast! | Default | X/√ | X/√ | √ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| | All | X/√ | X/√ | √ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Authentium Command | Default | X | 5 | 5 | 5 | √ | 5 | 2 | 5 | √ |
| | All | X | X/4 | X/4 | X/4 | X/√ | X/4 | X/2 | X/4 | X/√ |
| AVG I.S. Network Edition | Default | X | √ | √ | √ | √ | √ | √ | √ | X |
| | All | X | X | X | X | X | X | X | X | √ |
| Avira AntiVir Server | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| BitDefender Security | Default | √ | √ | 8 | √ | √ | √ | 8 | √ | √ |
| | All | X/√ | X/√ | √ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| CA eTrust | Default | X | √ | X | √ | √ | √ | √ | √ | √ |
| | All | X | X | X | 1 | X | X | X | 1 | √ |
| eScan Internet Security | Default | √ | √ | 8 | √ | √ | √ | 8 | √ | √ |
| | All | X/√ | X/√ | X/8 | X/√ | X/√ | X/√ | X/8 | X/√ | √ |
| ESET NOD32 | Default | √ | √ | √ | √ | √ | √ | 5 | √ | √ |
| | All | X | X | X | X | X | X | X | X | √ |
| Filseclab Twister | Default | 5 | 3 | 3 | 4 | 1 | 4 | X | 5 | √ |
| | All | X | X | X | X | X | 1 | X | 2 | X |
| Fortinet FortiClient | Default | X/√ | √ | √ | √ | √ | √ | √ | 4 | √ |
| | All | X/√ | √ | √ | √ | √ | √ | √ | 4 | √ |
| Frisk F-PROT Antivirus | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X | X | 2 | 2 | X | X | X | 2 | √ |
| F-Secure Anti-Virus | Default | X/√ | √ | √ | √ | √ | √ | √ | √ | X/√ |
| | All | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| G Data AntiVirus | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | √ | √ | 4 | √ | √ | √ | 7 | 8 | √ |
| Ikarus virus.utilities | Default | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | √ |
| | All | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | √ |
| K7 Total Security | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | 1 | X | 1 | 1 | X | X | X | 1 | √ |
| Kaspersky Anti-Virus | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Kingsoft I.S. 2009 Advanced | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X | X | X | X | X | X | X | X | √ |
| Kingsoft I.S. 2009 Standard | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X | X | X | X | X | X | X | X | √ |
| McAfee VirusScan Enterprise | Default | X/2 | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| | All | X/2 | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Microsoft Forefront | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X | X | 1 | X | X | X | X | 1 | √ |
| 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 |
| 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 | X | 3/√ | 3/√ | 3/√ | 3/√ | 3/√ | X/5 | 3/√ | √ |
| | All | X | X | X | X | X | X | X | X | √ |
| Trustport Antivirus | Default | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | All | X/√ | X/√ | X/√ | 1/√ | X/√ | X/√ | X/√ | 1/√ | √ |
| VirusBuster for Servers | Default | 2 | √ | √ | X/√ | X | √ | √ | √ | X/√ |
| | 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




A logical layout provides easy access to a very satisfactory range of options, quite suited to the business audience the firm targets.



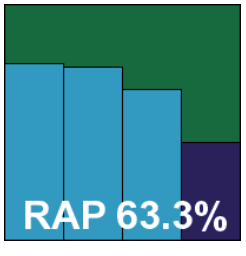

Scanning speeds were pretty decent and overheads low, and detection rates showed considerable improvement over recent tests as more of the product's optional 'extended databases' seem to have been moved to the default set-up – we noted a further jump in detection when these full databases were activated. RAP scores were somewhat uneven, and here the increased detection from the extended data was particularly significant.

No problems were found in the clean set, but in the WildList a small handful of samples of one of the Virut strains were not detected. Although we were able to generate further undetected samples to provide to the vendor fairly easily, the company's own research produced no more from batches in the tens of thousands of samples, indicating that the issue only affects a very small proportion of potential infections. Nevertheless, the misses are considered enough to deny *Fortinet* a VB100 award this month.

## Frisk F-PROT Antivirus 6.0.9.3

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 99.78% |
| **ItW (o/a)** | 99.99% | **Trojans** | 67.25% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*F-PROT* has a fairly speedy install process, although we found the phrasing of the licensing page somewhat confusing, and a reboot is required to complete. The interface remains minimalist in the extreme, with very little by way of configuration and some of what

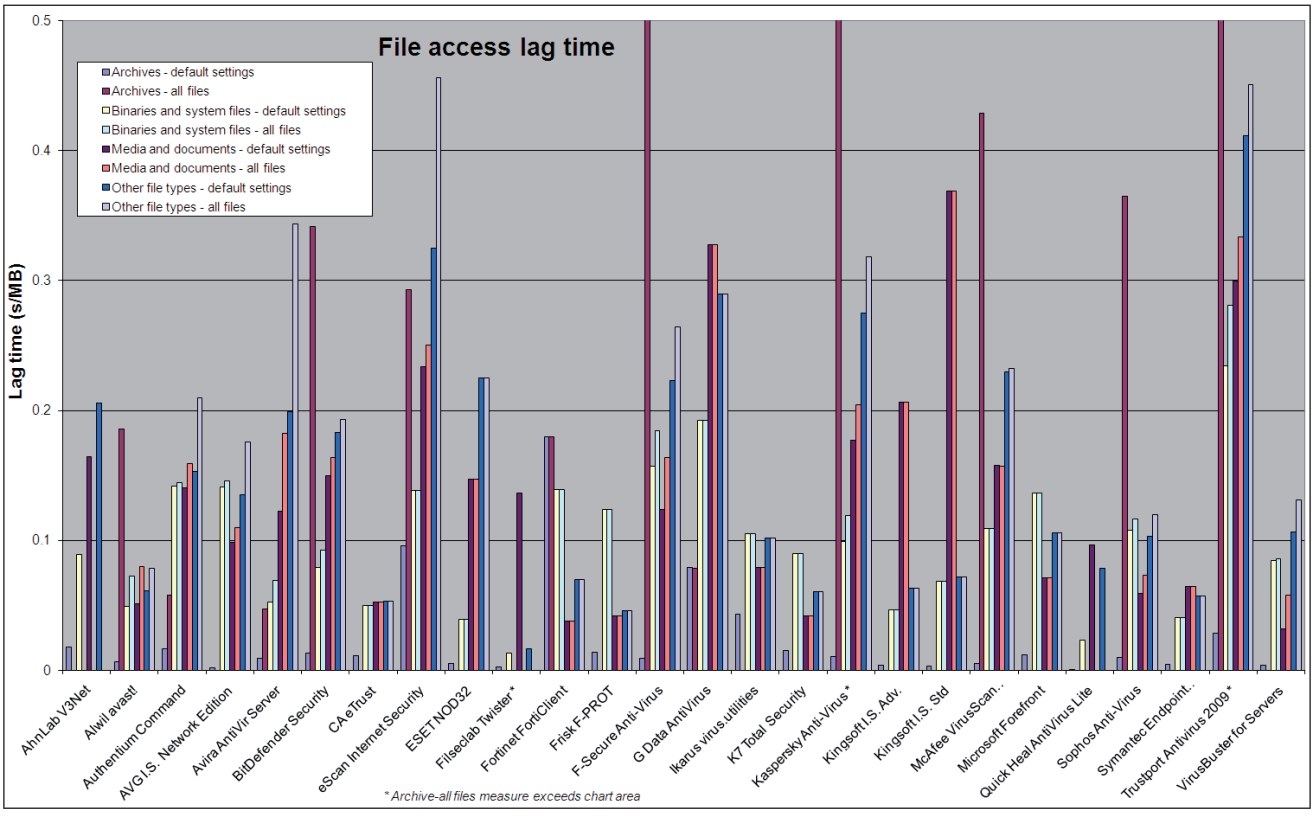


| **On-demand throughput** (Time = s; Throughput = MB/s) | Archive files | | | | Binaries and system files | | | | Media and documents | | | | Other file types | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Default settings | | All files | | Default settings | | All 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 |
| AhnLab | 2138 | 1.41 | 2186 | 1.37 | 312 | 8.30 | 312 | 8.30 | 501 | 4.12 | 501 | 4.12 | 258 | 3.64 | 258 | 3.64 |
| Alwil | 12 | 250.40 | 481 | 6.25 | 109 | 23.76 | 139 | 18.63 | 83 | 24.87 | 114 | 18.10 | 21 | 44.67 | 51 | 18.39 |
| Authentium | 343 | 8.76 | 343 | 8.76 | 297 | 8.72 | 297 | 8.72 | 150 | 13.76 | 150 | 13.76 | 88 | 10.66 | 88 | 10.66 |
| AVG | 4255 | 0.71 | 4255 | 0.71 | 381 | 6.80 | 381 | 6.80 | 318 | 6.49 | 318 | 6.49 | 138 | 6.80 | 138 | 6.80 |
| Avira | 585 | 5.14 | 635 | 4.73 | 163 | 15.89 | 165 | 15.69 | 309 | 6.68 | 328 | 6.29 | 231 | 4.06 | 245 | 3.83 |
| BitDefender | 619 | 4.85 | 1302 | 2.31 | 239 | 10.83 | 233 | 11.11 | 340 | 6.07 | 334 | 6.18 | 186 | 5.04 | 182 | 5.15 |
| CA | 1177 | 2.55 | 1177 | 2.55 | 130 | 19.92 | 130 | 19.92 | 108 | 19.11 | 108 | 19.11 | 49 | 19.14 | 49 | 19.14 |
| eScan | 1129 | 2.66 | 1254 | 2.40 | 1404 | 1.84 | 1408 | 1.84 | 4936 | 0.42 | 4936 | 0.42 | 2879 | 0.33 | 2879 | 0.33 |
| ESET | 1084 | 2.77 | 1084 | 2.77 | 543 | 4.77 | 543 | 4.77 | 302 | 6.83 | 302 | 6.83 | 208 | 4.51 | 208 | 4.51 |
| Filseclab | 3330 | 0.90 | 3330 | 0.90 | 259 | 10.00 | 259 | 10.00 | 401 | 5.15 | 401 | 5.15 | 201 | 4.67 | 201 | 4.67 |
| Fortinet | 609 | 4.93 | 609 | 4.93 | 422 | 6.14 | 422 | 6.14 | 109 | 18.94 | 109 | 18.94 | 106 | 8.85 | 106 | 8.85 |
| Frisk | 386 | 7.78 | 386 | 7.78 | 327 | 7.92 | 327 | 7.92 | 103 | 20.04 | 103 | 20.04 | 57 | 16.46 | 57 | 16.46 |
| F-Secure | 803 | 3.74 | 1872 | 1.61 | 346 | 7.48 | 373 | 6.94 | 172 | 12.00 | 282 | 7.32 | 150 | 6.25 | 162 | 5.79 |
| G Data | 1087 | 2.76 | 1087 | 2.76 | 195 | 13.28 | 195 | 13.28 | 262 | 7.88 | 262 | 7.88 | 165 | 5.69 | 165 | 5.69 |
| Ikarus | 132 | 22.76 | NA | NA | 277 | 9.35 | 277 | 9.35 | 392 | 5.27 | 392 | 5.27 | 123 | 7.63 | 123 | 7.63 |
| K7 | 375 | 8.01 | 375 | 8.01 | 264 | 9.81 | 264 | 9.81 | 76 | 27.16 | 76 | 27.16 | 47 | 19.96 | 47 | 19.96 |
| Kaspersky | 3120 | 0.96 | 3120 | 0.96 | 277 | 9.35 | 277 | 9.35 | 370 | 5.58 | 370 | 5.58 | 265 | 3.54 | 265 | 3.54 |
| Kingsoft Adv. | 17 | 176.75 | 2084 | 1.44 | 120 | 21.58 | 128 | 20.23 | 431 | 4.79 | 433 | 4.77 | 64 | 14.66 | 64 | 14.66 |
| Kingsoft Std | 3291 | 0.91 | 3291 | 0.91 | 197 | 13.14 | 197 | 13.14 | 775 | 2.66 | 775 | 2.66 | 69 | 13.60 | 69 | 13.60 |
| McAfee | 26 | 115.57 | 1451 | 2.07 | 268 | 9.66 | 297 | 8.72 | 282 | 7.32 | 279 | 7.40 | 186 | 5.04 | 173 | 5.42 |
| Microsoft | 1315 | 2.29 | 1315 | 2.29 | 376 | 6.89 | 376 | 6.89 | 149 | 13.85 | 149 | 13.85 | 94 | 9.98 | 94 | 9.98 |
| Quick Heal | 1058 | 2.84 | 1674 | 1.79 | 88 | 29.42 | 86 | 30.11 | 323 | 6.39 | 328 | 6.29 | 118 | 7.95 | 131 | 7.16 |
| Sophos | 20 | 150.24 | 1307 | 2.30 | 288 | 8.99 | 318 | 8.14 | 275 | 7.51 | 197 | 10.48 | 111 | 8.45 | 143 | 6.56 |
| Symantec | 1363 | 2.20 | 1368 | 2.20 | 171 | 15.14 | 178 | 14.55 | 228 | 9.05 | 228 | 9.05 | 109 | 8.61 | 109 | 8.61 |
| Trustport | 1807 | 1.66 | 1807 | 1.66 | 444 | 5.83 | 444 | 5.83 | 403 | 5.12 | 403 | 5.12 | 263 | 3.57 | 263 | 3.57 |
| VirusBuster | 343 | 8.76 | 1302 | 2.31 | 230 | 11.26 | 235 | 11.02 | 156 | 13.23 | 213 | 9.69 | 84 | 11.17 | 109 | 8.61 |

is available seems rather improbable – few other products offer the option to only detect *Microsoft Office*-related malware.

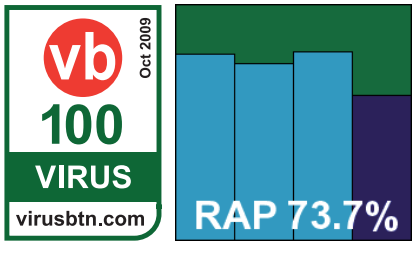
Scanning speeds were impressive and on-access overheads feather-light. A few times during on-demand scans the product tripped up and presented its own error console report, but on-access protection remained stable and restarting the scan proved simple. Detection rates were decent, with some good improvement in the RAP scores, and the clean set was also handled with aplomb.

As expected from the results of other products based on *Frisk*'s technology however, a handful of Virut samples were missed in the WildList set, and *F-PROT* does not win a VB100 award.




## F-Secure Anti-Virus for Windows Servers 8.01 build 207

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 91.11% |
| **Worms & bots** | 100.00% | **False positives** | 0 |







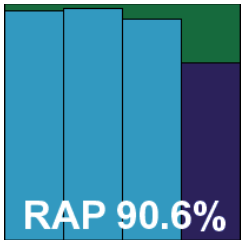
*F-Secure*'s server product bears little evident difference from the standard desktop ranges. The install follows the standard path and needs no reboot, running through fairly speedily. The interface is simple, cool and clear with a good level of configuration, and scanning and protection throughout seemed stable and well-behaved.

For the on-demand scans of the infected sets a command-line tool was used, as logging issues have caused problems in the past, but for all other tests including the speed measurements standard GUI scans were used. These showed the usual rather heavy overheads on access, especially with full-depth scanning enabled (something not recommended by the manufacturer), but on-demand speeds were much more impressive. Detection rates were similarly impressive, scoring fairly well across the board, and with no problems in either the WildList or the clean sets, *F-Secure* thus comfortably earns another VB100 award.

## G Data AntiVirus 10.5.51.2

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

In the past *G Data* has mainly taken part in our desktop comparatives, missing out on the server tests, but it recently emerged that this was due to some miscommunication and the company does indeed

| **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 |
| AhnLab | 57 | 0.02 | NA | NA | 248 | 0.09 | NA | NA | 400 | 0.16 | NA | NA | 226 | 0.21 | NA | NA |
| Alwil | 22 | 0.01 | 563 | 0.19 | 144 | 0.05 | 205 | 0.07 | 166 | 0.05 | 225 | 0.08 | 91 | 0.06 | 108 | 0.08 |
| Authentium | 53 | 0.02 | 177 | 0.06 | 383 | 0.14 | 392 | 0.14 | 351 | 0.14 | 389 | 0.16 | 177 | 0.15 | 231 | 0.21 |
| AVG | 9 | 0.00 | NA | NA | 383 | 0.14 | 394 | 0.15 | 264 | 0.10 | 287 | 0.11 | 161 | 0.14 | 198 | 0.18 |
| Avira | 30 | 0.01 | 145 | 0.05 | 154 | 0.05 | 196 | 0.07 | 314 | 0.12 | 437 | 0.18 | 220 | 0.20 | 356 | 0.34 |
| BitDefender | 42 | 0.01 | 1031 | 0.34 | 223 | 0.08 | 256 | 0.09 | 371 | 0.15 | 399 | 0.16 | 205 | 0.18 | 215 | 0.19 |
| CA | 38 | 0.01 | NA | NA | 147 | 0.05 | 147 | 0.05 | 170 | 0.05 | 170 | 0.05 | 84 | 0.05 | 84 | 0.05 |
| eScan | 291 | 0.10 | 885 | 0.29 | 376 | 0.14 | 376 | 0.14 | 543 | 0.23 | 577 | 0.25 | 338 | 0.32 | 462 | 0.46 |
| ESET | 19 | 0.01 | NA | NA | 119 | 0.04 | 119 | 0.04 | 365 | 0.15 | 365 | 0.15 | 245 | 0.23 | 245 | 0.23 |
| Filseclab | 11 | 0.00 | NA | NA | 52 | 0.01 | NA | NA | 342 | 0.14 | NA | NA | 49 | 0.02 | NA | NA |
| Fortinet | 544 | 0.18 | 544 | 0.18 | 377 | 0.14 | 377 | 0.14 | 139 | 0.04 | 139 | 0.04 | 100 | 0.07 | 100 | 0.07 |
| Frisk | 44 | 0.01 | NA | NA | 337 | 0.12 | 337 | 0.12 | 147 | 0.04 | 147 | 0.04 | 77 | 0.05 | 77 | 0.05 |
| F-Secure | 31 | 0.01 | 2529 | 0.84 | 424 | 0.16 | 494 | 0.18 | 316 | 0.12 | 399 | 0.16 | 243 | 0.22 | 282 | 0.26 |
| G Data | 240 | 0.08 | 240 | 0.08 | 515 | 0.19 | 515 | 0.19 | 737 | 0.33 | 737 | 0.33 | 305 | 0.29 | 305 | 0.29 |
| Ikarus | 134 | 0.04 | NA | NA | 289 | 0.11 | 289 | 0.11 | 225 | 0.08 | 225 | 0.08 | 129 | 0.10 | 129 | 0.10 |
| K7 | 48 | 0.01 | NA | NA | 250 | 0.09 | 250 | 0.09 | 148 | 0.04 | 148 | 0.04 | 91 | 0.06 | 91 | 0.06 |
| Kaspersky | 34 | 0.01 | 3772 | 1.25 | 274 | 0.10 | 325 | 0.12 | 426 | 0.18 | 482 | 0.20 | 292 | 0.28 | 332 | 0.32 |
| Kingsoft Adv. | 15 | 0.00 | NA | NA | 137 | 0.05 | 137 | 0.05 | 487 | 0.21 | 487 | 0.21 | 93 | 0.06 | 93 | 0.06 |
| Kingsoft Std | 14 | 0.00 | NA | NA | 194 | 0.07 | 194 | 0.07 | 822 | 0.37 | 822 | 0.37 | 101 | 0.07 | 101 | 0.07 |
| McAfee | 20 | 0.01 | 1293 | 0.43 | 296 | 0.11 | 300 | 0.11 | 386 | 0.16 | 385 | 0.16 | 249 | 0.23 | 252 | 0.23 |
| Microsoft | 39 | 0.01 | NA | NA | 370 | 0.14 | 370 | 0.14 | 207 | 0.07 | 207 | 0.07 | 133 | 0.11 | 133 | 0.11 |
| Quick Heal | 5 | 0.00 | NA | NA | 76 | 0.02 | NA | NA | 259 | 0.10 | NA | NA | 107 | 0.08 | NA | NA |
| Sophos | 32 | 0.01 | 1100 | 0.36 | 296 | 0.11 | 319 | 0.12 | 183 | 0.06 | 211 | 0.07 | 131 | 0.10 | 146 | 0.12 |
| Symantec | 18 | 0.00 | NA | NA | 122 | 0.04 | 122 | 0.04 | 194 | 0.06 | 194 | 0.06 | 87 | 0.06 | 87 | 0.06 |
| Trustport | 88 | 0.03 | 3138 | 1.04 | 623 | 0.23 | 744 | 0.28 | 679 | 0.30 | 749 | 0.33 | 420 | 0.41 | 456 | 0.45 |
| VirusBuster | 16 | 0.00 | NA | NA | 236 | 0.08 | 239 | 0.09 | 127 | 0.03 | 181 | 0.06 | 134 | 0.11 | 157 | 0.13 |

provide a full range of corporate and server solutions. Due to timing issues our first look at the server offering was provided in German only, but thanks to the remarkable linguistic talents of the lab team it was fairly simple both to set it up and to use it.

The install process involves setting up a management tool and deploying to individual clients (in this case the local machine) from there, but unlike many such tools it performed its task without fuss or obstacle, despite the language issue.

The control centre, based in the management tool, provides a detailed range of controls and monitoring tools, with some nice statistics reporting. The raw logging, required by us to gather detailed detection data, was a little gnarly

| Reactive And Proactive (RAP) detection scores | Reactive | | | Reactive average | Proactive | Overall average |
|---|---|---|---|---|---|---|
| | week -3 | week -2 | week -1 | | week +1 | |
| AhnLab V3Net | 70.60% | 59.20% | 49.30% | 59.70% | 27.00% | 51.53% |
| Alwil avast! | 93.20% | 94.30% | 91.50% | 93.00% | 55.40% | 83.60% |
| Authentium Command | 74.40% | 73.40% | 63.10% | 70.30% | 41.20% | 63.03% |
| AVG I.S. Network Edition | 92.60% | 91.70% | 90.00% | 91.43% | 61.10% | 83.85% |
| Avira AntiVir Server | 96.30% | 91.80% | 89.90% | 92.67% | 59.00% | 84.25% |
| BitDefender Security | 88.00% | 86.20% | 83.30% | 85.83% | 65.60% | 80.78% |
| CA eTrust | 44.60% | 36.20% | 34.40% | 38.40% | 23.10% | 34.58% |
| eScan Internet Security | 88.00% | 86.30% | 83.20% | 85.83% | 65.40% | 80.73% |
| ESET NOD32 | 93.40% | 94.80% | 91.20% | 93.13% | 70.00% | 87.35% |
| Filseclab Twister | 46.80% | 39.80% | 44.50% | 43.70% | 29.00% | 40.03% |
| Fortinet FortiClient | 60.50% | 23.00% | 41.50% | 41.67% | 16.10% | 35.28% |
| Frisk F-PROT | 74.60% | 73.40% | 63.90% | 70.63% | 41.40% | 63.33% |
| F-Secure Anti-Virus | 78.70% | 75.00% | 79.80% | 77.83% | 61.30% | 73.70% |
| G Data AntiVirus | 96.60% | 97.70% | 93.20% | 95.83% | 75.00% | 90.63% |
| Ikarus virus.utilities | 97.20% | 98.50% | 95.90% | 97.20% | 76.50% | 92.03% |
| K7 Total Security | 74.40% | 64.30% | 59.20% | 65.97% | 35.60% | 58.38% |
| Kaspersky Anti-Virus | 76.10% | 67.20% | 73.30% | 72.20% | 52.20% | 67.20% |
| Kingsoft I.S. 2009 Advanced | 28.40% | 24.30% | 31.10% | 27.93% | 17.50% | 25.33% |
| Kingsoft I.S. 2009 Standard | 15.00% | 12.30% | 21.20% | 16.17% | 8.00% | 14.13% |
| McAfee VirusScan Enterprise | 88.10% | 86.50% | 83.40% | 86.00% | 59.90% | 79.48% |
| Microsoft Forefront | 93.00% | 90.80% | 89.40% | 91.07% | 68.40% | 85.40% |
| Quick Heal AntiVirus Lite | 76.10% | 60.90% | 59.60% | 65.53% | 30.10% | 56.68% |
| Sophos Anti-Virus | 88.70% | 83.40% | 81.00% | 84.37% | 58.70% | 77.95% |
| Symantec Endpoint Protection | 94.30% | 91.30% | 50.70% | 78.77% | 24.40% | 65.18% |
| Trustport Antivirus 2009 | 98.20% | 98.50% | 96.80% | 97.83% | 77.60% | 92.78% |
| VirusBuster for Servers | 79.10% | 74.90% | 70.10% | 74.70% | 40.80% | 66.23% |

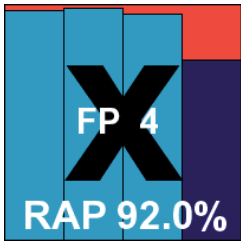
to handle and in places seemed a little malformed, perhaps due in part to the system halting unexpectedly during one of the heavier scan runs (we were delighted to note, however, that scanning continued where it had left off as soon as the system was back online).

In the final reckoning, we found just what we had expected from the multi-engine approach: some fairly slow scanning speeds but quite jaw-dropping detection rates, including an average of over 90% for the four weeks of the RAP test. With barely a thing missed anywhere including in the WildList, and no issues with false positives either, *G Data* easily wins another VB100 award.

## Ikarus virus.utilities 1.0.108

| | | | |
|---|---|---|---|
| **ItW** | 99.87% | **Polymorphic** | 73.93% |
| **ItW (o/a)** | 99.87% | **Trojans** | 98.54% |
| **Worms & bots** | 99.88% | **False positives** | 4 |

*Ikarus*, having first entered a *VB* comparative many years ago, became a semi-regular entrant in the tests for a while before dropping out of sight again for the past year. Back in again at last, we were intrigued to see what improvements had been made in the intervening months. Initially there was little to see, with the install and interface much as remembered, although the product's stability seemed greatly improved. The design is fairly basic and provides minimal configuration, and is occasionally a little tricky to navigate, but generally works well. On a couple of occasions we noticed the main interface freezing up for periods during on-access testing of large numbers of infected samples, but few real-world users are likely to put their product under such strain, and it soon righted itself once the bombardment was over.

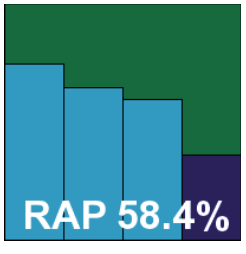



Looking through the results we saw some very good speeds in both measures, and detection results were really quite remarkable, powering effortlessly through the RAP and trojan sets with barely a sample undetected even in the week +1 set. Viruses proved to be less of a specialty however, with slightly lower scores in the polymorphic set and a fair number of Virut samples also not detected. Along with a handful of false positives from items recently added to the clean set, including files from major houses such as *Oracle* and *Sun Microsystems*, *Ikarus* does not quite reach the required standard for a VB100 award this time, and is also denied the chance to see its superb scores recorded on our cumulative RAP quadrant, but judging by the general excellence of detection looks likely to take its first award very soon.

## K7 Total Security Desktop Edition 10.0.0015

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 86.09% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*K7* has become a fixture in our tests in the past year or so, and has slowly drawn closer to the required mark, with its sporadic failures to achieve certification caused by increasingly minor issues. The now familiar product has an extremely fast and simple install process, and presents a pleasant and colourful interface which proved easy to navigate and use. A few problems did emerge during testing, including a dreaded blue screen during the on-demand scan of the infected sets, but the problem did not recur on retrying the scan. We also had some problems persuading the scheduler to operate.

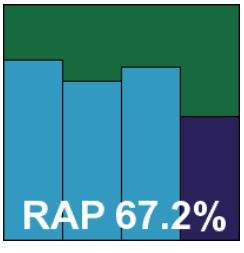




These issues aside, scanning speeds were quite excellent on demand, and on-access overheads were also highly impressive. Detection rates continue to improve in both the trojans and RAP sets, and handling of polymorphic items, including those in the WildList, was faultless. With no further problems with false positives, *K7* continues its VB100 odyssey with another award.

## Kaspersky Anti-Virus 6 for Windows Servers Enterprise Edition 6.0.2.555

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 90.24% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

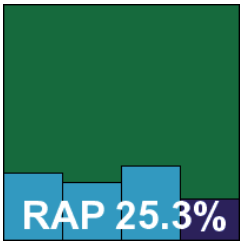
*Kaspersky* provides another proper server-oriented product, again using the MMC as its control console. The management tool requires separate installation from the main protective component, and it took some time to explore and familiarize ourselves with the rather complex layout, some useful options being rather hard to find; users may be best advised to read the full manual before deployment. We also noted some more frustrating behaviours, including scan options resetting themselves when other areas of configuration are changed.


Despite the awkwardness and misbehaviour of the interface, testing proceeded without major difficulties, and as usual the thoroughness of the protection led to some slowish scan times and fairly heavy overheads. Detection rates were generally pretty good, perhaps not quite as high as expected over the RAP sets, but there were no problems in the WildList or clean sets and *Kaspersky* duly qualifies for a VB100 award.

## Kingsoft Internet Security 2009 Advanced Edition 2008.11.6.63

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 61.94% |
| **ItW (o/a)** | 99.99% | **Trojans** | 21.20% |
| **Worms & bots** | 99.58% | **False positives** | 0 |

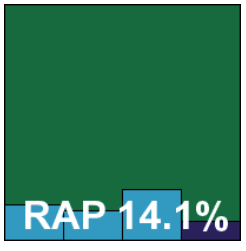



*Kingsoft* once again provided two products that are indistinguishable on the surface. The install for both is fairly zippy and straightforward, with no major obstacles and no reboot required, although the registering of some services after the initial install process does take a few moments. The interface is rather plain and un-jazzy, but provides a basic set of configuration with some clarity and ease of use. A prompt offers to update the product before any on-demand scan, to ensure maximum detection, which is an interesting touch.

Scanning speeds were pretty good and overheads around average, but detection rates left much to be desired, especially in the RAP and trojans sets. The WildList set, with its large complement of Virut samples, proved too much this time, with several samples of one of the two strains missed, and despite no false positives *Kingsoft* is denied a VB100 award for its Advanced edition.

## Kingsoft Internet Security 2009 Standard Edition 2008.11.6.63

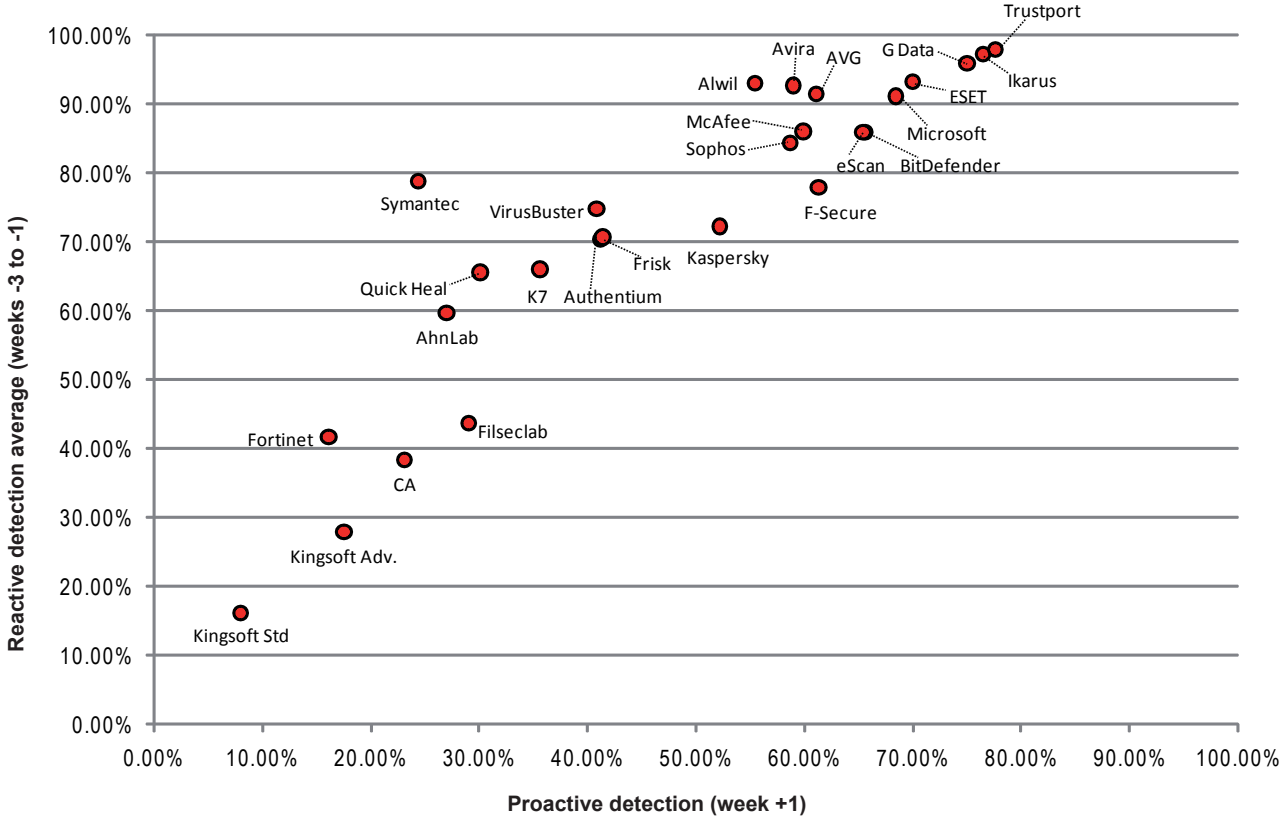
| | | | |
|---|---|---|---|
| **ItW** | 99.91% | **Polymorphic** | 59.94% |
| **ItW (o/a)** | 99.91% | **Trojans** | 7.20% |
| **Worms & bots** | 99.54% | **False positives** | 0 |




As mentioned above, the Standard version of *Kingsoft*'s product is all but impossible to tell apart from the Advanced one, and provides an identical installation and operation experience, including the option to join a community scheme sharing data on attacks and infections.

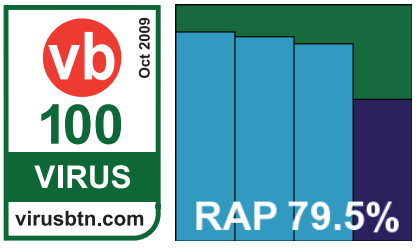
As on previous occasions, however, this version proved less 'advanced' than its counterpart in many ways, including much less impressive performance in the speed tests and even lower scores in the infected sets. Again no false positives were recorded, but fairly large numbers of samples of both Virut strains went undetected, and *Kingsoft*'s second chance at a VB100 is also doomed.

### Rap detection scores – October 2009



## McAfee VirusScan Enterprise 8.7.0i

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 90.62% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

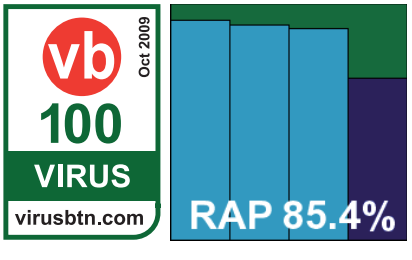



*McAfee*'s corporate product remains its sober and sensible self, barely changed for the past several years. No problem there for us, as it remains as solid, stable and well-behaved as ever. Installation and set-up presented no problems, with a comprehensive range of options available to suit the most demanding administrator. Changing these settings produced one oddity noted here before: on-access protection remains inactive for a few seconds after it has been switched on and is claimed to be operational by the interface – but it seems unlikely that this tiny window will present much of an opportunity for infection.

The product does include one new item added in recent months: the option to use the company's 'in-the-cloud' look-up system to improve protection – but as this is disabled by default in the corporate line it could not be included in VB100 results even were it logistically possible. Even without it, detection rates were pretty decent across the board, although scanning speeds were no more than reasonable, and with no problems handling our polymorphic samples or clean sets *McAfee* easily wins another VB100 award.

## Microsoft Forefront Client Security 1.5.1972.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 92.57% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

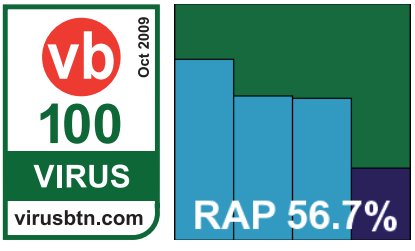



*Microsoft*'s corporate product is another which remains little changed after many tests, and we hope to see it joined in the next comparative by a shiny new sibling in the shape of the free *Security Essentials* product, formerly codenamed 'Morro'. The install process is somewhat complicated by the demands of our lab set-up, and the interface remains almost completely lacking in controls, but with a reasonable set of defaults the product had no problem powering through the tests.

Scanning speeds leaned towards the better end of the scale, and detection rates showed a continuation of *Microsoft*'s inexorable improvement, with some excellent scores in the RAP sets once again. No problems were encountered in the WildList or clean sets, and *Microsoft* takes another VB100 award comfortably in its stride.

## Quick Heal AntiVirus Lite 10.00

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 98.28% |
| **ItW (o/a)** | 100.00% | **Trojans** | 81.41% |
| **Worms & bots** | 99.88% | **False positives** | 0 |

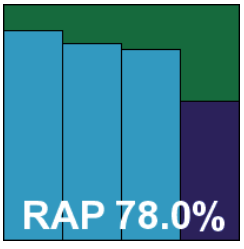



*Quick Heal* continues to carve its own special furrow with the smallest, fastest and simplest installer and its usual remarkable simplicity and speed. The interface, once up and ready a few moments after starting the installation, is pared down and attractive, but manages to provide a fair range of options under the hood. Some server admins may find the lack of option to scan all file types on access a rather significant omission – but additional file types can be added manually to the extension list.

Setting up scans took a little longer than expected, with a considerable lag after pressing the browse button, but once up and running it produced some decent speeds – perhaps less impressive than usual over some sets, but way ahead of the field over the most significant set of binaries. On access, lag times were pretty superb too. Detection rates were fairly decent, with a notable and somewhat strange drop in detection between on-demand and on-access over the trojans set, which was confirmed by multiple retries. The WildList was handled without issue though, and with no false alarms either, *Quick Heal* adds another VB100 award to its trophy cabinet.

## Sophos Anti-Virus 7.6.10

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 99.99% | **Trojans** | 90.60% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

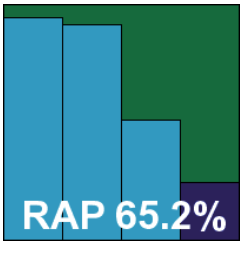



*Sophos*'s product is another that has remained unchanged on the surface since time immemorial, with a pleasantly easy install process remarkable only for the offer to remove third-party security software. Configuration is available in multiple levels going to extreme depth, and is generally simple to use although the setting up of on-demand scans proved slightly more fiddly than necessary. On one occasion, by carefully meddling with the product settings while subjecting it to heavy bombardment with infected samples, we managed to freeze the test machine, but could not repeat this feat.

Performance in the speed tests was very good indeed, and detection rates generally excellent too, with a very shallow decline across the reactive portion of the RAP sets hinting at few issues keeping up with the influx of new items. No false positives were alerted on, but in the WildList set a single sample of one of the W32/Virut strains was not detected. Further investigation found no further such samples even after producing many tens of thousands more, but the developers were able to diagnose the issue and pinned it down to a small window of a few days either side of the submission date, when detection for a tiny percentage of Virut samples was temporarily broken. Despite the rarity of such examples, a single miss is all it takes under our strict rules, and *Sophos* is unlucky to miss out on a VB100 award this month.

## Symantec Endpoint Protection 11.0.4014.26

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 92.13% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

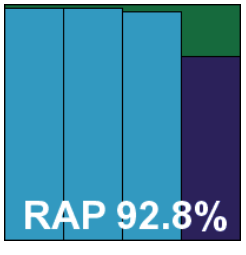

*Symantec*'s corporate product had a facelift not so long ago, giving it a much more colourful, curvy appearance which has not been popular with everyone here. However, a fresh pair of eyes on it this month found that while the install process is perhaps rather more complex than required, with a reboot needed to complete, the interface itself is fairly usable and pleasant to operate. Configuration is fairly thorough although limited in some areas, and the interface takes a few seconds to update its displays when a major configuration change is in place. In many cases this is perhaps a good thing, though, it being better to warn that protection is not yet ready when it is in fact up and running than to prematurely proclaim full operation.

Testing tripped merrily along with some decent on-demand speeds and some excellent on-access overheads, and while on-demand scans of the infected sets were slow in the extreme – taking several days where the fastest products handled the same sets in less than an hour – few real-world users will be running scans anything like as large as ours.

Logging as usual is provided in vast detail, usually far too much for the interface to handle and somewhat fiddly to extract from the raw data, but results were eventually obtained and showed some excellent detection rates over older samples, dropping off rather sharply in the most recent reactive week of the RAP set. No issues with false positives were observed, and in the WildList and polymorphic sets *Symantec* showed it has recovered from the minor stumble of the last comparative and is once again a comfortable winner of a VB100 award.

## Trustport Antivirus 2009 5.0.0.4041

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 97.97% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

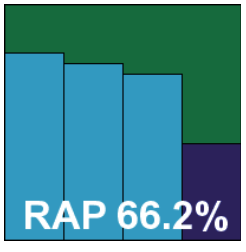

*Trustport* is another multi-engine product. This first becomes evident during the install when, among the standard set-up choices, an option is provided to perform some advanced configuration of the engines and the way in which they are used. These same choices can also be made at any time from within the main configuration interface. The control system is somewhat unusual, providing a selection of separate mini-GUIs for different purposes, but the central control panel provides most requirements in ample depth.

As expected, the multi-engine approach does not make for the best speeds, and on-access overheads are also pretty heavy, but detection rates were stratospheric, pushing perfection in most areas and highest of all this month's entrants in all the RAP weeks. With this excellence carried over to the standard sets and not balanced, as might be

expected, by any false alarms, *Trustport* is more than worthy of a VB100 award.

### VirusBuster for Servers 6.1.163

| | | | |
|---|---|---|---|
| **ItW** | 99.99% | **Polymorphic** | 90.43% |
| **ItW (o/a)** | 99.99% | **Trojans** | 79.92% |
| **Worms & bots** | 99.92% | **False positives** | 0 |




Another proper server product with another MMC interface to provide the controls, *VirusBuster*'s server offering has a fairly standard installation but proves a little less straightforward to operate once up and running. The layout within the GUI is complex and at times a little confusing. In some parts it lacks uniformity with other areas, and it is easy to confuse the GUI by clicking too impatiently on slow-to-respond buttons. Nevertheless, with some patience a decent level of control is available, although the option to scan archives on access, which seems clear, appears to have no function.

With everything set up according to our requirements, testing progressed apace thanks to some highly impressive scanning speeds in both modes, and produced some very commendable detection figures. Most test sets were handled well, but for the last time this month one of those sets of Virut samples proved too much to handle, and *VirusBuster* misses out on a VB100 award despite an otherwise generally decent performance.

## CONCLUSIONS

Another month, another comparative, another set of highs and lows. On the plus side, this month we saw very few false positives – perhaps mostly thanks to a relatively small update to the clean sets. We also observed much less instability this month than in the last comparative, with only a handful of crashes and freezes, most of which proved to be one-offs. Of course, it could be that this was helped along by the stability of the platform, which proved remarkably resilient at all times.

We saw a good selection of products, both regular desktop editions and dedicated server products, with some interesting additional features likely to be of interest to the server administrator.

The results of our RAP tests continue to develop trends and patterns, with most products scoring consistently in line with previous performances, and a new arrival looking set to make some considerable waves on our cumulative quadrants once false positive issues are eliminated. The most interesting part of the RAP results is not the pure numbers but their interrelation week on week, with steep downward curves hinting at some lag between the appearance of samples and inclusion of detection. The proactive week also indicates good response times, with some detections being added even before *VB* has had first sight of a sample, as well as heuristic and generic detection of truly unknown items.

The dominant issue this month has, of course, been the pair of highly complex polymorphic file-infecting viruses in the WildList. The large sample sets we were able to include, thanks to an automated generation and validation system, have cut a swathe through the field of entrants once again, separating those whose coverage is flawless (or nearly so) from those that have some improvements to make. A couple of products were hit by single, highly rare and unusual samples which tested their detection to breaking point, and while some may feel hard done by, we feel it is required of us to ensure that we test detection of the WildList as thoroughly and completely as possible. We may need to impose some limits however, if only for the sake of our own sanity and the time restrictions of the test, and plan to include some detail on our policy on virus replication in an update to our general procedures, expected soon. We will also continue to monitor how other areas of the procedures are performing.

In the next comparative review (due for publication in the December issue of *VB*), we should see a major and exciting new platform for the VB100, with the next test deadline expected just a few days after the official public release date of *Microsoft*'s new *Windows 7*. Assuming all goes well with the release, we expect to see a record number of products joining the comparative, and hope to make a few further improvements to our tests. As always, we welcome suggestions on any further information which may be of value or interest to our readers.

**Technical details**

**Test environment:** All products were tested on identical systems with *AMD Athlon64 X2* Dual Core 5200+ processors, 2 GB RAM, dual 80GB and 400GB hard drives, running *Microsoft Windows Server 2008 Standard Edition, Service Pack 2, 32 bit.*

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

# END NOTES & NEWS

**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/.

**A step by step masterclass in digital forensics and cybercrime will be run by ICFE on 19 November 2009 in Kuala Lumpur, Malaysia**. The masterclass follows the launch of CSI Malaysia. See http://www.icfe-cg.com/.

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

**Black Hat DC 2010 takes place 31 January to 3 February 2010 in Washington, DC, USA**. Online registration opens 15 October. For details see http://www.blackhat.com/.

**RSA Conference 2010 will be held 1–5 March 2010 in San Francisco, CA, USA**. For details see http://www.rsaconference.com/.

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

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

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

**NISC11 will be held 20–23 May 2010**. Interest in attending can be registered at http://nisc.org.uk/.

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

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

**VB2010 will take place 29 September to 1 October 2010 in Vancouver, Canada**. For details of sponsorship opportunities and any other queries relating to VB2010, please contact conference@virusbtn.com.




## SUBSCRIPTION RATES

**Subscription price for 1 year (12 issues):**

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

Corporate rates include a licence for intranet publication.

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

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