JULY 2012

virus BULLETIN

Fighting malware and spam

# JULY 2012 VBSPAM COMPARATIVE REVIEW

Most anti-malware engines 'know' about various kinds of malware. Their developers work hard to develop detection for new malware and malware variants and regularly add new signatures[1] to their engines.

Spam filters generally work differently. They don't 'know' about specific spam campaigns. Rather, they know what characteristics spam has, and using these characteristics they tend to do a good job of blocking spam – even if it is sent as part of a new campaign.

As a consequence, it is not easy to determine which spam filters are the first to detect a new outbreak – and, in fact, it is not necessarily relevant. I have seen many examples where a filter blocked the first hundred instances of a spam campaign, only to miss the 101st email.

Another consequence is that spam filters make mistakes and occasionally cause false positives. Not just because an incorrect signature is added to a database (which also happens from time to time with anti-malware engines where it can have serious consequences) but because heuristics are never 100% perfect. We acknowledge that such false positives are always going to happen, and that is why products that miss a legitimate email do not automatically fail our test.

Nevertheless, we think that products should work hard to avoid false positives as much as they can. Hence we put a lot of time and effort into creating and maintaining a feed of legitimate emails. And this is why, when we 'average' the false positive and false negative rates[2] to compute a final score, we give a weight of five to the former.

This month, 20 complete anti-spam solutions[3] participated, each of which won a VBSpam award, as did one of the two participating partial solutions (DNS blacklists). One product combined a high spam catch rate with a total absence of false positives and thus won a VBSpam+ award.

## THE TEST SET-UP

The VBSpam test methodology can be found at http://www.virusbtn.com/vbspam/methodology/. As usual, email was sent to the products in parallel and in real time, and products were given the option to block email pre-DATA. Five products chose to make use of this option.

As in previous tests, the products that needed to be installed on a server were installed on a *Dell PowerEdge R200*, with a 3.0GHz dual core processor and 4GB of RAM. The *Linux* products ran on *SuSE Linux Enterprise Server 11*; the *Windows Server* products ran on either the 2003 or the 2008 version, depending on which was recommended by the vendor.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the false positive (FP) rate. Products earn VBSpam certification if this value is at least 97:

$$SC - (5 \times FP) \geq 97$$

Those products that combine a spam catch rate of 99.5% or higher with no false positives earn a VBSpam+ award.

It is important to note that there is no objective justification for using the weight of five in the calculation of the final score. In fact, the spam catch rate and false positive rate are two distinct metrics of a spam filter, and any way in

[1] To avoid treading on the toes of anti-malware developers for whom this is a sensitive issue, I implicitly include heuristic signatures in my definition.

[2] The 'final score' as used in the test uses the spam catch rate rather than the false negative rate; mathematically the final score is equivalent to using the weighted average of false positive and false negative rates.

[3] In the past, these have been referred to as 'full solutions'. To make the differentiation clearer between these and partial solutions, we will henceforth refer to them as 'complete solutions'.

ISSN 1749-7027

which they are combined into a one-dimensional metric will be arbitrary.

We use the weighting to highlight the importance of false positives, without allowing false positives to become the single metric that determines whether products pass or fail. We have received various suggestions both to increase and to decrease the weight. Readers who prefer to use a different weight – or a different formula altogether – are encouraged to do so using the numbers presented in our tables.

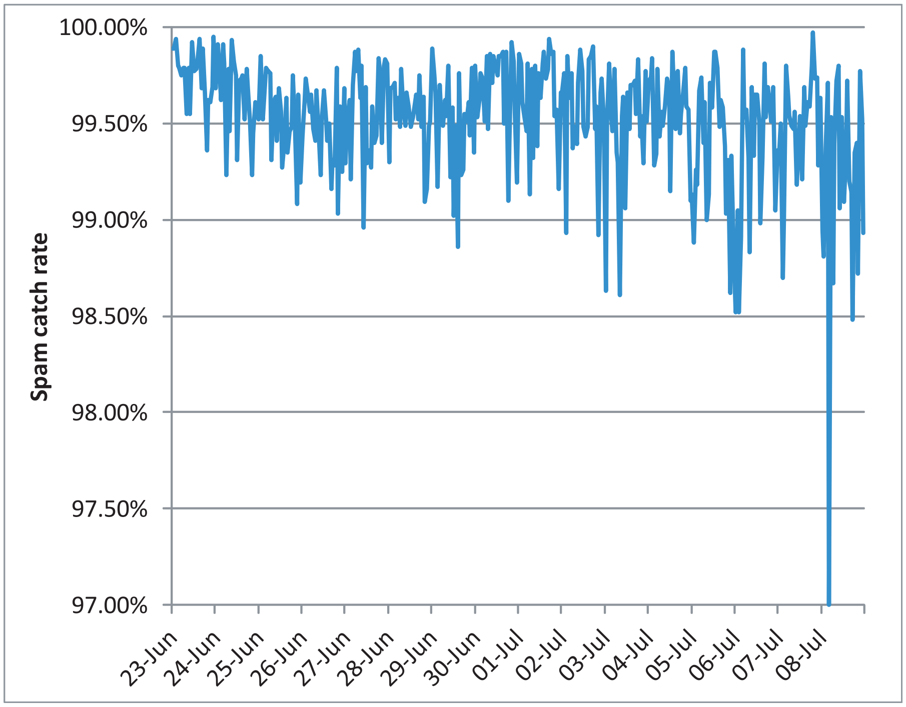


*Figure 1: Spam catch rate of all complete solutions throughout the test period.*

## THE EMAIL CORPUS

The test ran for 16 consecutive days, from 12am GMT on Saturday 23 June 2012 until 12am GMT on Monday 9 July 2012.

The corpus contained 131,182 emails, 120,763 of which were spam. All of these were provided by *Project Honey Pot* (unlike in previous tests, there was no *Spamfeed.me* feed from *Abusix*[4]). They were all relayed in real time, as were the 10,237 legitimate emails ('ham') and the remaining 182 emails, which were all legitimate newsletters.

Figure 1 shows the catch rate of all complete solutions throughout the test. To avoid the average being skewed by poorly performing products, the highest and lowest catch rates have been excluded for each hour.

Comparing this graph with the one produced in the last test (two months ago), it is immediately obvious that the average is lower, that the graph contains more troughs and that those troughs dip down lower than in the previous test. Indeed, all but three[5] solutions had a lower spam catch rate on this occasion than in the previous test.

This is a trend we have seen throughout the year: in the March report we noticed a significant decline in filters' performance compared to the test that preceded it. In May, the situation remained stable, but now the decrease continues. It does suggest that spammers are getting better at finding ways to evade filters – it may even be the case that mass actions against many spam-sending botnets have forced spammers to look for improved evasion techniques.

One such technique may be sending spam through compromised legitimate accounts. In our ham corpus we noticed close to two dozen spam messages sent from compromised accounts – presumably to contacts in the compromised user's address book. (We removed these messages from the ham corpus and because most of them were not received directly from the sender, but relayed through a legitimate third-party sender, we decided to not include them in the test at all.)

Prior to this test we also made some technical changes to the ham corpus that should have made it less easy for products to automatically recognize ham. Because many products automatically adapt to the feeds they see, we made sure there was ample time between making these changes and the start of the test.

## IPV6 AND DKIM

Last month (appropriately on the sixth of the sixth), the Internet celebrated 'World IPv6 Launch', a follow-up to a similar event ('World IPv6 Day'*)* a year earlier, when many organizations had ensured they were ready for the switch from IPv4 to IPv6. This year it was 'for real' and many

[4] The reason for the absence of *Spamfeed.me* in this test was a technical issue which meant we were unable to relay the emails exactly as they had been received by the spam traps; this would be unlikely to have affected other users of the feed.

[5] Four if one compares the catch rates only with those measured on the *Project Honey Pot* feed last time, which is arguably fairer.

organizations permanently enabled IPv6 on their networks, and on their web and mail servers.

I will not explain here what IPv6 is, why it is important and why it should be treated with caution[6] – what matters is that organizations are starting to use it. They are even starting to accept mail sent over IPv6, even though one could argue that there isn't a need for email to switch to IPv6 any time soon: the number of mail servers is still small enough for the IPv4 address space to be sufficient.

But as IPv6 gains momentum, it may well be that demand for email over IPv6 rises – which is why, as of this test, we will report which products are IPv6-capable. We have performed some very basic tests to ensure that IPv6 is indeed working; whether it works *well* cannot be said for certain until the volume of IPv6 email (and, presumably, IPv6 spam) has increased significantly. We do not make a statement on whether products should be able to filter spam sent over IPv6.

We have also introduced another new check in this test: whether DKIM plays a role in the filtering of spam.

DKIM (short for DomainKeys Identified Email) links an email to a domain – usually, though not necessarily, that of the sender – via a cryptographic signature. When an email is DKIM-signed by example.com, it means that it is DKIM-signed by example.com. While this may seem like meaningless tautology, it is important to realize that no other part of the email but the sending IP address can be assumed to be true.

This means that DKIM can be used to whitelist 'good' domains and blacklist the bad ones. Some products allow this and we could fairly easily test to see if this works. However, for many products, DKIM plays a more subtle role in determining whether an email is spam. Because one use of DKIM is not necessarily better than the other, we have simply asked all participants whether DKIM plays any role in their spam filter.

Again, we do not make a statement as to whether DKIM should be used within a spam filter. However, the fact that the majority of spam filters use DKIM could suggest that senders of legitimate email[7] would be well advised to start signing their emails using DKIM.

## RESULTS

In the text that follows, unless otherwise specified, 'ham' or 'legitimate email' refers to email in the ham corpus – which excludes the newsletters – and a 'false positive' is a message in that corpus that has been erroneously marked by a product as spam.

The 'false negative rate' is the complement of the spam catch (SC) rate (the percentage of spam messages that was blocked). It can be computed by subtracting the SC rate from 100%.

Because the size of the newsletter corpus is significantly smaller than that of the ham corpus, a missed newsletter will have a much greater effect on the newsletter false positive rate than a missed legitimate email will have on the false positive rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of slightly less than 0.01%, while one missed email in the newsletter corpus results in an FP rate of almost 0.6%).

Readers are also reminded that on this occasion the spam feed only consisted of the *Project Honey Pot* feed.

### AnubisNetworks Mail Protection Service

**SC rate:** 99.47%

**FP rate:** 0.02%

**Final score:** 99.37

**Newsletters FP rate:** 0.0%

*AnubisNetworks offers IPv6 connections, and also uses DKIM in its spam filter.*

In the last test, *AnubisNetworks* suffered from a fairly large number of false positives – something that was quite extraordinary for this solution. I was pleasantly surprised to see that this was seemingly a one-off glitch, as this month it missed just two legitimate emails. This may have been paid for by a drop in the spam catch rate (though *Anubis* was far from alone in this respect) but the final score improved nevertheless and the product now has a dozen VBSpam awards to its name.

### Bitdefender Security for Mail Servers 3.1.2

**SC rate:** 99.77%

**FP rate:** 0.05%

**Final score:** 99.53

**Newsletters FP rate:** 0.6%

*The Linux-based Bitdefender Security for Mail Servers has been supporting IPv6-based connections for some time. DKIM is not used.*

The six false positives served up by *Bitdefender* will no doubt cause some disappointment among its developers – this is the greatest number of FPs the product has had

[6] http://www.virusbtn.com/virusbulletin/archive/2012/02/vb201202-IPv6.

[7] And spammers too: DKIM is one of the few technologies that would be good (from an anti-spam point of view) for spammers to adopt.

| | True negatives | False positives | FP rate | False negatives | True positives | SC rate | Final score |
|---|---|---|---|---|---|---|---|
| AnubisNetworks | 10235 | 2 | 0.02% | 639 | 120124 | 99.47% | 99.37 |
| Bitdefender | 10232 | 5 | 0.05% | 282 | 120481 | 99.77% | 99.53 |
| ESET | 10235 | 2 | 0.02% | 638 | 120125 | 99.47% | 99.37 |
| FortiMail | 10234 | 3 | 0.03% | 610 | 120153 | 99.49% | 99.34 |
| GFI | 10235 | 2 | 0.02% | 443 | 120320 | 99.63% | 99.53 |
| Halon Security | 10236 | 1 | 0.01% | 1546 | 119217 | 98.72% | 98.67 |
| IBM | 10229 | 8 | 0.08% | 3033 | 117730 | 97.49% | 97.10 |
| Kaspersky LMS | 10236 | 1 | 0.01% | 296 | 120467 | 99.75% | 99.70 |
| Libra Esva | 10234 | 3 | 0.03% | 50 | 120713 | 99.96% | 99.81 |
| McAfee Email Gateway | 10232 | 5 | 0.05% | 290 | 120473 | 99.76% | 99.52 |
| McAfee SaaS | 10227 | 10 | 0.10% | 114 | 120649 | 99.91% | 99.42 |
| M+Guardian | 10232 | 5 | 0.05% | 1408 | 119355 | 98.83% | 98.59 |
| OnlyMyEmail | 10234 | 3 | 0.03% | 12 | 120751 | 99.99% | 99.84 |
| Sophos | 10236 | 1 | 0.01% | 602 | 120161 | 99.50% | 99.45 |
| SPAMfighter | 10224 | 13 | 0.13% | 809 | 119954 | 99.33% | 98.70 |
| SpamTitan | 10237 | 0 | 0.00% | 155 | 120608 | 99.87% | 99.87 |
| Symantec | 10228 | 9 | 0.09% | 404 | 120359 | 99.67% | 99.23 |
| The Email Laundry | 10232 | 5 | 0.05% | 496 | 120267 | 99.59% | 99.35 |
| Vamsoft ORF | 10237 | 0 | 0.00% | 1824 | 118939 | 98.49% | 98.49 |
| ZEROSPAM | 10224 | 13 | 0.13% | 112 | 120651 | 99.91% | 99.28 |
| | | | | | | | |
| Spamhaus ZEN+DBL* | 10237 | 0 | 0.00% | 2080 | 118683 | 98.28% | 98.28 |
| SURBL* | 10237 | 0 | 0.00% | 37001 | 83762 | 69.36% | 69.36 |

* Spamhaus and SURBL are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

(*Please refer to the text for full product names.*)

since we started using the current method of gathering ham. Still, with a good spam catch rate (albeit one that was slightly lower than in previous tests) the product earns its 20th VBSpam award.

### ESET Mail Security for Microsoft Exchange Server

**SC rate:** 99.47%

**FP rate:** 0.02%

**Final score:** 99.37

**Newsletters FP rate:** 2.2%

*DKIM isn't currently used in this product, though the engine supports it, and IPv6 connections are not currently supported; however, Exchange (which the product uses as its MTA) does support IPv6.*

vb
VERIFIED
SPAM
virusbtn.com

For most readers of this report, *ESET* is not a new name: it is a well-known security brand and it has won many VB100 awards for its anti-malware solution. The vendor also offers an email security product, which now debuts in the VBSpam tests.

As noted above, *ESET* uses *Microsoft Exchange Server* as the MTA to take care of mail reception and delivery. The user interface, which I found pleasant to use, gives administrators the option to fine-tune the product; for those who prefer to use the command line, the product can also be managed through a console, while the product natively supports *ESET Remote Administrator*. Unsurprisingly, the product uses *ESET ThreatSense* to scan for malicious attachments and its developers pointed out that it uses the real file extension when doing so.

A spam catch rate of close to 99.5% makes for an impressive debut for *ESET*. The product missed only two legitimate emails, both from the same sender, and thus it easily achieved its first VBSpam award – we hope that many more will follow.

### Fortinet FortiMail

**SC rate:** 99.49%
**FP rate:** 0.03%
**Final score:** 99.34
**Newsletters FP rate:** 3.3%

*Fortinet's FortiMail appliance is capable of accepting email sent over IPv6. It can also verify DKIM signatures – the results of which can be used to have the appliance take actions such as rate throttling, temporarily failing, or rejecting the email.*

*Fortinet* didn't escape the fate that most products suffered this month and saw its spam catch rate decrease. In addition, the product's false positive rate increased, though with only three missed legitimate emails, it was still low. *FortiMail* easily won its 19th VBSpam award in as many tests.

### GFI MailEssentials 2012

**SC rate:** 99.63%
**FP rate:** 0.02%
**Final score:** 99.53
**Newsletters FP rate:** 0.6%

*MailEssentials does not use DKIM as part of its spam filtering, but is capable of accepting email over IPv6 connections.*

For this test, *GFI* submitted a new version of its *MailEssentials* product. The 2012 version combines the anti-spam technology from the 2010 version with the company's previous email security solution. Five different anti-virus engines are used to check for malicious attachments. The product can be accessed using a web interface.

While *GFI* did see a decrease in its spam catch rate, the same was true for the false positive rate – it missed only two legitimate emails. With the fifth highest final score, the product easily earns its eighth VBSpam award.

### Halon Security

**SC rate:** 98.72%
**FP rate:** 0.01%
**Final score:** 98.67
**Newsletters FP rate:** 2.8%

*Halon supports both IPv6 and DKIM.*

I have previously praised *Halon*'s user interface which gives administrators a lot of flexibility and even lets them program rules in a language developed by the company. If required, IPv6 and DKIM can be included in these rules.

*Halon* was one of many products that missed more spam emails this month – in fact, its false negative rate almost doubled. On a more positive note, there was also a reduction in false positives (there was only one this time) and the product wins its ninth VBSpam award.

### IBM Lotus Protector for Mail Security

**SC rate:** 97.49%
**FP rate:** 0.08%
**Final score:** 97.10
**Newsletters FP rate:** 0.0%

*The virtual anti-spam appliance from the grand old man of IT, IBM, currently supports neither IPv6 nor DKIM.*

This month's test result was a little disappointing for *IBM* as fewer than one in 20 spam messages were blocked – representing a significant drop in its spam catch rate. A handful of false positives means that the final score was barely above the threshold of 97. Although the product earns its sixth VBSpam award, the disappointing score should hopefully motivate its developers to demonstrate that this was just a temporary glitch.

### Kaspersky Linux Mail Security 8.0

**SC rate:** 99.75%
**FP rate:** 0.01%
**Final score:** 99.70
**Newsletters FP rate:** 0.0%

*DKIM is not used in Kaspersky's anti-spam engine, but the product can accept email over IPv6.*

*Kaspersky* is not new to VBSpam comparative testing: *Kaspersky Anti-Spam* has already won more than a dozen VBSpam awards.

| | Newsletters | | Project Honey Pot | | pre-DATA† | | STDev‡ |
|---|---|---|---|---|---|---|---|
| | False positives | FP rate | False negatives | SC rate | False negatives | SC rate | |
| AnubisNetworks | 0 | 0.0% | 639 | 99.47% | | | 1.03 |
| Bitdefender | 1 | 0.6% | 282 | 99.77% | | | 0.38 |
| ESET | 4 | 2.2% | 638 | 99.47% | | | 1.14 |
| FortiMail | 6 | 3.3% | 610 | 99.49% | | | 1.08 |
| GFI | 1 | 0.6% | 443 | 99.63% | | | 1.12 |
| Halon Security | 5 | 2.8% | 1546 | 98.72% | | | 1.47 |
| IBM | 0 | 0.0% | 3033 | 97.49% | | | 2.02 |
| Kaspersky LMS | 0 | 0.0% | 296 | 99.75% | | | 0.33 |
| Libra Esva | 3 | 1.7% | 50 | 99.96% | 117410 | 97.22% | 0.13 |
| McAfee Email Gateway | 13 | 7.1% | 290 | 99.76% | | | 0.51 |
| McAfee SaaS | 17 | 9.3% | 114 | 99.91% | | | 0.25 |
| M+Guardian | 3 | 1.7% | 1408 | 98.83% | 116636 | 96.58% | 1.60 |
| OnlyMyEmail | 2 | 1.1% | 12 | 99.99% | | | 0.08 |
| Sophos | 0 | 0.0% | 602 | 99.50% | | | 0.57 |
| SPAMfighter | 5 | 2.8% | 809 | 99.33% | | | 0.69 |
| SpamTitan | 5 | 2.8% | 155 | 99.87% | | | 0.27 |
| Symantec | 1 | 0.6% | 404 | 99.67% | | | 0.41 |
| The Email Laundry | 0 | 0.0% | 496 | 99.59% | 118451 | 98.09% | 1.18 |
| Vamsoft ORF | 0 | 0.0% | 1824 | 98.49% | | | 1.72 |
| ZEROSPAM | 6 | 3.3% | 112 | 99.91% | 118532 | 98.15% | 0.22 |
| | | | | | | | |
| Spamhaus ZEN+DBL* | 0 | 0.0% | 2080 | 98.28% | 117060 | 96.93% | 1.59 |
| SURBL* | 0 | 0.0% | 37001 | 69.36% | | | 15.76 |

* *Spamhaus* and *SURBL* are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

† pre-DATA filtering was optional and was applied on the full corpus. One of the false positives for *ZEROSPAM* occurred pre-DATA; all the other false positives occurred post-DATA.

‡ The standard deviation of a product is calculated using the set of its hourly spam catch rates.

(*Please refer to the text for full product names.*)

However, the vendor's *Linux Mail Security* product is new to the test bench. As the name suggests, it runs on *Linux* (a *Postfix* server on *Ubuntu*, in our case) and fans of the operating system will not be surprised to learn that it can be controlled using the command line, as well as using a web interface. The anti-virus engine used by the product will come as no surprise either: *Kaspersky*'s own engine.

In a month where more spam was missed than in many previous tests, *Kaspersky LMS* blocked more spam than the average product. What is more, the product missed only a single legitimate email. The product makes its debut with the fourth highest final score and earns a VBSpam award to start its collection.

## Libra Esva 2.6

**SC rate:** 99.96%

**FP rate:** 0.03%

**Final score:** 99.81

**SC rate pre-DATA:** 97.22%

**Newsletters FP rate:** 1.7%

*Libra Esva's virtual machine does not accept connections sent over IPv6. The product does check DKIM signatures and can use these signatures to whitelist emails from certain senders.*

Compared to the previous test, the Italian product saw its spam catch rate drop by just one hundredth of a per cent, and its false positive rate increased by the same amount. This meant another impressive performance and the product more than deserves to add a 13th VBSpam award to its tally.

### McAfee Email Gateway 7.0

**SC rate:** 99.76%

**FP rate:** 0.05%

**Final score:** 99.52

**Newsletters FP rate:** 7.1%

*McAfee's Email Gateway can accept email over IPv6 connections and performs DKIM checks.*

*McAfee*'s *Email Gateway* appliance was one of the few products that saw its spam catch rate increase in this test. What is more, the product saw its false positive rate halved at the same time. A third VBSpam award in as many tests is thus well deserved.

### McAfee SaaS Email Protection

**SC rate:** 99.91%

**FP rate:** 0.10%

**Final score:** 99.42

**Newsletters FP rate:** 9.3%

*McAfee SaaS Email Protection also supports IPv6 and checks DKIM signatures – the results of the latter can be used by administrators to trigger certain actions.*

Like its sibling product, the cloud-based solution from *McAfee* saw its false negative rate decrease and missed fewer than one in one thousand emails. The false positive rate did increase a little, but the product's final score was still well above 97 and *McAfee* earns another VBSpam award for its SaaS product.

### Messaging Architects M+Guardian

**SC rate:** 98.83%

**FP rate:** 0.05%

**Final score:** 98.59

**SC rate pre-DATA:** 96.58%

**Newsletters FP rate:** 1.7%

*M+Guardian, the virtual appliance from Messaging Architects, can accept email sent over IPv6. It also performs DKIM checks on incoming emails.*

*M+Guardian* was one of the many products that saw an increase in their false negative rates – in this case the false negative rate more than tripled. However, at the same time the false positive rate was reduced to a sixth of its previous value and I am tempted to see this as an improvement. Indeed, with an increased final score the product earns another VBSpam award.

### OnlyMyEmail's Corporate MX-Defender

**SC rate:** 99.99%

**FP rate:** 0.03%

**Final score:** 99.84

**Newsletters FP rate:** 1.1%

*OnlyMyEmail checks the DKIM-signatures of incoming emails and the result of these checks is one of many factors that help the product make a decision on whether to block the email. Lack of demand means IPv6 is not implemented at the moment, though according to its developers the product is technically capable of accepting IPv6 emails.*

*OnlyMyEmail* continues to impress with its spam catch rate – missing less than one in ten thousand spam messages in this test. The false positive rate also remains below average. With another impressive performance and the second highest final score, the product wins its 11th VBSpam award.

### Sophos Email Appliance

**SC rate:** 99.50%

**FP rate:** 0.01%

**Final score:** 99.45

**Newsletters FP rate:** 0.0%

*In its current version, Sophos Email Appliance doesn't accept emails sent over IPv6 and does not check for DKIM signatures.*

In this test, the appliance saw its false negative rate increase, but its false positive rate decreased to a single missed email – which was the only thing to get in the way of it winning a VBSpam+ award. The product earns its 15th consecutive VBSpam award.

| Hosted solutions | Anti-malware | IPv6 | DKIM | Multiple MX-records | Multiple locations |
|---|---|---|---|---|---|
| AnubisNetworks | ClamAV, external engines upon request | √ | √ | √ | √ |
| McAfee SaaS | McAfee | √ | √ | √ | √ |
| OnlyMyEmail | Proprietary (optional) | | √ | √ | √ |
| The Email Laundry | Included* | | √ | √ | √ |
| ZEROSPAM | ClamAV | | | √ | √ |

* Vendor prefers not to reveal identity of anti-malware engine.

(*Please refer to the text for full product names.*)

| Local solutions | Anti-malware | IPv6 | DKIM | Interface | | | |
|---|---|---|---|---|---|---|---|
| | | | | CLI | GUI | Web GUI | API |
| Bitdefender | Bitdefender | √ | | √ | | √ | |
| ESET | ESET ThreatSense | | | √ | √ | | |
| FortiMail | Fortinet | √ | √ | √ | | √ | |
| GFI | Five anti-virus engines | √ | | | | √ | |
| Halon Security | Commtouch, Kaspersky, ClamAV | √ | √ | √ | | √ | √ |
| IBM | Sophos, IBM Remote Malware Detection | | | √ | | √ | |
| Kaspersky LMS | Kaspersky | √ | | | | | |
| Libra Esva | ClamAV, others optional | | √ | | | √ | |
| M+Guardian | Proprietary | √ | √ | √ | | | |
| McAfee Email Gateway | McAfee | √ | √ | √ | √ | √ | |
| Sophos | Sophos | | | | | √ | |
| SPAMfighter | VIRUSfighter (optional) | √ | | | | √ | |
| SpamTitan | Kaspersky, ClamAV | √ | √ | √ | | √ | √ |
| Symantec | Symantec | | √ | √ | | √ | |
| Vamsoft ORF | Optional* | | | | √ | | |

* Various engines can be plugged in.

(*Please refer to the text for full product names.*)

## SPAMfighter Mail Gateway

**SC rate:** 99.33%

**FP rate:** 0.13%

**Final score:** 98.70

**Newsletters FP rate:** 2.8%

*The Windows-based SPAMfighter solution is capable of accepting connections sent over IPv6. DKIM is not used in its anti-spam agent.*

*SPAMfighter* stood out among this month's participants as it saw a significant increase in its spam catch rate. Against that stood a small increase in the false positive rate, but the final score shows an overall improvement. Another VBSpam award should spur the developers on to improve the scores even further.

## SpamTitan 5.11

**SC rate:** 99.87%

**FP rate:** 0.00%

### SpamTitan 5.11 contd.

**Final score:** 99.87

**Newsletters FP rate:** 2.8%

vb
VERIFIED
SPAM +
virusbtn.com

*SpamTitan's appliance checks DKIM-signatures of inbound messages. If requested, IPv6 can be supported as well.*

*SpamTitan* submitted version 5.11 of its virtual appliance to this test, a new version which adds some new features such as the ability to block mail based on the top-level domain or emails matching certain regular expressions.

Like most products, *SpamTitan* saw its spam catch rate drop a little in this test. However, it remained high and was combined with a lack of false positives – one of only two complete solutions to achieve a zero false positive score this month. As the spam catch rate was well over 99.5%, *SpamTitan* is the only product in this test (and only the second product overall) to win a VBSpam+ award – it also achieved this month's highest final score.

### Symantec Messaging Gateway 9.5

**SC rate:** 99.67%

**FP rate:** 0.09%

**Final score:** 99.23

**Newsletters FP rate:** 0.6%

vb
VERIFIED
SPAM
virusbtn.com

*Symantec's virtual appliance has the ability to sign outbound email using DKIM as well as check signatures of inbound email. IPv6 is not supported, but version 10 of the product, which will be released later this year, is able to accept IPv6 connections.*

A small decrease in the product's spam catch rate was combined with an increase in its false positive rate – and thus a worse performance was recorded, no matter how you measure it. Despite this, the product's final score was still well over the 97 threshold and thus earns its 16th consecutive VBSpam award.

### The Email Laundry

**SC rate:** 99.59%

**FP rate:** 0.05%

**Final score:** 99.35

**SC rate pre-DATA:** 98.09%

**Newsletters FP rate:** 0.0%

vb
VERIFIED
SPAM
virusbtn.com

*The hosted solution does not accept mail sent over IPv6, but DKIM checks are performed.*

| Complete solutions sorted by final score | |
|---|---|
| SpamTitan | 99.87 |
| OnlyMyEmail | 99.84 |
| Libra Esva | 99.81 |
| Kaspersky LMS | 99.70 |
| GFI | 99.53 |
| Bitdefender | 99.53 |
| McAfee Email Gateway | 99.52 |
| Sophos | 99.45 |
| McAfee SaaS | 99.42 |
| AnubisNetworks | 99.37 |
| ESET | 99.37 |
| The Email Laundry | 99.35 |
| FortiMail | 99.34 |
| ZEROSPAM | 99.28 |
| Symantec | 99.23 |
| SPAMfighter | 98.70 |
| Halon Security | 98.67 |
| M+Guardian | 98.59 |
| Vamsoft ORF | 98.49 |
| IBM | 97.10 |

*(Please refer to text for full product names.)*

We were pleased to see *The Email Laundry* return to the test bench after having been absent from the last test. Looking back at previous scores, it is fair to say that *The Email Laundry* hasn't been spared the drop in catch rate seen almost across the board this month. However, with just a handful of false positives, the product still managed to achieve a decent enough final score to earn its 13th VBSpam award.

### Vamsoft ORF

**SC rate:** 98.49%

**FP rate:** 0.00%

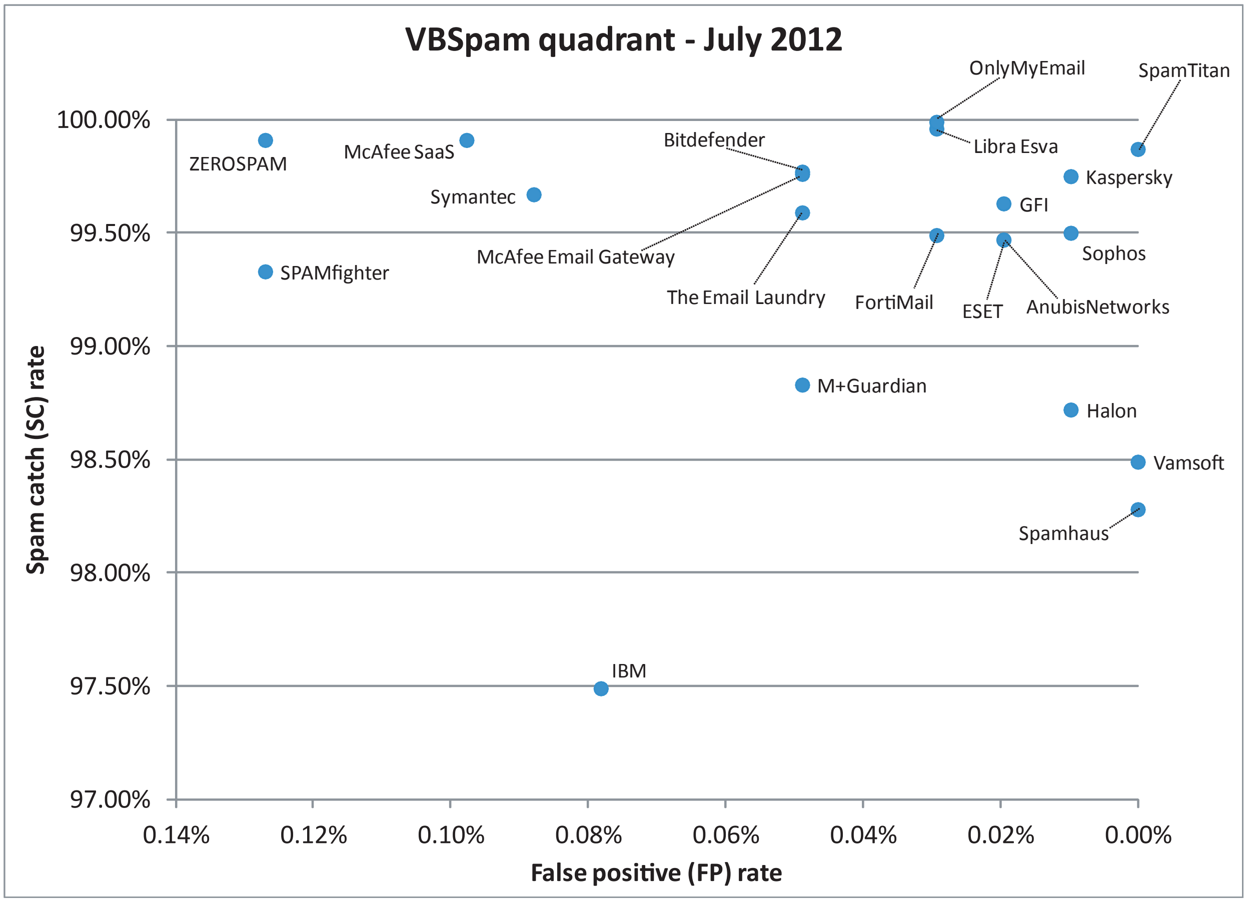
**Final score:** 98.49

**Newsletters FP rate:** 0.00%

vb
VERIFIED
SPAM
virusbtn.com

*Vamsoft's ORF doesn't use DKIM and does not accept mail sent over IPv6.*

In this test, *ORF* once again did not miss a single legitimate email. While the product's spam catch rate did decrease, if we take into account the fact that we only included the *Project Honey Pot* corpus, we actually saw an increase (compared with



*(Please refer to text for full product names.)*

the product's score on the *Project Honey Pot* corpus in the last test). Although there is some room for improvement, *Vamsoft* earns its 14th VBSpam award.

## ZEROSPAM

**SC rate:** 99.91%
**FP rate:** 0.13%
**Final score:** 99.28
**SC rate pre-DATA:** 98.15%
**Newsletters FP rate:** 3.3%

*ZEROSPAM does not accept email sent over IPv6 at its servers, and does not make use of DKIM in its anti-spam engine. However, the developers say they are working on implementing both.*

vb VERIFIED SPAM virusbtn.com

In this test, *ZEROSPAM* equalled its last spam catch rate – not a bad thing, given other products' performance and given that it was already higher than average. However, the 13 false positives were a bit of a disappointment. Although *ZEROSPAM* has done enough to earn its third VBSpam award, its developers should be working hard to show that this slip in performance was just a one-off.

## Spamhaus ZEN+DBL

**SC rate:** 98.28%
**FP rate:** 0.00%
**Final score:** 98.28
**SC rate pre-DATA:** 96.93%
**Newsletters FP rate:** 0.0%

As a partial solution, DKIM compatibility isn't relevant for *Spamhaus*, but that doesn't mean the project ignores this feature: since last year it has been publishing a domain-based whitelist which uses DKIM.

vb VERIFIED SPAM virusbtn.com

The impact of a possible switch to IPv6 will, of course, be huge for what is mostly an IPv4-based blacklist. Thus by its nature, *Spamhaus ZEN* is not 'IPv6-ready'. But here again *Spamhaus* has not been quiet and has done quite a lot of work on IPv6-based whitelists.

In this test, *Spamhaus* saw a slight decrease in its spam catch rate – as we have said before, this may be an indication that spammers are increasingly using legitimate mail servers to send their emails. Once again, there were no false positives and *Spamhaus* adds another VBSpam award to its tally.

### SURBL

**SC rate:** 69.36%
**FP rate:** 0.00%
**Final score:** 69.36
**Newsletters FP rate:** 0.0%

As domain-based filtering is agnostic to the IP version used, the *SURBL* URI blacklist is by nature IPv6-ready – though it is worth mentioning that *SURBL* also runs nameservers that accept IPv6 requests. Obviously, *SURBL* itself does not perform DKIM checks, though the domains seen in DKIM can, of course, be checked against the blacklist; it is fair to say, though, that this is probably not where DKIM's core strength lies.

Compared to the previous test, *SURBL*'s spam catch rate decreased somewhat – though still almost seven out of ten spam messages were blocked purely by checking the domains present in the emails. As in all previous tests, there were no false positives.

## CONCLUSION

With 20 VBSpam awards and a VBSpam+ award, this test shows once again that there is ample choice of decent spam filters for potential customers.

But that is only half of the story. Most spam filters have seen another increase in the percentage of spam they missed. This is a worrying trend which, from the end-user's point of view, undoes a lot of the good work that has been done in reducing the global volume of spam. When we first reported this trend back in March, many responded by saying that catch rates are still high. While this is true, and we're certainly not losing the war against spam yet, we are losing an important battle.

It is really up to the industry to tackle this issue. If the issue is not addressed, then in the cat-and-mouse game of spam fighting, the mice will simply run faster.

The next VBSpam test will run in August 2012, with the results scheduled for publication in September. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Dr Morton Swimmer

**Test Team Director:** John Hawes

**Anti-Spam Test Director:** Martijn Grooten

**Security Test Engineer:** Simon Bates

**Sales Executive:** Allison Sketchley

**Perl Developer:** Tom Gracey

**Consulting Editors:**
Nick FitzGerald, *AVG, NZ*
Ian Whalley, *Google, USA*
Dr Richard Ford, *Florida Institute of Technology, USA*

## SUBSCRIPTION RATES

**Subscription price for Virus Bulletin magazine (including comparative reviews) 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.*

**Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):**

- Comparative subscription: $100

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

**Editorial enquiries, subscription enquiries, orders and payments:**

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park,
Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139  Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: http://www.virusbtn.com/

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.