JULY 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW JULY 2015

INTRODUCTION

Times are exciting for *Virus Bulletin* in general and for the VBSpam test in particular. A new member has just joined the team to help run the VBSpam tests, we're building a new environment on which to run the tests, and we're also working on an extra vector to be tested.

Thanks to the combined effects of a holiday and the ongoing preparations for the annual VB Conference, this report appears later than planned – though we have already published a summary of the results. Alongside a test summary, however, we believe it is important to detail the individual performance of each product, which is what you will find in this report.

As already mentioned in the summary, the overall performance in this test was good, resulting in 14 VBSpam awards among the 15 participating solutions, with five of them achieving a VBSpam+ award.

THE TEST SET-UP

The VBSpam test methodology can be found at http://www.virusbtn.com/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)

Products earn VBSpam certification if the value of the final score is at least 98:

SC - (5 x WFP) ≥ 98

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives and no more than 2.5% false positives among the newsletters earn a VBSpam+ award.

THE EMAIL CORPUS

The test started on Saturday 23 June at 12am and finished 16 days later, on Monday 8 July at 12am. On this occasion there were no serious issues affecting the test.

The test corpus consisted of 166,129 emails. 156,250 of these emails were spam, 61,870 of which were provided by *Project Honey Pot*, with the remaining 94,380 spam emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 9,552 legitimate emails ('ham') and 327 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. Comparing this chart with that published in May, one can immediately see that there were higher catch rates on this occasion.

ISSN 1749-7027

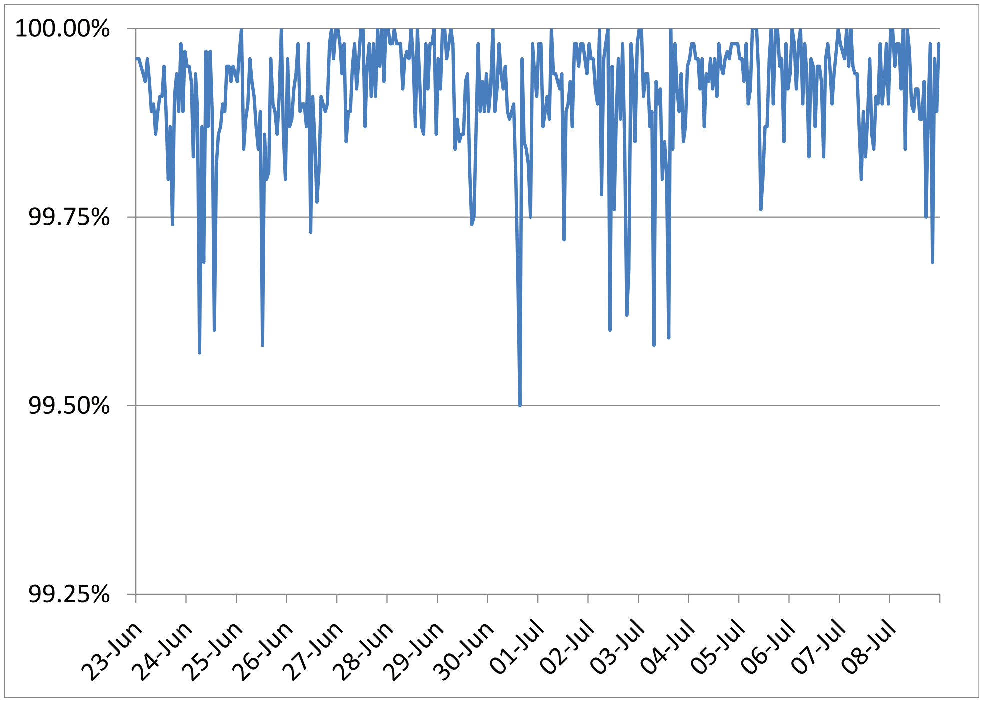


Figure 1: Spam catch rate of all full solutions throughout the test period.

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' refers to a message in that corpus that has been erroneously marked by a product as spam.

Axway MailGate 5.3.1

SC rate: 99.79%

FP rate: 0.05%

Final score: 99.44

Project Honey Pot SC rate: 99.52%

Abusix SC rate: 99.97%

Newsletters FP rate: 2.8%

For *Axway*'s *MailGate* virtual appliance, the July test was good on all fronts: the product saw its spam catch rate increase to almost 99.8% – the highest it has ever been in our tests – and with just five false positives, the glitch the product experienced in the May test was proven to have been a one-off occurrence. With a decrease in the false positive rate among the newsletters as well, *Axway*'s developers have plenty to be pleased about and the product earns its eighth VBSpam award in a row.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.96%

FP rate: 0.00%

Final score: 99.95

Project Honey Pot SC rate: 99.94%

Abusix SC rate: 99.97%

Newsletters FP rate: 0.3%

A VBSpam participant and award winner since the very first test, *Bitdefender* has already notched up 13 VBSpam+ awards. In this test, the product blocked 99.96% of spam emails and no legitimate emails, achieving the fourth highest final score – and earning its 14th VBSpam+ award.

Egedian Mail Security

SC rate: 99.93%

FP rate: 0.01%

Final score: 99.82

Project Honey Pot SC rate: 99.86%

Abusix SC rate: 99.97%

Newsletters FP rate: 1.5%

Egedian has been a VBSpam participant since the spring of 2014, and we have seen a gradual improvement in the product's performance over time. On this occasion there was further improvement, with the product blocking no fewer than 99.93% of the emails in our spam feeds (having blocked only just over 99% in the last test). While such significant increases in catch rate are often accompanied by an increase in false positive rate, the virtual solution blocked just one legitimate email, meaning that it easily earns its seventh VBSpam award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%

vb VERIFIED SPAM + virusbtn.com

ESET's VBSpam history goes back three years – and its VB100 history much longer than that – but for this test, the company submitted a different solution from the one we have tested before: one that also works with *Microsoft*'s popular *Exchange Server* mail server, but which includes, as the company described it, a 'completely remodelled anti-spam engine developed internally by *ESET*'.

It is thus a little unfair to compare this month's test results with those of the other *ESET* solution we have tested, but in fact this new product would have looked good against just about any other product: it misclassified a mere 21 spam emails (out of more than 155,000), and there were no false positives in either feed. The second highest final score this month and a VBSpam+ award make this a fantastic debut for *ESET*'s *Mail Security for Microsoft Exchange Server*.

Fortinet FortiMail

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%

vb VERIFIED SPAM + virusbtn.com

In its long VBSpam test history, which goes all the way back to the second VBSpam test, *Fortinet*'s *FortiMail* appliance has always performed well, never missing a VBSpam award, and earning several VBSpam+ awards along the way. But a 99.98% catch rate is impressive even by these standards. Moreover, the appliance didn't block any of the more than 9,500 legitimate emails and blocked just a single newsletter, resulting in the third highest final score and the company's fifth VBSpam+ award.

GFI MailEssentials

SC rate: 99.67%
FP rate: 0.00%
Final score: 99.66
Project Honey Pot SC rate: 99.68%
Abusix SC rate: 99.66%
Newsletters FP rate: 0.3%

vb VERIFIED SPAM + virusbtn.com

GFI's *MailEssentials* is one of the products for which this month's test only brings good news. The *Windows*-based solution saw its performance improve in all three vectors, with most notably a total lack of false positives. The product's seventh VBSpam+ award is thus very well deserved.

IBM Lotus Protector for Mail Security

SC rate: 99.87%
FP rate: 0.02%
Final score: 99.75
Project Honey Pot SC rate: 99.70%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%

vb VERIFIED SPAM virusbtn.com

Like almost all products in this month's test, *IBM* saw its spam catch rate improve slightly – to 99.87%. However, it also blocked more legitimate emails than it did in May's test: two, compared to a clean sheet back then. It thus misses out on a VBSpam+ award for the first time this year, nevertheless it easily achieved a VBSpam award.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.92%
FP rate: 0.02%
Final score: 99.81
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%

vb VERIFIED SPAM virusbtn.com

Until this month, *Kaspersky*'s *Linux*-based anti-spam solution had the honour of being the

Product name	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	9547	5	0.05%	329	155921	99.79%	99.44
Bitdefender	9552	0	0.00%	59	156191	99.96%	99.95
Egedian	9551	1	0.01%	115	156135	99.93%	99.82
ESET	9552	0	0.00%	21	156229	99.99%	99.99
FortiMail	9552	0	0.00%	27	156223	99.98%	99.97
GFI	9552	0	0.00%	521	155729	99.67%	99.66
IBM	9550	2	0.02%	208	156042	99.87%	99.75
Kaspersky LMS	9550	2	0.02%	128	156122	99.92%	99.81
Libra Esva	9551	1	0.01%	37	156213	99.98%	99.91
McAfee SaaS	9547	5	0.05%	247	156003	99.84%	99.54
OnlyMyEmail	9552	0	0.00%	1	156249	99.999%	99.999
Scrollout	9324	228	2.39%	777	155473	99.50%	86.97
Sophos	9551	1	0.01%	281	155969	99.82%	99.77
SpamTitan	9551	1	0.01%	103	156147	99.93%	99.85
ZEROSPAM	9549	3	0.03%	164	156086	99.90%	99.69
Spamhaus DBL*	9548	4	0.04%	108059	48191	30.84%	30.63
Spamhaus ZEN*	9552	0	0.00%	11393	144857	92.71%	92.71
Spamhaus ZEN+DBL*	9548	4	0.04%	7147	149103	95.43%	95.22

**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.*

product with the current longest unbroken run of VBSpam+ awards, having not missed any since November last year. Unfortunately, that record was broken this month when the product missed two legitimate emails – both written in English. This doesn't mean this wasn't yet another decent set of results for the product, but on this occasion a standard VBSpam award has to suffice.

Libra Esva 3.4.1.0

SC rate: 99.98%

FP rate: 0.01%

Final score: 99.91

Project Honey Pot SC rate: 99.95%

Abusix SC rate: 100.00%

Newsletters FP rate: 0.3%

More often than not in the past two years, *Libra Esva* has achieved a VBSpam+ award. So the results of this test, when a single legitimate email prevented it from doing so, will no doubt be seen as a disappointment. A small one, hopefully, as the virtual appliance blocked an impressive 99.98% of spam and, amid fierce competition, ended up with the fifth highest final score.

McAfee SaaS Email Protection

SC rate: 99.84%

FP rate: 0.05%

Final score: 99.54

Project Honey Pot SC rate: 99.68%

Abusix SC rate: 99.95%

Newsletters FP rate: 1.2%

You win some, you lose some. The spam catch rate of *McAfee*'s SaaS solution increased by almost a percentage point to 99.84% – we noticed quite a

	Newsletters		Project Honey Pot		Abusix		STDev[†]
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	
Axway	9	2.8%	299	99.52%	30	99.97%	0.28
Bitdefender	1	0.3%	35	99.94%	24	99.97%	0.14
Egedian	5	1.5%	89	99.86%	26	99.97%	0.17
ESET	0	0.0%	14	99.98%	7	99.99%	0.13
FortiMail	1	0.3%	17	99.97%	10	99.99%	0.07
GFI	1	0.3%	200	99.68%	321	99.66%	0.41
IBM	1	0.3%	186	99.70%	22	99.98%	0.24
Kaspersky LMS	0	0.0%	54	99.91%	74	99.92%	0.25
Libra Esva	1	0.3%	34	99.95%	3	100.00%	0.1
McAfee SaaS	4	1.2%	198	99.68%	49	99.95%	0.22
OnlyMyEmail	0	0.0%	0	100.00%	1	99.999%	0.01
Scrollout	167	51.1%	247	99.60%	530	99.44%	0.8
Sophos	0	0.0%	264	99.57%	17	99.98%	0.26
SpamTitan	3	0.9%	89	99.86%	14	99.99%	0.18
ZEROSPAM	5	1.5%	136	99.78%	28	99.97%	0.19
Spamhaus DBL[*]	0	0.0%	20226	67.31%	87833	6.94%	6.83
Spamhaus ZEN[*]	0	0.0%	8671	85.99%	2722	97.12%	2.37
Spamhaus ZEN+DBL[*]	0	0.0%	4531	92.68%	2616	97.23%	1.69

[*] *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.*

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

few emails in French and Spanish among those that were missed – but against that stood five false positives (from three different senders). Nevertheless, the product's final score improved significantly and easily earns *McAfee* another VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%

FP rate: 0.00%

Final score: 99.999

Project Honey Pot SC rate: 100.00%

Abusix SC rate: 99.999%

Newsletters FP rate: 0.0%

A dubious advertisement for a financial product in German – that we believe should be classified as spam – was the only one of more than 165,000 emails that *OnlyMyEmail* classified incorrectly. It's the sort of thing we've come to expect from this hosted solution, but it's still impressive. Of course, the product ends up with the highest final score and another VBSpam+ award – the product's tenth.

Scrollout F1

SC rate: 99.50%

FP rate: 2.39%

Final score: 86.97

Project Honey Pot SC rate: 99.60%

Abusix SC rate: 99.44%

Newsletters FP rate: 51.1%

Scrollout F1 isn't having a good run in our tests. While a spam catch rate of 99.50% is certainly decent enough (albeit the lowest among all full solutions in this test), the

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
McAfee SaaS	McAfee	√	√	√		√	√
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
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	√				√		√	√
ESET	ESET Threatsense					√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Profil	Bitdefender	√				√		√	√
Scrollout	ClamAV			√		√		√	
Sophos	Sophos		√	√				√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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

product's false positive rate – well over 2% – is simply poor. So poor, that we've come to suspect that the product might not be fully adjusted to the test environment – a view that is shared by the product's developers. While they are looking into the issue, we are forced to deny the open-source solution a VBSpam award.

Sophos Email Appliance

SC rate: 99.82%

FP rate: 0.01%

Final score: 99.77

Project Honey Pot SC rate: 99.57%

Abusix SC rate: 99.98%

Newsletters FP rate: 0.0%

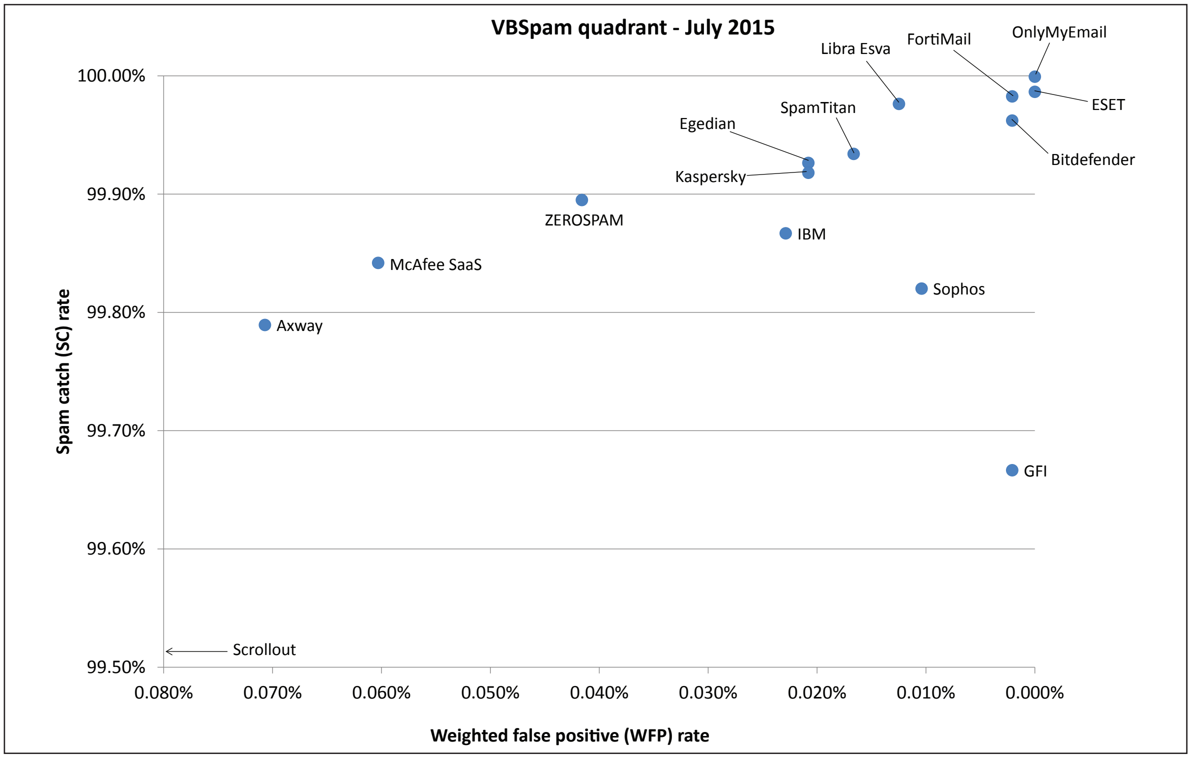
A single legitimate email in this test was blocked by *Sophos*'s *Email Appliance*. The reason is often unclear for us as testers, but in this case it might have been the use of various (legitimate) URL shorteners. In any case, the false positive prevents the product from achieving another VBSpam+ award in what was otherwise a very good test, in which its catch rate increased slightly and its newsletter false positive rate dropped to zero. Another VBSpam award, *Sophos*'s 33rd, is thus more than well deserved.

SpamTitan 6.00

SC rate: 99.93%

FP rate: 0.01%

Final score: 99.85



(Please refer to the full report for full product names and details.)

SpamTitan 6.00 contd.

Project Honey Pot SC rate: 99.86%

Abusix SC rate: 99.99%

Newsletters FP rate: 0.9%

It was also a single false positive for *SpamTitan* that prevented it from achieving another VBSpam+ award in an otherwise decent performance – the product missed just 103 spam emails in a variety of languages and blocked three newsletters. Another VBSpam award should keep the developers motivated to get that 'plus' back though.

ZEROSPAM

SC rate: 99.90%

FP rate: 0.03%

Final score: 99.69

Project Honey Pot SC rate: 99.78%

Abusix SC rate: 99.97%

Newsletters FP rate: 1.5%

With the exception of the newsletters – which is a small corpus that contributes little overall – *ZEROSPAM*'s performance on this occasion was very similar to that in the last test. Three false positives in as many different languages prevented the product from earning another VBSpam+ award, but after missing slightly fewer than one in a thousand spam emails, its 21st VBSpam award is well deserved.

Spamhaus DBL

SC rate: 30.84%

FP rate: 0.04%

Final score: 30.63

Project Honey Pot SC rate: 67.31%

Abusix SC rate: 6.94%

Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 92.71%

FP rate: 0.00%

Final score: 92.71

Project Honey Pot SC rate: 85.99%

Abusix SC rate: 97.12%

Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 95.43%

FP rate: 0.04%

Final score: 95.22

Project Honey Pot SC rate: 92.68%

Abusix SC rate: 97.23%

Newsletters FP rate: 0.0%

The performance of *Spamhaus* in these tests remains volatile, which is natural for the partial solution: spam filtering is a multi-layered approach and *Spamhaus* only offers two of these layers (IP and domain blocking); hence we don't count it as a full product.

In this test, the *DBL* domain blacklist performed significantly better than it did in the last test, although there were four false positives due to the inclusion of two domains that, our feeds show, were also used in legitimate emails. The catch rate for the *ZEN* aggregated IP-based blacklist decreased slightly, but there were no false positives, while the catch rate for the combined list remained well over 95%.

CONCLUSION

July 2015 was a good month for products in the VBSpam test. As always, one is right to wonder whether this was a mere coincidence – behind the decimal point, the performance of spam filters tends to be volatile – or whether this is part of a trend. The next test will tell – and will also introduce a new metric that shows how much the various filters delay the emails that are sent through them.

The next VBSpam test will have finished by the time this report is published, with the results scheduled for publication in September. The test following that will run in October, with the results scheduled for publication in November. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Lewis Jones

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

© 2015 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/