MARCH 2016

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MARCH 2016

Martijn Grooten & Ionuţ Răileanu

INTRODUCTION

Last month, computer programmer Ray Tomlinson passed away at the age of 74. Although Ray had made numerous contributions to the tech community, he was best known for sending the first email in 1971 – and for adopting the '@' sign to separate the name of the user from that of the machine.

Email has changed a lot in the 45 years since Ray sent the first email (like *VB*, he preferred the unhyphenated version of the word). At the same time, it has changed very little, especially since it was standardized in RFCs in the early 1980s. And despite many predictions of its impending death, and predictions that everyone would soon switch to SMS, instant messaging or social networks, email continues to thrive and to be used by billions on the Internet every day.

What makes this even more remarkable is the fact that, for more than a decade, the majority of emails being sent have been unwanted – and quite often malicious. The reason people put up with this situation is that they often don't notice it: an infrastructure has been built that deals very successfully with the majority of spam before it reaches users' inboxes. Spam filters play an important part in this infrastructure.

For the past seven years, *VB* has been looking at how various spam filters have fared in the ever-changing spam landscape and how well they have been able to protect users' inboxes. The main conclusion we continue to draw from these tests is that, while no spam filter is perfect, there are a lot of decent options for organizations to choose between.

Indeed, in this month's comparative VBSpam test, we tested 18 full email security solutions, all of which achieved a VBSpam award.

THE TEST SET-UP

The VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/. As usual, emails were sent to the products in parallel and in real time, and products were given the option to block email pre-DATA (that is, based on the SMTP envelope and before the actual email was sent). However, on this occasion no products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. As different products have different hardware requirements – not to mention those running on their own hardware, or those running in the cloud – there is little point comparing the memory, processing power or hardware the products were provided with; we followed the developers' requirements and note that the amount of email we receive is representative of that received by a small organization.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the weighted false positive (WFP) rate. The WFP rate is defined as the false positive rate of the ham and newsletter corpora taken together, with emails from the latter corpus having a weight of 0.2:

WFP rate = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #newsletters)

Final score = SC - (5 x WFP)

In addition, for each product, we measure how long it takes to deliver emails from the ham corpus (excluding false positives) and, after ordering these emails by this time, we colour-code the emails at the 10th, 50th, 95th and 98th percentiles:

- (green) = up to 30 seconds
- (yellow) = 30 seconds to two minutes
- (orange) = two to ten minutes
- (red) = more than ten minutes

ISSN 1749-7027

Products earn VBSpam certification if the value of the final score is at least 98 *and* the 'delivery speed colours' at 10 and 50 per cent are green or yellow and that at 95 per cent is green, yellow or orange.

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives, no more than 2.5% false positives among the newsletters *and* 'delivery speed colours' of green at 10 and 50 per cent and green or yellow at 95 and 98 per cent earn a VBSpam+ award.

THE EMAIL CORPUS

The test ran for 16 days, from 12am on 27 February to 12am on 14 March 2016. Part of this period coincided with a visit by one of the authors to the RSA Conference in San Francisco. This is relevant in that an attempt to fix a relatively minor issue on one of the test servers from a US airport, at a little past midnight in the UK, actually made things worse and led us to exclude 11 hours' worth of email during the night between 6 and 7 March. Other than that, there were no issues that affected the test.

This month's test corpus consisted of 187,720 emails. Of these, 177,486 were spam, 95,413 of which were provided by *Project Honey Pot*, with the remaining 82,073 spam emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed to the products in real time, as were the 9,913 legitimate emails ('ham') and 321 newsletters.

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.

As the graph suggests, once again we saw very good performance among spam filters – the average catch rate was down only slightly from 99.95% in the last test to a still impressive 99.93%. The two noticeable dips in the average catch rates that can be seen in the graph were caused by coinciding drops in performance of two products and did not reflect a 'difficult' moment for spam filters in general.

The most difficult-to-filter spam – which was missed by no fewer than nine products – was a message that urged the user to open an attached PDF, which contained information on an alleged prize in an *MSN/Yahoo* lottery. The PDF was not malicious.

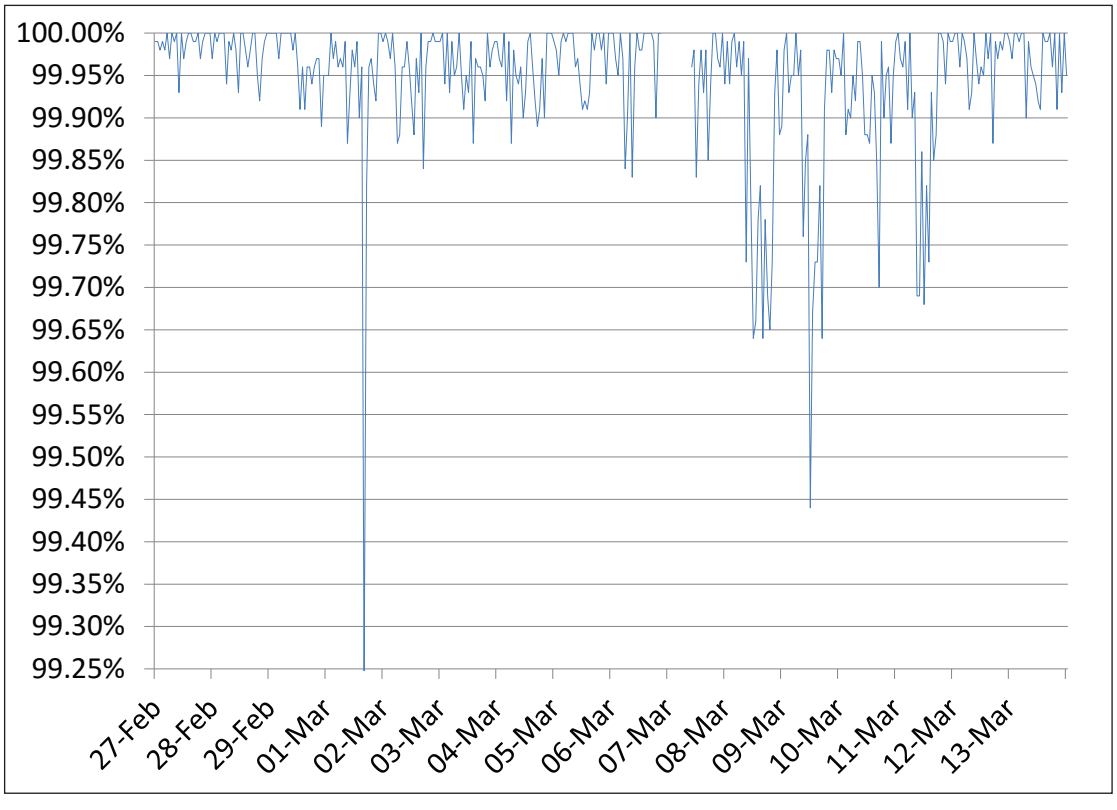


Figure 1: Spam catch rate of all full solutions throughout the test period.

RESULTS

Axway MailGate 5.3.1

SC rate: 99.84%
FP rate: 0.03%
Final score: 99.66
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

This was a good test for *Axway*'s *MailGate* appliance. The product saw only a small decrease in its spam catch rate alongside decreases in its false positive and newsletter FP rates – the latter was particularly noticeable. With an improved final score of 99.66, *Axway* achieves its 12th VBSpam award in succession.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

This test completes the first seven years of *Virus Bulletin*'s spam filter tests, and for *Bitdefender* these have been seven years of good luck – or, rather, seven years of excellent performance: the product has never failed to achieve a VBSpam award and has regularly impressed us with its performance. This test was no different, with just 25 missed spam emails and no false positives in either the ham corpus or the newsletter corpus. This performance resulted in the second highest final score of the test, and of course another VBSpam+ award.

Egedian Mail Security

SC rate: 99.95%
FP rate: 0.08%
Final score: 99.52
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Egedian's spam catch rate remains very high at 99.95%, which was better than average. Unfortunately, the product misclassified eight legitimate emails – four each from two senders – which meant we couldn't give *Egedian* its second VBSpam+ award. A VBSpam award was easily achieved though.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

After missing just ten spam emails in January's test, this time around only two out of more than 177,000 spam emails slipped through *ESET*'s grasp – one of which appeared to be broken. And that was all that went wrong, resulting in an impressive final score barely distinguishable from a perfect 100 – and of course another VBSpam+ award for *ESET*.

Fortinet FortiMail

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

This was the 41st time in a row that *Fortinet* has participated in our VBSpam test, using the very same *FortiMail* appliance. This test saw the product achieve its fifth consecutive 99.9+ final score with no false positives, few blocked newsletters and very few spam emails missed (just 21 this time). Another VBSpam+ award is well deserved.

GFI MailEssentials

SC rate: 99.75%
FP rate: 0.08%
Final score: 99.34
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.75%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	9910	3	0.03%	276	177210	99.84%	99.66
Bitdefender	9913	0	0.00%	25	177461	99.99%	99.99
Egedian	9905	8	0.08%	96	177390	99.95%	99.52
ESET	9913	0	0.00%	2	177484	99.999%	99.999
FortiMail	9913	0	0.00%	21	177465	99.99%	99.95
GFI	9905	8	0.08%	442	177044	99.75%	99.34
IBM	9913	0	0.00%	86	177400	99.95%	99.95
Kaspersky LMS	9913	0	0.00%	63	177423	99.96%	99.95
Kaspersky SMG	9913	0	0.00%	105	177381	99.94%	99.93
Libra Esva	9913	0	0.00%	17	177469	99.99%	99.98
modusGate	9913	0	0.00%	96	177390	99.95%	99.94
Netmail Secure	9912	1	0.01%	29	177457	99.98%	99.88
OnlyMyEmail	9913	0	0.00%	1	177485	99.999%	99.95
Scrollout	9898	15	0.15%	50	177436	99.97%	99.10
Sophos	9911	2	0.02%	261	177225	99.85%	99.75
SpamTitan	9910	3	0.03%	86	177400	99.95%	99.79
Vade Retro MailCube	9913	0	0.00%	373	177113	99.79%	99.77
ZEROSPAM	9908	5	0.05%	118	177368	99.93%	99.58
Spamhaus DBL*	9913	0	0.00%	107877	69609	39.22%	39.22
Spamhaus ZEN*	9913	0	0.00%	5640	171846	96.82%	96.82
Spamhaus ZEN+DBL*	9913	0	0.00%	3871	173615	97.82%	97.82

**The Spamhaus products are partial solutions and their performance should not be compared with that of other products. (Please refer to the text for full product names and details.)*

Dating spam – notoriously hard to filter – was what we found among the spam emails missed by *GFI*'s *MailEssentials* product, which only missed one in every 400 spam emails. That's certainly a good catch rate, though unfortunately it also blocked eight legitimate emails, all in English, which denied it a VBSpam+ award. Another VBSpam award was easily earned though.

IBM Lotus Protector for Mail Security

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It is hard for an email security solution to avoid false positives, but it is even harder to do so among newsletters which, by their nature, share a number of properties with spam emails. Yet *IBM*'s *Lotus Protector* product did just that, making it one of only three products this month with a clean sheet of false positives. Combined with a 99.95% spam catch rate, *IBM* has every reason to be proud of another VBSpam+ award.

Kaspersky Linux Mail Security 8.0

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

	Newsletters		Project Honey Pot		Abusix		STDev†	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	3	0.9%	258	99.73%	18	99.98%	0.25	🟢	🟢	🟢	🟡
Bitdefender	0	0.0%	14	99.99%	11	99.99%	0.07	🟢	🟢	🟢	🟢
Egedian	2	0.6%	85	99.91%	11	99.99%	0.14	🟢	🟢	🟢	🟢
ESET	0	0.0%	1	99.999%	1	99.999%	0.03	🟢	🟢	🟢	🟢
FortiMail	4	1.3%	10	99.99%	11	99.99%	0.06	🟢	🟢	🟢	🟢
GFI	1	0.3%	234	99.75%	208	99.75%	0.6	🟢	🟢	🟡	🟡
IBM	0	0.0%	74	99.92%	12	99.99%	0.1	🟢	🟢	🟢	🟢
Kaspersky LMS	1	0.3%	46	99.95%	17	99.98%	0.78	🟢	🟢	🟢	🟡
Kaspersky SMG	1	0.3%	74	99.92%	31	99.96%	0.78	🟢	🟢	🟢	🟡
Libra Esva	1	0.3%	10	99.99%	7	99.99%	0.06	🟢	🟢	🟢	🟢
modusGate	1	0.3%	83	99.91%	13	99.98%	0.14	🟢	🟢	🟢	🟢
Netmail Secure	5	1.6%	29	99.97%	0	100.00%	0.06	🟢	🟢	🟡	🟡
OnlyMyEmail	5	1.6%	1	99.999%	0	100.00%	0.01	🟢	🟢	🟢	🟢
Scrollout	12	3.7%	23	99.98%	27	99.97%	0.12	🟢	🟢	🟢	🟢
Sophos	0	0.0%	193	99.80%	68	99.92%	0.21	🟢	🟢	🟢	🟢
SpamTitan	1	0.3%	81	99.92%	5	99.99%	0.13	🟢	🟢	🟢	🟢
Vade Retro MailCube	2	0.6%	348	99.64%	25	99.97%	0.62	🟢	🟢	🟢	🟢
ZEROSPAM	10	3.1%	110	99.88%	8	99.99%	0.2	🟢	🟢	🟢	🟢
Spamhaus DBL	0	0.0%	47772	49.93%	60105	26.77%	15.89				
Spamhaus ZEN	0	0.0%	4984	94.78%	656	99.20%	1.47				
Spamhaus ZEN+DBL	0	0.0%	3304	96.54%	567	99.31%	1.19				

** The Spamhaus products are partial solutions and their performance should not be compared with that of other products.*

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

🟢 *0–30 seconds;* 🟡 *30 seconds to two minutes;* 🟠 *two minutes to 10 minutes;* 🔴 *more than 10 minutes.*

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

The impressive spam catch rate of 99.96% achieved by *Kaspersky*'s *Linux Mail Security* product this month was marginally higher than the catch rate it managed in the last test. With no false positives in the ham corpus and just one message misclassified in the tricky newsletter corpus, the product easily earned its 13th VBSpam+ award.

Kaspersky Secure Mail Gateway

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.3%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟡

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Retro MailCube	DrWeb; proprietary	√	√	√		√	√
ZEROSPAM	ClamAV			√		√	√

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender, ClamAV	√				√		√	√
ESET	ESET ThreatSense					√	√		
FortiMail	Fortinet	√	√	√	√	√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Kaspersky SMG	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
modusGate	Avira; Bitdefender		√	√		√	√		
Netmail Secure	Proprietary	√	√	√		√		√	
Scrollout	ClamAV			√		√		√	
Sophos	Sophos		√	√				√	√
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	

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

Like its *Linux* counterpart, the virtual version of *Kaspersky*'s product combined a marginal increase in its spam catch rate with a lack of false positives and just a single blocked newsletter – the same one, unsurprisingly. This means that there is ample choice of product, even for those customers who have narrowed their choice down to using *Kaspersky*. Of course, *Secure Mail Gateway* also earned a VBSpam+ award.

Libra Esva 3.6.5.0

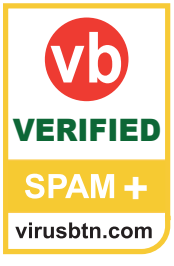
SC rate: 99.99%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Product	Final score
ESET	99.999
Bitdefender	99.99
Libra Esva	99.98
Kaspersky LMS	99.95
IBM	99.95
OnlyMyEmail	99.95
FortiMail	99.95
modusGate	99.94
Kaspersky SMG	99.93
Netmail Secure	99.88
SpamTitan	99.79
Vade Retro MailCube	99.77
Sophos	99.75
Axway	99.66
ZEROSPAM	99.58
Egedian	99.52
GFI	99.34
Scrollout	99.10

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

In this test *Libra Esva* put in a performance that was identical to that in the last test – which is great news as it performed very well back then: a 99.99% spam catch rate, no false positives, a single blocked newsletter and a final score of 99.98. Once again this results in one of the highest final scores in the test and of course another VBSpam+ award for the Italian hosted solution.

modusGate



SC rate: 99.95%
FP rate: 0.00%
Final score: 99.94
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In its third appearance since its return to the VBSpam tests, *modusGate* continues its good performance with a 99.95% catch rate, a lack of false positives and just a single blocked newsletter. The product easily earns another VBSpam+ award.

Netmail Secure

SC rate: 99.98%
FP rate: 0.01%
Final score: 99.88
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 100.00%
Newsletters FP rate: 1.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

I was pleased to see *Netmail Secure* return to our test bench this month as the product has a long and successful VBSpam history, going back to the first test. I was even more pleased to find that the product missed just 29 out of more than 177,000 spam emails. It did erroneously block a single legitimate email, and thus was denied a VBSpam+ award, but a regular VBSpam award is well deserved.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 1.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Yet again, *OnlyMyEmail*'s spam catch rate falls within a rounding error of 100%: the product missed just a single spam email – fewer than any other product. Alongside that, it didn't block any legitimate emails and misclassified just five newsletters, resulting in a final score of 99.95 and yet another VBSpam+ award.

Scrollout F1

SC rate: 99.97%
FP rate: 0.15%
Final score: 99.10
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.97%
Newsletters FP rate: 3.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

I was rather pleased to see *Scrollout F1* achieve a pass in the last VBSpam test with a very high catch rate. It did so again this time around. It did have some false positives – more than any other product, and also more than it had in the last test – but the final score remained above 99 and the open-source product earns another VBSpam award.

Sophos Email Appliance

SC rate: 99.85%
FP rate: 0.02%
Final score: 99.75
Project Honey Pot SC rate: 99.80%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

We found mostly dating and medical spam among the emails missed by *Sophos*'s *Email Appliance*, but there were only 261 of them, which out of a corpus of more than 177,000 emails is a very small number, showing that the product did its job well. It did block two legitimate emails – from the same sender – which denied it a VBSpam+ award, but it is worth mentioning that no newsletters were blocked and with a final score of 99.75 a VBSpam award is certainly well deserved.

SpamTitan 6.00

SC rate: 99.95%
FP rate: 0.03%
Final score: 99.79
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Yet again, *SpamTitan* blocked well over 99.95% of all spam emails in the test, though for the first time in a little while it did not manage to avoid false positives. The three of these meant that it missed out on a VBSpam+ award on this occasion, but with a final score of 99.79 a regular VBSpam award is easily earned.

Vade Retro MailCube

SC rate: 99.79%
FP rate: 0.00%
Final score: 99.77
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Even though *Vade Retro* hasn't participated in our tests since the beginning of 2012, we have followed the company's progress with interest and watched it become a prominent player in the international security market. Now, the company returns to our tests to demonstrate to (potential) customers how well its *MailCube* product blocks spam.

It does this well: the product blocked 99.79% of spam emails and, perhaps more importantly, it didn't block any legitimate emails. With just two blocked newsletters – one in Russian and one in French – *Vade Retro* makes a triumphant return to our tests with a VBSpam+ award.

ZEROSPAM

SC rate: 99.93%
FP rate: 0.05%
Final score: 99.58
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.99%
Newsletters FP rate: 3.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Although, like every other anti-spam solution, *ZEROSPAM* didn't reduce the spam to zero, at 0.07% (or a block rate of 99.93%) it came pretty close. It did have some false positives in both corpora, which denied the product a VBSpam+ award, but yet another VBSpam award is well deserved.

Spamhaus DBL

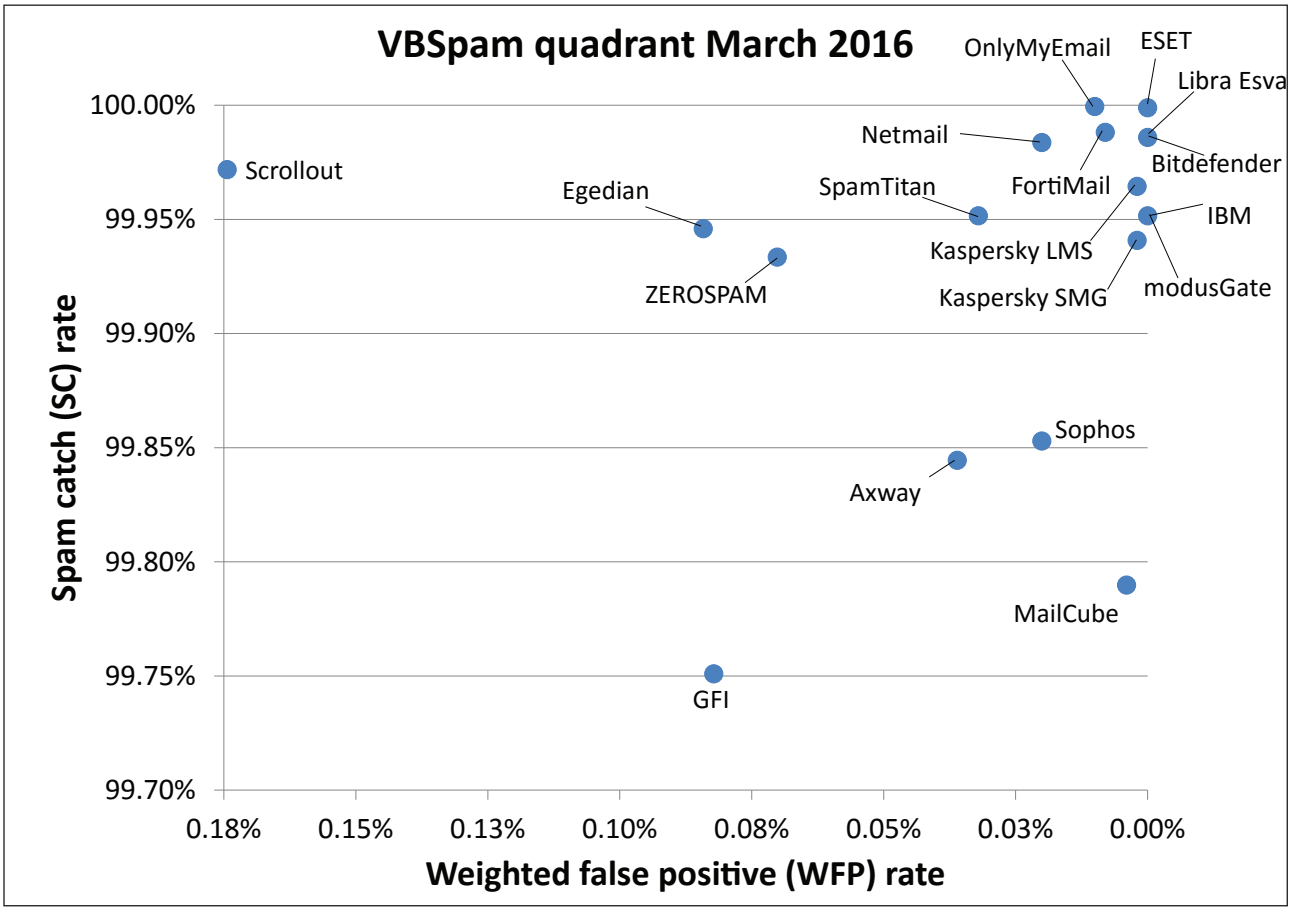
SC rate: 39.22%
FP rate: 0.00%
Final score: 39.22
Project Honey Pot SC rate: 49.93%
Abusix SC rate: 26.77%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 96.82%
FP rate: 0.00%
Final score: 96.82
Project Honey Pot SC rate: 94.78%
Abusix SC rate: 99.20%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 97.82%
FP rate: 0.00%
Final score: 97.82
Project Honey Pot SC rate: 96.54%
Abusix SC rate: 99.31%
Newsletters FP rate: 0.0%



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

In this test, the various DNS blacklists provided by *The Spamhaus Project* stopped fewer emails in their tracks than they did in January – in particular, domain-based blocking became less effective – but such changes tend to say as much about the ever-changing spam landscape as they do about the product. With no false positives, it remains the case that the inclusion of a blacklist like *Spamhaus* could be a great first layer in many a spam filter.

CONCLUSION

We were pleased to see that the high catch rates of the last test were, if not repeated, at least approached again. The billions of people who use email every day have good reason to feel well protected by this important part of a layered security model.

The next VBSpam test will run in April and May 2016, with the results scheduled for publication in May. Developers interested in submitting products, or who want to know more about how Virus Bulletin can help their company measure or improve its spam filter performance, should email martijn.grooten@virusbtn.com.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com Web: https://www.virusbulletin.com/