MARCH 2013

virus BULLETIN

Covering the global threat landscape

# MARCH 2013 VBSPAM COMPARATIVE REVIEW

## INTRODUCTION

While writing this review, I received an email asking 'didn't you get the email I sent you last week?'. Red faced, I dug into the spam quarantine, expecting to find the email there. But it wasn't a false positive – or, rather, it wasn't the spam filter's false positive, it was mine.

Like most people, aside from receiving a fair amount of typical spam, I also receive email that many would classify not as spam, but as unsolicited newsletters – more a nuisance than a crime. Indeed, it may well be that the same newsletters are welcomed by some of their recipients. As a tester who has repeatedly warned against false positives, I can understand spam filters erring on the side of caution and not blocking emails of this type.

As an end-user, however, I see these emails cluttering up my inbox, which I prefer to see tidy. Thankfully, my keyboard has a delete button, which I use to mop up all the unwanted messages, leaving my inbox blissfully free from clutter. However, I have learned the hard way that an apparently unfamiliar sender and a somewhat generic subject line do not necessarily mean that I don't want to read the email. Thus, as a user, I would have liked all the other unsolicited, newsletter-style emails to have been blocked.

Products participating in the VBSpam tests are faced with some choices: they may choose to block all such not-quite-spam emails, resulting in a higher spam catch rate, but also potentially in a higher false positive rate, especially amongst the (legitimate, solicited) newsletters. Alternatively, they may be more hesitant (perhaps at their users' request) and thus achieve lower catch rates, but with lower false positive rates.

There isn't necessarily a 'right' choice to be made here – and as much as they inform customers about how products perform, our tests also reflect what choices the products' developers have made.

In this month's VBSpam test, 17 out of 19 complete anti-spam solutions performed well enough to earn a VBSpam award. Two of those combined a very high catch rate with a lack of false positives and thus earned VBSpam+ awards.

## 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 *CentOS 6.3* (*Bitdefender*) or *Ubuntu 11* (*Kaspersky*); 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 98:

$SC - (5 \times FP) \geq 98$

Meanwhile, those products that combine a spam catch rate of 99.50% or higher with a lack of false positives earn a VBSpam+ award.

## THE EMAIL CORPUS

As usual, the test ran for 16 consecutive days, from 12am GMT on Saturday 16 February 2013 until 12am GMT on Monday 4 March 2013. A bug in one of the main test MTAs caused the test to be interrupted for a short period

ISSN 1749-7027

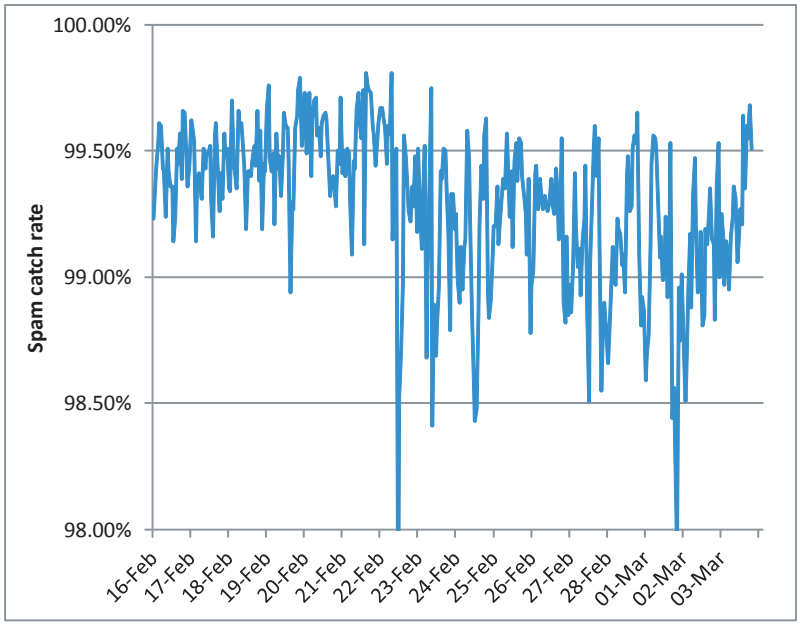



*Figure 1: Spam catch rate of all complete solutions throughout the test period.*

a few times. To ensure that no product's performance was affected by this interruption, we liberally excluded emails from the test that were sent immediately before or after each interruption.

The corpus contained 84,576 emails, 71,298 of which were part of the spam corpus: 56,781 were provided by *Project Honey Pot* and 14,517 by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the remaining emails, consisting of 12,532 legitimate emails ('ham'), 223 newsletters and 523 phishing emails provided by *Wombat Security Technologies*.

Figure 1 shows the catch rate of all full 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.

Compared to the last test, there has been a significant drop in average catch rates. Indeed, 15 of the 19 complete solutions missed more spam than they did in the last test – and nine products at least doubled the relative amount of missed spam. The drop in performance was seen in both spam corpora.

While spam catch rates dropped, most products also saw their false positive rates increase. This wasn't too surprising, however, as prior to the test, a number of new sources of legitimate emails were added, including legitimate emails in German, French, Greek and Russian – non-English emails (and particularly those using a non-Latin character set) tend to trigger more false positives. Thus there is all the more reason to praise those products that managed to classify each of the more than 12,500 legitimate emails (yet another record) correctly.

We were pleased to be able to include the *Wombat* feed once again this month (after an absence from the previous test), with 523 phishing emails all attempting to lure the recipient into leaving their banking or login details on phony websites. Compared with the November 2012 test, when this feed was first included, some products performed slightly better, while others performed slightly worse. The average catch rate increased by less than two percentage points – hardly significant.

The *Wombat* feed consists of live, run-of-the-mill phishing emails. It is skewed towards consumer-oriented phishing emails written in English, such as emails claiming to come from financial institutions or popular online services such as *Facebook* and *Twitter*. The emails in the feed generally urge the user to click a link to reverse an account suspension, confirm an update or read a new message. In most cases the links direct the user to a fake site phishing for account information, though in some cases they lead to malicious sites which install malware on the recipient's machine via a drive-by download.

Figure 2 plots the products' performance on the *Wombat* feed against that on the overall spam feed. Perhaps

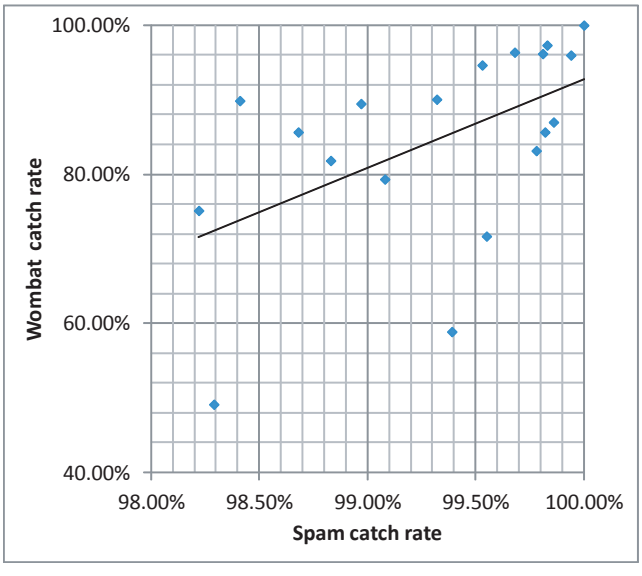



*Figure 2: Products' performance on the Wombat feed of phishing emails against their overall spam catch rate.*

unsurprisingly, there is a correlation: the products that block more general spam also block more phishing emails, and the opposite is also true. Compared to the November test, the correlation is significantly stronger. However, there are notable exceptions, with some products performing surprisingly badly or surprisingly well on the phishing feed.

## 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.

Because the size of the newsletter corpus is significantly smaller than that of the ham corpus, a missed newsletter has a much greater effect on the newsletter false positive rate than a missed legitimate email has on the false positive rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of less than 0.01%, while one missed email in the newsletter corpus results in an FP rate of more than 0.4%).

Likewise, a missed email in the *Wombat* corpus makes the spam catch rate drop by almost 0.2%, whereas in the general spam feed, a little over seven false negatives caused the spam catch rate to drop by just 0.01%.

### Bitdefender Security for Mail Servers 3.1.2

**SC rate:** 99.81%
**FP rate:** 0.00%
**Final score:** 99.81
**Project Honey Pot SC rate:** 99.91%
**Abusix SC rate:** 99.43%
**Wombat SC rate:** 96.2%
**Newsletters FP rate:** 0.9%


This month marks four full years of participation in the VBSpam tests for *Bitdefender*. The Romanian anti-spam product was submitted to the very first test in 2009 and has not missed one since then. What is more, the product (we have always tested the *Linux* version, but the same engine is used in *Windows* products) has never failed to achieve a VBSpam award and has regularly ranked among the better performers in the test.

This occasion is no exception. In fact, the product's high spam catch rate combined with no false positives sees it earn its second VBSpam+ award in a row, with the second highest final score in this test. It was also good to see that *Bitdefender* had one of the higher catch rates on the phishing corpus, in which it missed fewer than one in 25 emails – thus leaving its users well protected against most of these arguably more dangerous threats.

### ESET Mail Security for Microsoft Exchange Server

**SC rate:** 99.68%
**FP rate:** 0.01%
**Final score:** 99.64
**Project Honey Pot SC rate:** 99.66%
**Abusix SC rate:** 99.78%
**Wombat SC rate:** 96.4%
**Newsletters FP rate:** 4.0%


*ESET* prides itself on its excellent track record in the VB100 anti-malware certification tests. The company is a relative newcomer to the VBSpam tests, this being only its fourth participation, but what it may lack in quantity of submissions, it makes up for in quality: *ESET* has already achieved two VBSpam+ awards.

In this test, the company's anti-spam solution for *Microsoft Exchange* came within an inch of earning a third VBSpam+ award, but a single German email that was incorrectly marked as spam (which was also incorrectly blocked by a few other products) was the fly in the ointment. Nevertheless, with a high spam catch rate and the third highest score against the corpus of phishing emails, there is plenty of reason for *ESET*'s developers to celebrate their product's fourth VBSpam award.

### Fortinet FortiMail

**SC rate:** 99.82%
**FP rate:** 0.02%
**Final score:** 99.70
**Project Honey Pot SC rate:** 99.78%
**Abusix SC rate:** 99.97%
**Wombat SC rate:** 85.7%
**Newsletters FP rate:** 0.9%


*Fortinet*'s *FortiMail* hardware appliance has been active in our lab since the spring of 2009 (the second VBSpam test), and since then the product has never failed to win a VBSpam award. The appliance requires very little maintenance and has always combined good catch rates with low false positive rates.

This test is no exception, and the product yet again finds itself with a top-five final score. Performance against phishing emails and newsletters was average, but both the spam catch rate and the false positive rate were above average. The three false positives (two of which came from

| | True negatives | False positives | FP rate | False negatives | True positives | SC rate | Final score |
|---|---|---|---|---|---|---|---|
| Bitdefender | 12532 | 0 | 0.00% | 134 | 71164 | 99.81% | 99.81 |
| ESET | 12531 | 1 | 0.01% | 225 | 71073 | 99.68% | 99.64 |
| FortiMail | 12529 | 3 | 0.02% | 129 | 71169 | 99.82% | 99.70 |
| GFI | 12531 | 1 | 0.01% | 338 | 70960 | 99.53% | 99.49 |
| Halon Security | 12528 | 4 | 0.03% | 732 | 70566 | 98.97% | 98.81 |
| IBM | 12529 | 3 | 0.02% | 1269 | 70029 | 98.22% | 98.10 |
| Kaspersky LMS | 12532 | 0 | 0.00% | 435 | 70863 | 99.39% | 99.39 |
| Libra Esva | 12532 | 0 | 0.00% | 44 | 71254 | 99.94% | 99.94 |
| McAfee Email Gateway | 12511 | 21 | 0.17% | 655 | 70643 | 99.08% | 98.24 |
| McAfee SaaS | 12502 | 30 | 0.24% | 1131 | 70167 | 98.41% | 97.21 |
| Netmail Secure | 12528 | 4 | 0.03% | 121 | 71177 | 99.83% | 99.67 |
| OnlyMyEmail | 12523 | 9 | 0.07% | 0 | 71298 | 100.00% | 99.64 |
| Sophos | 12532 | 0 | 0.00% | 482 | 70816 | 99.32% | 99.32 |
| SPAMfighter | 12511 | 21 | 0.17% | 833 | 70465 | 98.83% | 97.99 |
| SpamTitan | 12528 | 4 | 0.03% | 103 | 71195 | 99.86% | 99.70 |
| Symantec | 12530 | 2 | 0.02% | 321 | 70977 | 99.55% | 99.47 |
| The Email Laundry | 12531 | 1 | 0.01% | 940 | 70358 | 98.68% | 98.64 |
| Vamsoft ORF | 12528 | 4 | 0.03% | 1221 | 70077 | 98.29% | 98.13 |
| ZEROSPAM | 12525 | 7 | 0.06% | 158 | 71140 | 99.78% | 99.50 |
| | | | | | | | |
| Spamhaus ZEN+DBL* | 12528 | 4 | 0.03% | 4121 | 67177 | 94.22% | 94.06 |
| SURBL* | 12532 | 0 | 0.00% | 39746 | 31552 | 44.25% | 44.25 |

* *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.*)

the same sender) mean that *Fortinet*'s developers have a little longer to wait for their first VBSpam+ award, but the product's 23rd consecutive VBSpam award is no trivial achievement.

## GFI MailEssentials

**SC rate:** 99.53%
**FP rate:** 0.01%
**Final score:** 99.49
**Project Honey Pot SC rate:** 99.69%
**Abusix SC rate:** 98.89%
**Wombat SC rate:** 94.7%
**Newsletters FP rate:** 10.8%


*GFI MailEssentials* first joined the VBSpam test in 2011, by which time the company had already won several VBSpam awards with the *VIPRE* product. *MailEssentials* is a *Windows*-based anti-spam solution that hooks into mail servers like *Microsoft Exchange* and *ISS*. We have been testing a version using the latter MTA.

*MailEssentials* has never missed a VBSpam award, but that wasn't the only goal for its developers, as is evidenced by the product's improved performance in almost every test, culminating in a VBSpam+ award in the last one. However, as was the case for most products this month, *GFI*'s performance dropped slightly in this test, and a single false positive prevented it from winning a second VBSpam+ award. Nevertheless, with a good performance on the phishing emails, and its relatively high newsletter false positive rate only a minor concern, the developers of *MailEssentials* should be pleased to reach a dozen VBSpam awards in as many tests.

## Halon Security

**SC rate:** 98.97%
**FP rate:** 0.03%
**Final score:** 98.81
**Project Honey Pot SC rate:** 99.29%
**Abusix SC rate:** 97.74%
**Wombat SC rate:** 89.5%
**Newsletters FP rate:** 0.9%


*Halon Security* still holds the informal record for the fastest set-up time in a VBSpam test: the product was set up (as a virtual machine) and running in under two hours. Less than 36 hours later it joined its first test, in which it was one of the better performing products. In the 11 tests since then, the Swedish product has never failed to achieve a VBSpam award – and in each of the two most recent tests it has won a VBSpam+ award.

This time the solution saw its spam catch rate drop a little (which was no exception this month), and as a result (combined with misclassifying four legitimate emails) it missed out on a VBSpam+ award. Nevertheless, *Halon*'s 13th participation was not unlucky: with a final score well above the standard VBSpam threshold, the company can add another VBSpam award to its tally.

## IBM Lotus Protector for Mail Security

**SC rate:** 98.22%
**FP rate:** 0.02%
**Final score:** 98.10
**Project Honey Pot SC rate:** 98.37%
**Abusix SC rate:** 97.64%
**Wombat SC rate:** 75.1%
**Newsletters FP rate:** 0.0%


*IBM* is a name that reaches way beyond the security industry, and the company was around well before email even existed. The fact that *IBM* is currently very active in security, including email security, shows how well it has adapted to a changing landscape.

*Lotus Protector for Mail Security* can run either on *IBM System* hardware or as a virtual appliance in *VMware*; we have always tested the latter. *IBM* is one of those products that hasn't needed looking at in the lab since it first started – which is always a good thing. Its performance has also been good, almost always earning a VBSpam award.

The last test was the only exception, so it was nice to see that, against the grain, *IBM* saw its spam catch rate increase this month, while its false positive rate was lower than in the last test and it didn't incorrectly block any newsletters. There is still some room for improvement in the product's spam catch rate – including the catch rate on phishing emails – but overall, the product regaining its VBSpam status is something worth celebrating.

## Kaspersky Linux Mail Security 8.0

**SC rate:** 99.39%
**FP rate:** 0.00%
**Final score:** 99.39
**Project Honey Pot SC rate:** 99.37%
**Abusix SC rate:** 99.48%
**Wombat SC rate:** 58.9%
**Newsletters FP rate:** 0.0%


We have seen in our tests that legitimate emails in non-Latin characters have a higher than average chance of being incorrectly marked as spam. As *Kaspersky Lab* is headquartered in Russia, it may not be surprising that the company's product has few problems with such emails – but it also has few problems with English-language ham: in its four previous participations, *Kaspersky Linux Mail Security* has never had more than one false positive.

In the last test the product had no false positives at all – which (alongside an excellent spam catch rate) earned it a VBSpam+ award. The product managed another clean sheet when it came to false positives this month, but as with most products, its spam catch rate dropped, falling below the VBSpam+ threshold on this occasion but still earning it a standard VBSpam award. The product's low catch rate on the *Wombat* phishing feed is a bit of a concern, but at least users of this *Kaspersky* product won't have to search their spam folders for legitimate emails.

## Libra Esva 2.9

**SC rate:** 99.94%
**FP rate:** 0.00%
**Final score:** 99.94
**Project Honey Pot SC rate:** 99.93%
**Abusix SC rate:** 99.99%
**SC rate pre-DATA:** 91.76%
**Wombat SC rate:** 96.0%
**Newsletters FP rate:** 0.0%


*Libra Esva* first joined the test three years ago and has been impressing us with very high catch rates ever since. It was as long ago as 2011 when the product's catch rate last dipped below 99.9% – and this test is no exception. What is more, the virtual appliance has historically had rather low false positive rates: it was the first product to achieve a VBSpam+ award upon its introduction, and has been edging close to a second one ever since.

| | Newsletters | | Project Honey Pot | | Abusix | | Wombat | | pre-DATA† | | STDev‡ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | False positives | FP rate | False negatives | SC rate | False negatives | SC rate | False negatives | SC rate | False negatives | SC rate | |
| Bitdefender | 2 | 0.9% | 51 | 99.91% | 83 | 99.43% | 20 | 96.2% | | | 0.48 |
| ESET | 9 | 4.0% | 193 | 99.66% | 32 | 99.78% | 19 | 96.4% | | | 0.59 |
| FortiMail | 2 | 0.9% | 124 | 99.78% | 5 | 99.97% | 75 | 85.7% | | | 0.67 |
| GFI | 24 | 10.8% | 177 | 99.69% | 161 | 98.89% | 28 | 94.7% | | | 0.90 |
| Halon Security | 2 | 0.9% | 404 | 99.29% | 328 | 97.74% | 55 | 89.5% | | | 1.37 |
| IBM | 0 | 0.0% | 927 | 98.37% | 342 | 97.64% | 130 | 75.1% | | | 1.66 |
| Kaspersky LMS | 0 | 0.0% | 359 | 99.37% | 76 | 99.48% | 215 | 58.9% | | | 2.39 |
| Libra Esva | 0 | 0.0% | 42 | 99.93% | 2 | 99.99% | 21 | 96.0% | 5877 | 91.76% | 0.25 |
| McAfee Email Gateway | 6 | 2.7% | 310 | 99.45% | 345 | 97.62% | 108 | 79.4% | | | 0.94 |
| McAfee SaaS | 1 | 0.5% | 352 | 99.38% | 779 | 94.63% | 53 | 89.9% | | | 2.00 |
| Netmail Secure | 13 | 5.8% | 114 | 99.80% | 7 | 99.95% | 14 | 97.3% | 4725 | 93.37% | 0.38 |
| OnlyMyEmail | 17 | 7.6% | 0 | 100.00% | 0 | 100.00% | 0 | 100.0% | | | 0.00 |
| Sophos | 0 | 0.0% | 420 | 99.26% | 62 | 99.57% | 52 | 90.1% | | | 0.76 |
| SPAMfighter | 4 | 1.8% | 591 | 98.96% | 242 | 98.33% | 95 | 81.8% | | | 1.53 |
| SpamTitan | 4 | 1.8% | 99 | 99.83% | 4 | 99.97% | 68 | 87.0% | | | 0.38 |
| Symantec | 1 | 0.5% | 200 | 99.65% | 121 | 99.17% | 148 | 71.7% | | | 0.71 |
| The Email Laundry | 3 | 1.4% | 388 | 99.32% | 552 | 96.20% | 75 | 85.7% | 3274 | 95.41% | 1.88 |
| Vamsoft ORF | 0 | 0.0% | 1086 | 98.09% | 135 | 99.07% | 266 | 49.1% | | | 1.28 |
| ZEROSPAM | 9 | 4.0% | 141 | 99.75% | 17 | 99.88% | 88 | 83.2% | 2334 | 96.73% | 0.52 |
| | | | | | | | | | | | |
| Spamhaus ZEN+DBL* | 0 | 0.0% | 2277 | 95.99% | 1844 | 87.30% | 383 | 26.8% | 5993 | 91.59% | 6.67 |
| SURBL* | 0 | 0.0% | 31685 | 44.20% | 8061 | 44.47% | 429 | 18.0% | | | 14.04 |

* *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. Two of the false positives for *ZEROSPAM* occurred pre-DATA. The others were all 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.*)

In this test, even with a more difficult ham corpus, the product achieved a clean sheet, including a lack of false positives amongst the newsletters. It performed very well on phishing emails too, and easily earns its second VBSpam+ award.

## McAfee Email Gateway 7.0

**SC rate:** 99.08%

**FP rate:** 0.17%

**Final score:** 98.24

**Project Honey Pot SC rate:** 99.45%

**Abusix SC rate:** 97.62%

**Wombat SC rate:** 79.4%

**Newsletters FP rate:** 2.7%

The 7.0 version of *McAfee*'s *Email Gateway* appliance joined the test last year – but the machine builds on the technology of two previous *McAfee* appliances, both of which had a longer VBSpam history. This appliance has never failed to achieve a VBSpam award, though it has scored relatively highly on false positives.

Unfortunately, this test was no exception, and the product blocked 21 legitimate emails in a number of Western languages. On the other hand, the spam catch rate barely dropped, and thus *McAfee* is able to add another VBSpam award to its tally.

## McAfee SaaS Email Protection

**SC rate:** 98.41%
**FP rate:** 0.24%
**Final score:** 97.21
**Project Honey Pot SC rate:** 99.38%
**Abusix SC rate:** 94.63%
**Wombat SC rate:** 89.9%
**Newsletters FP rate:** 0.5%

Filtering spam is not a one-size-fits-all business – something that *McAfee* has demonstrated by submitting two (and in the past even three) products to the test. As the name suggests, *McAfee SaaS Email Protection* is a cloud-based solution, offering spam filtering for organizations that do not want to have to deal with running a spam filter themselves.

In recent tests, the SaaS product scored fewer false positives than its sister product, but this time the roles were reversed, with this product missing 30 legitimate emails, interestingly enough in the same four Western languages (English, German, Spanish and Portuguese). As there was also a drop in the spam catch rate, the final score dropped well below 98, thus ending the product's unbroken run of VBSpam awards. However, better-than-average scores on both phishing emails and newsletters mean there is still something to celebrate for the product's developers, as they work towards improving its performance for the next test.

## Messaging Architects Netmail Secure

**SC rate:** 99.83%
**FP rate:** 0.03%
**Final score:** 99.67
**Project Honey Pot SC rate:** 99.80%
**Abusix SC rate:** 99.95%
**SC rate pre-DATA:** 93.37%
**Wombat SC rate:** 97.3%
**Newsletters FP rate:** 5.8%

*Messaging Architects* submitted a hardware appliance to the very first VBSpam test, which performed very well. After a few tests, the company took a break, but later returned with the *Netmail Secure* virtual appliance. After some initial struggles (possibly due to it taking the developers some time to find the right settings for the test set-up), the product has done very well in recent tests and has earned VBSpam+ awards in the last two tests.

On this occasion four false positives (two each in both German and English) meant that a third VBSpam+ award was out of the question, but with a small increase in the already high spam catch rate, and the second highest catch rate on the *Wombat* corpus, there is good reason for the product's developers to celebrate yet another VBSpam award.

## OnlyMyEmail's Corporate MX-Defender

**SC rate:** 100.00%
**FP rate:** 0.07%
**Final score:** 99.64
**Project Honey Pot SC rate:** 100.00%
**Abusix SC rate:** 100.00%
**Wombat SC rate:** 100.0%
**Newsletters FP rate:** 7.6%

Not even those who have cast no more than a casual glance at recent VBSpam reports can have failed to notice *OnlyMyEmail*'s stand-out performances. The Michigan-based company takes spam filtering to the extreme and its hosted solution has historically missed very few spam emails in our tests, while also having very low false positive rates. This culminated in a perfect score in the last test – no email was misclassified at all.

Of course, a perfect score is impossible to improve upon and not an easy thing to maintain. Nevertheless, once again, the product did not miss a single spam message – not even in *Wombat*'s phishing corpus. It did miss some legitimate emails this time, however, although none of these were in English (which, presumably, is the language the vast majority of the product's users communicate in). *OnlyMyEmail* thus cruises easily to its 15th consecutive VBSpam award.

## Sophos Email Appliance

**SC rate:** 99.32%
**FP rate:** 0.00%
**Final score:** 99.32
**Project Honey Pot SC rate:** 99.26%
**Abusix SC rate:** 99.57%
**Wombat SC rate:** 90.1%
**Newsletters FP rate:** 0.0%

For most participating vendors, the VBSpam tests are as much a way to help them improve the performance of their filters as they are a way to demonstrate to potential customers how well their products perform. As a tester, therefore, it is always nice to see an improvement in a product's performance.

| **Hosted solutions** | Anti-malware | IPv6 | DKIM | SPF | Multiple MX-records | Multiple locations |
|---|---|---|---|---|---|---|
| McAfee SaaS | McAfee | √ | √ | √ | √ | √ |
| OnlyMyEmail | Proprietary (optional) | | √ | √ | √ | √ |
| The Email Laundry | Included* | | √ | √ | √ | √ |
| ZEROSPAM | ClamAV | | | √ | √ | √ |

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

| **Local solutions** | Anti-malware | IPv6 | DKIM | SPF | Interface | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | CLI | Desktop GUI | Web GUI | API |
| Bitdefender | Bitdefender | √ | | | √ | | √ | |
| ESET | ESET Threatsense | | | | √ | √ | | |
| FortiMail | Fortinet | √ | √ | √ | √ | | √ | |
| GFI | Five anti-virus engines | √ | | √ | | | √ | |
| Halon Security | Commtouch; Kaspersky; ClamAV; HRPS | √ | √ | √ | | | √ | √ |
| IBM | Sophos; IBM Remote Malware Detection | | | √ | √ | | √ | |
| Kaspersky LMS | Kaspersky | √ | | √ | √ | | √ | |
| Libra Esva | ClamAV; others optional | | √ | √ | √ | | √ | |
| McAfee Email Gateway | McAfee | √ | √ | √ | √ | √ | √ | |
| Netmail Secure | Proprietary | √ | √ | √ | √ | | √ | |
| 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.*)

As such, I was rather pleased by the performance of *Sophos*'s *Email Appliance* in this test which, after a series of tests in which it always blocked one or more legitimate emails, was one of only three products to avoid false positives altogether amongst ordinary ham and newsletters. At the same time, there was a barely perceptible drop in the spam catch rate (and more than nine out of 10 phishing emails were blocked), thus earning the company its 19th VBSpam award in as many tests and edging the product closer to its first VBSpam+ award.

## SPAMfighter Mail Gateway

**SC rate:** 98.83%

**FP rate:** 0.17%

**Final score:** 97.99

**Project Honey Pot SC rate:** 98.96%

**Abusix SC rate:** 98.33%

**Wombat SC rate:** 81.8%

**Newsletters FP rate:** 1.8%

*SPAMfighter* is well known for its widely used free home-user spam filter, but the company also offers a *Windows*-based filter for enterprise use. There is a version that hooks into *Microsoft Exchange*, but the one that we include in our tests – which has achieved 18 VBSpam awards since 2009 – uses its own MTA.

*SPAMfighter* was one of many products that saw its catch rate drop a fair amount this month, and while there was a small decrease in its false positive rate, this was still relatively high and pushed the final score to just a fraction below the all-important VBSpam threshold of 98 (to 97.994 to be precise). No doubt, this news will be received with some frustration at the company's headquarters in Copenhagen, but

there should be strong motivation for the developers to turn things around in the next test.

## SpamTitan 5.11

**SC rate:** 99.86%
**FP rate:** 0.03%
**Final score:** 99.70
**Project Honey Pot SC rate:** 99.83%
**Abusix SC rate:** 99.97%
**Wombat SC rate:** 87.0%
**Newsletters FP rate:** 1.8%


*SpamTitan* can run as a full operating system or as a virtual appliance, and since 2009, we have been testing the latter. Historically, the product has shown very good spam catch rates, having missed fewer than one in 500 spam emails in each of the last 14 tests. The two VBSpam+ awards amongst its collection are evidence that false positives are not a major issue for the product either.

In this test the product's spam catch rate was the third highest overall, and with only four false positives, it performed better than average on the ham corpus too. Performance on both newsletter and phishing emails was not bad either – although (as is the case for most products) the latter does leave some room for improvement. *SpamTitan* easily earns its 21st VBSpam award.

## Symantec Messaging Gateway 10.0

**SC rate:** 99.55%
**FP rate:** 0.02%
**Final score:** 99.47
**Project Honey Pot SC rate:** 99.65%
**Abusix SC rate:** 99.17%
**Wombat SC rate:** 71.7%
**Newsletters FP rate:** 0.5%


Since the beginning of 2010, we have been testing *Symantec*'s *Messaging Gateway*, which is one of several anti-spam products offered by the security giant. It has always performed rather well, never failing to achieve a VBSpam award and winning its first VBSpam+ award in the last test.

It did not manage to repeat that achievement this time, but with only two false positives, *Symantec* performed better than average in this test. The product suffered from a small drop in its catch rate, but still blocked more than 199 out of 200 spam emails. Perhaps the only point of attention should be the product's relatively poor performance on phishing emails. *Messaging Gateway* earns its 20th consecutive VBSpam award.

| Complete solutions sorted by final score | |
|---|---|
| Libra Esva | 99.94 |
| Bitdefender | 99.81 |
| FortiMail | 99.70 |
| SpamTitan | 99.70 |
| Netmail Secure | 99.67 |
| ESET | 99.64 |
| OnlyMyEmail | 99.64 |
| ZEROSPAM | 99.50 |
| GFI | 99.49 |
| Symantec | 99.47 |
| Kaspersky LMS | 99.39 |
| Sophos | 99.32 |
| Halon Security | 98.81 |
| The Email Laundry | 98.64 |
| McAfee Email Gateway | 98.24 |
| Vamsoft ORF | 98.13 |
| IBM | 98.10 |
| SPAMfighter | 97.99 |
| McAfee SaaS | 97.21 |

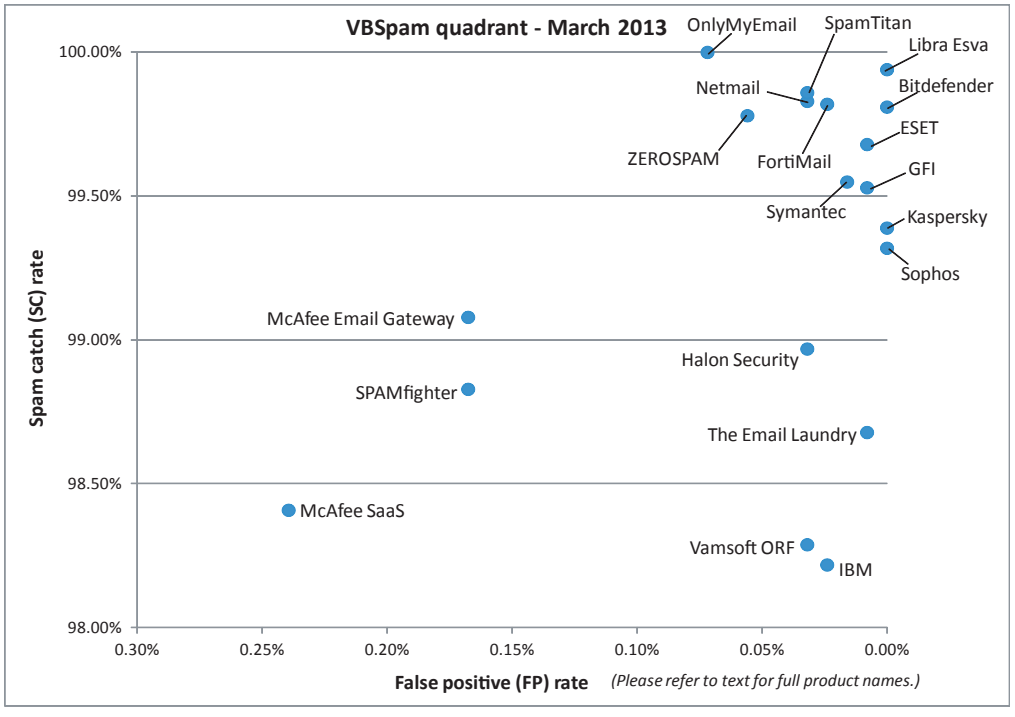
(*Please refer to the text for full product names.*)

## The Email Laundry

**SC rate:** 98.68%
**FP rate:** 0.01%
**Final score:** 98.64
**Project Honey Pot SC rate:** 99.32%
**Abusix SC rate:** 96.20%
**SC rate pre-DATA:** 95.41%
**Wombat SC rate:** 85.7%
**Newsletters FP rate:** 1.4%


*The Email Laundry*, a hosted solution operating from Ireland, prides itself not only on its ability to block a lot of spam, but also on its ability to block a lot of emails 'at the gate' or, more formally, 'pre-DATA' – based only on the connecting IP address, the HELO domain and the sender's email address. This method, combined with blocking more difficult spam further down the line, has already earned the company 16 VBSpam awards.

In this test, the product's catch rate dropped by quite a bit, but the false positive rate dropped too, with the product missing just a single legitimate email – fewer than it has done in a long time. With a final score well above the VBSpam threshold, *The Email Laundry* adds another VBSpam award to its tally.




## Vamsoft ORF

**SC rate:** 98.29%
**FP rate:** 0.03%
**Final score:** 98.13
**Project Honey Pot SC rate:** 98.09%
**Abusix SC rate:** 99.07%
**Wombat SC rate:** 49.1%
**Newsletters FP rate:** 0.0%


*Vamsoft*'s *ORF* (short for *Open Relay Filter*) was initially developed to solve a spam problem within the company itself – which until then only produced tax software for the Hungarian market. It worked so well that the company decided to develop it further and take it to market. This may explain the philosophy behind *ORF*: rather than working perfectly out of the box, it provides administrators with the tools to deal with the spam problem – which is no bad idea, given how much received spam differs between organizations. It may also explain why the product's spam catch rate tends to be a little lower than that of other products that are made to work straight out of the box.

Nevertheless, the product has a decent record in our tests, and on this occasion it adds its 17th VBSpam award to the tally. The only potential concern is its performance against phishing emails – having missed more than half in the corpus – but this could be something a clever system administrator could tailor the product for.

## ZEROSPAM

**SC rate:** 99.78%
**FP rate:** 0.06%
**Final score:** 99.50
**Project Honey Pot SC rate:** 99.75%
**Abusix SC rate:** 99.88%
**SC rate pre-DATA:** 96.73%
**Wombat SC rate:** 83.2%
**Newsletters FP rate:** 4.0%


*ZEROSPAM* completed a full year of testing last month and earned its first VBSpam+ award – and, judging by the 3D-printed VBSpam+ logo the developers subsequently sent us, this made the team rather happy (and deservedly so).

On this occasion, seven false positives – in English, French and German – prevented the product from repeating that achievement, but with another high catch rate, it easily earned a VBSpam award. It is also worth mentioning that, of those products that are set up to block spam 'pre-DATA', *ZEROSPAM* blocked the most spam messages in this phase.

## Spamhaus ZEN+DBL

**SC rate:** 94.22%
**FP rate:** 0.03%
**Final score:** 94.06
**Project Honey Pot SC rate:** 95.99%

**Abusix SC rate:** 87.30%
**SC rate pre-DATA:** 91.59%
**Wombat SC rate:** 26.8%
**Newsletters FP rate:** 0.0%

*Spamhaus*'s *ZEN+DBL* is a well-known blacklist that is used by many organizations and spam filters, including several that take part in this test. It is not a full solution, and thus its performance should not be compared with other products in the test, but *Spamhaus* has proved time and time again to be able to block the vast majority of spam based only on the sending IP address and domains present in the email.

On this occasion, *Spamhaus* missed four legitimate emails – a relatively rare occurrence for the product. The emails contained the bit.ly and is.gd domains – well-known URL shorteners that are popular amongst spammers for hiding the destination of their links, but which are also commonly seen in legitimate emails. Nevertheless, after catching over 94% of all emails (and over 91.5% based on the IP address alone), *Spamhaus* can be pleased with a decent result in this test.

## SURBL

**SC rate:** 44.25%
**FP rate:** 0.00%
**Final score:** 44.25
**Project Honey Pot SC rate:** 44.20%
**Abusix SC rate:** 44.47%
**Wombat SC rate:** 18.0%
**Newsletters FP rate:** 0.0%

Like *Spamhaus,* the *SURBL* URI blacklist is not intended as a full solution. It can be integrated into spam filters to block emails based on the presence of malicious or spammy domains. Maintaining such a blacklist is no trivial task, given the current trend amongst spammers to use compromised legitimate domains for redirection. This may explain the drop in *SURBL*'s catch rate in this test – but it was good to see that *SURBL*'s (single) false positive in the last test was a one-off.

## CONCLUSION

February and March don't seem to be good months for spam filters as, for two years in a row, we have seen a significant drop in performance during this period. Last year, the decline in performance continued until the summer – so we will be keeping a close eye on catch rates, and hoping that the filters manage to catch up more quickly this year.

*The next VBSpam test will run in April 2013, with the results scheduled for publication in May. 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/