JANUARY 2016

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW JANUARY 2016

INTRODUCTION

We have always made it clear that the numbers produced by the VBSpam tests should be seen within the context of the test: a product that blocks 99.90% of spam emails in this test probably wouldn't block 999 out of every thousand spam emails in a real situation.

There are a number of reasons for this, the most important of which is that the spam we use in our test is somewhat biased towards the larger campaigns and less towards the dubious companies that send you weekly emails just because they sneakily got hold of your email address at a trade show 12 years ago.

Of course, it's the former kind of email that tends to be the most damaging and is more likely to contain a malicious attachment or a link to a website serving malware. Indeed, such campaigns are also the focus of most spam filters, which for that reason are often called 'email security solutions'.

Still, I feel obliged to urge some caution when interpreting the results of this test, in which all participating products performed exceptionally well. While this is certainly great news – and something the developers should be proud of – it doesn't mean that using one of these spam filters will reduce the chance of bad emails reaching you to all but zero.

Of course, no security product does that, and spam filters do at least make the email lives of your users a lot easier – and a lot more secure.

Sixteen full anti-spam solutions participated in this test, all of which easily achieved a VBSpam award by blocking 99.8% or more spam. What's more, ten solutions reached the performance level required to earn 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

Products earn VBSpam certification if the value of the final score is at least 98 *and* the 'delivery speed colours' at 10

ISSN 1749-7027

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

Our test set-up runs 365 days a year (366 days in 2016), and thus starting the test on Christmas Day, 25 December, wasn't a problem. However, after a few days, one of the hypervisors running a number of products crashed due to a hard disk failure. While we were able to resolve the issue relatively quickly, we decided to start the test from scratch on Wednesday 30 December at 12am.

The test finished 16 days later, on Friday 14 January 2016 at 12am. An unrelated issue on the morning of 9 January forced us to exclude a few hours' worth of emails. Other than this, though, there were no significant issues affecting the test.

The test corpus consisted of 225,571 emails – more than we've seen in our tests in a long time. 216,053 of these emails were spam, 117,355 of which were provided by *Project Honey Pot*, with the remaining 98,698 provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 9,201 legitimate emails ('ham') and 317 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. Other than the fact that catch rates were very high, there is little that can be read from this graph.

RESULTS

Axway MailGate 5.3.1

SC rate: 99.89%
FP rate: 0.04%
Final score: 99.46
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.98%
Newsletters FP rate: 6.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

For *Axway*, as for many other products, this test saw the highest spam catch rate to date. The *MailGate* virtual appliance missed just 237 spam emails – quite a few of which were written in Brazilian Portuguese. Four false

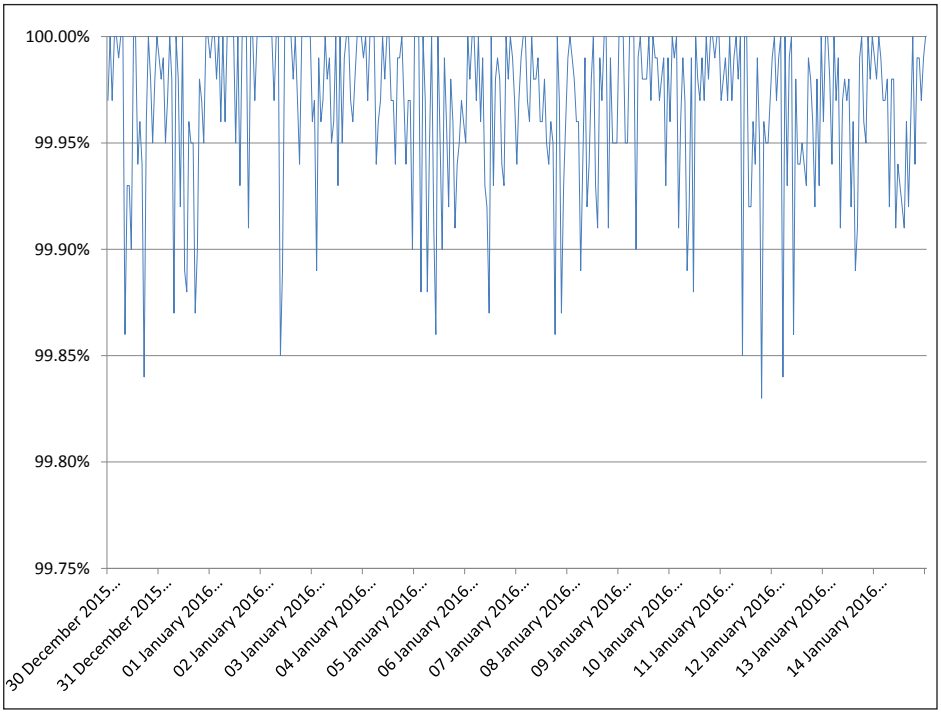


Figure 1: Spam catch rate of all full solutions throughout the test period.

positives and 20 erroneously blocked newsletters (mostly in English and German) meant a VBSpam+ award was out of the question on this occasion, but the product easily earns its 11th VBSpam award in a row.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.998%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender has a long history in these tests, going all the way back to the first VBSpam test in May 2009, and the product has performed well in every one of them. Yet never before has it performed this well: missing just four spam emails and blocking one newsletter as a sole false positive. With an impressively high final score, *Bitdefender*'s developers earn another VBSpam+ award to add to their collection.

Egedian Mail Security

SC rate: 99.96%
FP rate: 0.01%
Final score: 99.89
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The last test saw *Egedian* earn its first VBSpam+ award. This time, a single missed legitimate email put paid to the product earning its second. However, with a spam catch rate of 99.96% and just one newsletter false positive, the product's performance was almost as good – and certainly well deserving of a VBSpam award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.995%
FP rate: 0.00%
Final score: 99.995
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The November 2015 test saw *ESET* achieve a 'clean sheet' (no false positives at all) and a final score of 99.99 – a performance that would surely be hard to outdo. Yet the product did just that. Missing only ten spam emails (half of which were from the *Constant Comcast* ESP) in a corpus of more than 200,000 emails, the product achieved a final score of 99.995 – once again better than that of any other product. Clearly *ESET* is deserving of another VBSpam+ award.

Fortinet FortiMail

SC rate: 99.998%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 100.00%
Newsletters FP rate: 1.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet's *FortiMail* appliance has long been performing well in our tests, but its performance has improved even further in the past six months. Missing just four spam emails and erroneously blocking just three newsletters, the appliance gets a final score of 99.97 – its fourth 99.9+ score in a row – and also earns *Fortinet*'s developers their eighth VBSpam+ award.

GFI MailEssentials

SC rate: 99.80%
FP rate: 0.00%
Final score: 99.76
Project Honey Pot SC rate: 99.76%
Abusix SC rate: 99.85%
Newsletters FP rate: 1.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

GFI's *MailEssentials* product skipped the previous test (for reasons beyond the developers' control), so I was happy to see it return in this test. And not just that, the product didn't block a single ham email (and only blocked four newsletters), while missing fewer than one in 500 spam emails, resulting in a final score of 99.76 and the product's fifth VBSpam+ award.

IBM Lotus Protector for Mail Security

SC rate: 99.95%
FP rate: 0.01%
Final score: 99.90
Project Honey Pot SC rate: 99.91%

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	9197	4	0.04%	237	215816	99.89%	99.46
Bitdefender	9201	0	0.00%	4	216049	99.998%	99.99
Egedian	9200	1	0.01%	93	215960	99.96%	99.89
ESET	9201	0	0.00%	10	216043	99.995%	99.995
FortiMail	9201	0	0.00%	4	216049	99.998%	99.97
GFI	9201	0	0.00%	429	215624	99.80%	99.76
IBM	9200	1	0.01%	101	215952	99.95%	99.90
Kaspersky LMS	9201	0	0.00%	102	215951	99.95%	99.95
Kaspersky SMG	9201	0	0.00%	145	215908	99.93%	99.93
Libra Esva	9201	0	0.00%	23	216030	99.99%	99.98
modusGate	9201	0	0.00%	142	215911	99.93%	99.93
OnlyMyEmail	9201	0	0.00%	0	216053	100.00%	99.99
Scrollout	9196	5	0.05%	39	216014	99.98%	99.57
Sophos	9199	2	0.02%	249	215804	99.88%	99.77
SpamTitan	9201	0	0.00%	84	215969	99.96%	99.95
ZEROSPAM	9198	3	0.03%	38	216015	99.98%	99.69
Spamhaus DBL*	9201	0	0.00%	96137	119916	55.50%	55.50
Spamhaus ZEN*	9201	0	0.00%	5905	210148	97.27%	97.27
Spamhaus ZEN+DBL*	9201	0	0.00%	3510	212543	98.38%	98.38

**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.)*

IBM Lotus Protector for Mail Security contd.

Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM's catch rate of 99.95% in the last test was impressive, and this test proved that it wasn't a one-off thing: the product once again blocked fewer than one in 2,000 spam emails. Unfortunately, there was a single false positive, which prevented it from earning a VBSpam+ award – but with the product's highest final score to date, the developers of *Lotus Protector for Mail Security* have enough reason to be content with their VBSpam award.

Kaspersky Security 8 for Linux Mail Servers

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky's *Linux Mail Security* has had a number of clean sheets before, showing that the product doesn't stumble much over the harder-to-filter newsletters. This was once again the case in this test, and the product missed just over 100 spam emails in a very large corpus, resulting in a final score of 99.95 and the product's 12th VBSpam+ award.

	Newsletters		Project Honey Pot		Abusix		STDev†	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	20	6.3%	218	99.81%	19	99.98%	0.35	●	●	●	●
Bitdefender	1	0.3%	4	99.997%	0	100.00%	0.02	●	●	●	●
Egedian	1	0.3%	93	99.92%	0	100.00%	0.09	●	●	●	●
ESET	0	0.0%	10	99.99%	0	100.00%	0.03	●	●	●	●
FortiMail	3	1.0%	4	99.997%	0	100.00%	0.02	●	●	●	●
GFI	4	1.3%	280	99.76%	149	99.85%	0.28	●	●	●	●
IBM	0	0.0%	100	99.91%	1	100.00%	0.11	●	●	●	●
Kaspersky LMS	0	0.0%	77	99.93%	25	99.97%	0.12	●	●	●	●
Kaspersky SMG	0	0.0%	104	99.91%	41	99.96%	0.13	●	●	●	●
Libra Esva	1	0.3%	23	99.98%	0	100.00%	0.04	●	●	●	●
modusGate	0	0.0%	140	99.88%	2	100.00%	0.17	●	●	●	●
OnlyMyEmail	1	0.3%	0	100.00%	0	100.00%	0	●	●	●	●
Scrollout	13	4.1%	37	99.97%	2	100.00%	0.05	●	●	●	●
Sophos	1	0.3%	239	99.80%	10	99.99%	0.17	●	●	●	●
SpamTitan	1	0.3%	84	99.93%	0	100.00%	0.09	●	●	●	●
ZEROSPAM	12	3.8%	38	99.97%	0	100.00%	0.06	●	●	●	●
Spamhaus DBL*	0	0.0%	17895	84.75%	78242	20.73%	12.21				
Spamhaus ZEN*	0	0.0%	5016	95.73%	889	99.10%	1.4				
Spamhaus ZEN+DBL*	0	0.0%	2890	97.54%	620	99.37%	1				

** 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.)

Kaspersky Secure Mail Gateway

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

As its name suggests, *Kaspersky*'s *Linux Mail Security* product runs on a *Linux* server. But for the increasing number of organizations that have 'gone virtual', the security giant has a virtual solution as well.

As one would expect from any virtual solution, setting up *Kaspersky Secure Mail Gateway* involves little more than adding it to a hypervisor (*VMware*, in our case) and adding the virtual machine to the network.

The product's performance was pretty good, with a spam catch rate that was almost as good as the *Linux* version of the product (and at 99.93% still very high) and a clean sheet as far as false positives were concerned. *Kaspersky* thus earns a VBSpam+ award for its virtual product on its debut.

Libra Esva 3.6

SC rate: 99.99%
FP rate: 0.00%

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
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	√				√		√	√
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		√	√		√	√		
Scrollout	ClamAV			√		√		√	
Sophos	Sophos		√	√				√	√
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	

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

Libra Esva 3.6 contd.

Final score: 99.98
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Given its very strong history, 2015 was a relatively 'poor' year for *Libra Esva*, which 'only' achieved a VBSpam+ award in half of the tests it entered (earning a VBSpam award in all the rest). 2016 has started very well for the Italian solution, however, which missed just 23 spam emails in this test, had no false positives and blocked just a single newsletter. As such, with an impressive final score of 99.98, another VBSpam+ award is well deserved.

modusGate

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In November, *Vircom*'s *modusGate* solution returned to our tests with an impressive performance (and a VBSpam+

Product	Final score
ESET	99.995
OnlyMyEmail	99.99
Bitdefender	99.99
Libra Esva	99.98
FortiMail	99.97
Kaspersky LMS	99.95
SpamTitan	99.95
modusGate	99.93
Kaspersky SMG	99.93
IBM	99.90
Egedian	99.89
Sophos	99.77
GFI	99.76
ZEROSPAM	99.69
Scrollout	99.57
Axway	99.46

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

award for its efforts). In this test it managed to keep the momentum going and even outperformed itself by quite a bit, achieving a spam catch rate of 99.93% and a clean sheet. *modusGate* thus easily earns its second VBSpam+ award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

OnlyMyEmail's performance in this test might not stand out very much, so it's worth noting that its catch rate hasn't dipped lower than 99.99% for the past four years. On occasion it has even been a full 100% – as it was in this test, where a single blocked newsletter got in the way of a perfect score. Of course, with the second highest final score, *OnlyMyEmail* easily earns a VBSpam+ award.

Scrollout F1

SC rate: 99.98%
FP rate: 0.05%
Final score: 99.57
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 100.00%
Newsletters FP rate: 4.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

When *Scrollout F1*, a free and open source solution, failed to pass the most recent VBSpam test, we added a footnote suggesting that this may in part have been due to a configuration issue. We are pleased to report that, with this issue solved, the product increased its spam catch rate, on this occasion blocking 99.98% of spam. There were a handful of false positives, but nevertheless, this was a very good start to the year for *Scrollout*.

Sophos Email Appliance

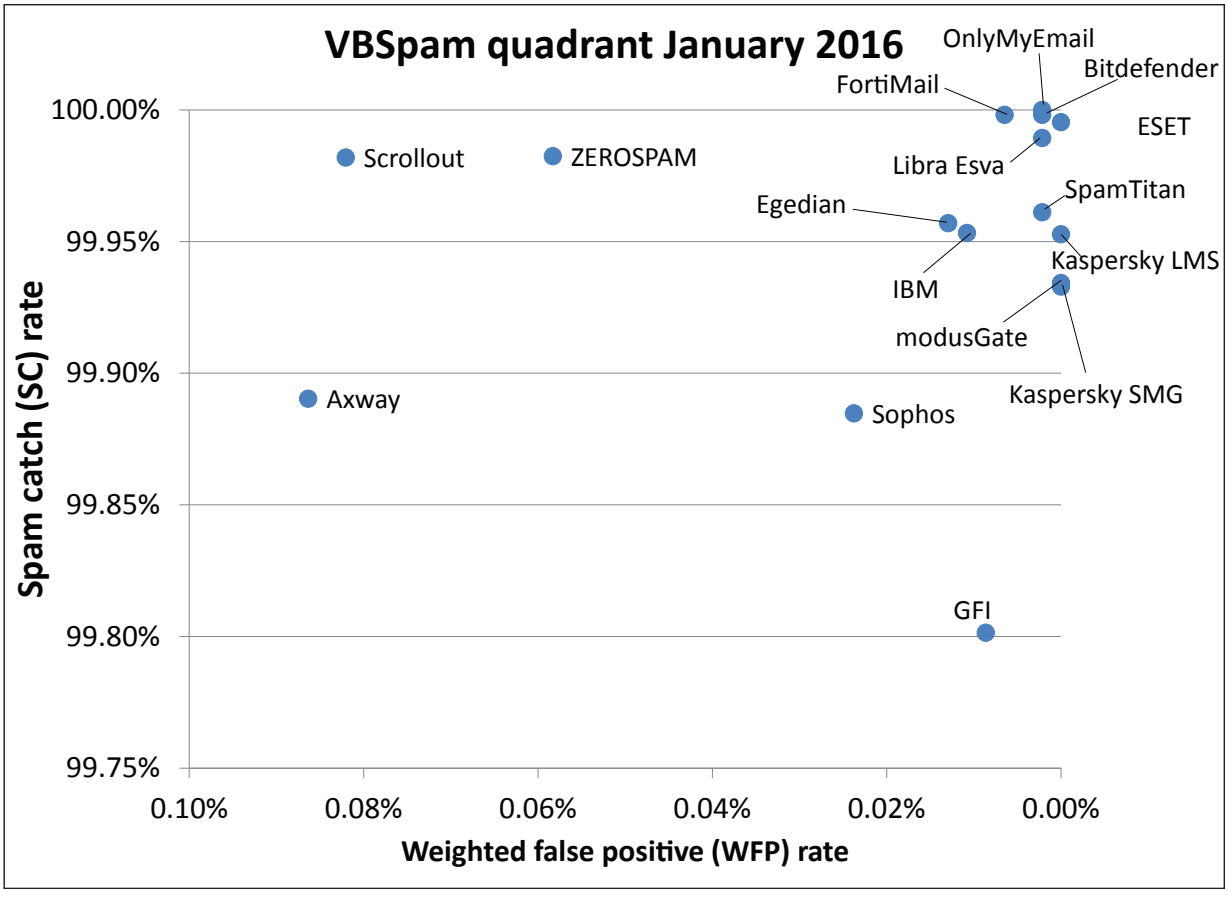
SC rate: 99.88%
FP rate: 0.02%
Final score: 99.77
Project Honey Pot SC rate: 99.80%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos's *Email Appliance* keeps edging close to another VBSpam+ award but two false positives this month meant that such an accolade wasn't in the bag this time. Still, with a really good catch rate of 99.88% and just one newsletter false positive, there are enough reasons for the product's developers to be happy with their 36th VBSpam award in as many tests.

SpamTitan 6.00

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

For the fourth time in a row, *SpamTitan* blocked more than 99.9% of spam – and for the third time in a row, it did so without any false positives. Noting that the two yellow marks in the speed performance should really be very pale yellow (these emails were returned in just a shade over 30



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

seconds), the product fully deserves its ninth VBSpam+ award.

ZEROSPAM

SC rate: 99.98%
FP rate: 0.03%
Final score: 99.69
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 100.00%
Newsletters FP rate: 3.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

While *ZEROSPAM*'s developers should be proud of their product's impressive 99.98% catch rate, they will be a little disappointed with the false positive rate and the blocked newsletters, which this time prevented the product from achieving a VBSpam+ award. An ordinary VBSpam award, however, is well deserved.

Spamhaus DBL

SC rate: 55.50%
FP rate: 0.00%
Final score: 55.50
Project Honey Pot SC rate: 84.75%
Abusix SC rate: 20.73%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 97.27%
FP rate: 0.00%
Final score: 97.27
Project Honey Pot SC rate: 95.73%
Abusix SC rate: 99.10%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 98.38%
FP rate: 0.00%
Final score: 98.38
Project Honey Pot SC rate: 97.54%
Abusix SC rate: 99.37%
Newsletters FP rate: 0.0%

The results for the two *Spamhaus* blacklists, as well as for the combination thereof in this test are interesting, not just because they are really good, but also because they indicate that the high catch rates of all products in the test may in part be because so much spam was sent from IP addresses and/or contained domains that were used solely by spammers and could thus be blacklisted.

Though not intended to be used on its own, the combined *ZEN+DBL* list in this test performed so well it would have achieved a VBSpam award had it participated as a full solution. That is certainly impressive!

CONCLUSION

With performance as good as it was in this test, the billions of email users will know that their chances of opening a malicious or otherwise unwanted email have been greatly reduced. Of course, we are looking forward to the next test and to seeing whether these high catch rates can be maintained.

The next VBSpam test will run in February and March 2016, with the results scheduled for publication in March. Developers interested in submitting products, or who want to know more about how Virus Bulletin can help your 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.virusbtn.com/