NOVEMBER 2014

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW NOVEMBER 2014

INTRODUCTION

At the risk of repeating myself, 2014 has been an exciting year for *Virus Bulletin*: a few new faces have joined the company while some longer established staff have shuffled roles; we have made our content free for everyone to access; and we have run our most successful and well-attended conference to date.

Of course, we have also tested many anti-malware and anti-spam solutions, bestowing awards upon those who have earned them and providing feedback to all participants so that they can work on improving their products.

In this final VBSpam review of the year – which, for a number of reasons beyond our control, is published more than two weeks late – we look at the performance of 15 full anti-spam solutions and two DNS-based blacklists during a 16-day period in October and November. We also look back at the performance of these products during the past year.

With the publication already running late, we have switched back to a single report on this occasion, but we hope that it provides a good overview of the products' performance, not just in this test but throughout the year.

Although all but one product achieved a VBSpam award in this test, and five of them performed so well they earned a VBSpam+ award, performance on most counts was poorer than it has been in recent tests.

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). Two 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 smaller 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 period started at 12am on Saturday 25 October and ran for 16 consecutive days, ending at 12am on Monday 11 November.

The test corpus consisted of 80,034 emails. 68,542 of these emails were spam, 51,471 of which were provided by *Project Honey Pot*, with the remaining 17,071 emails

ISSN 1749-7027

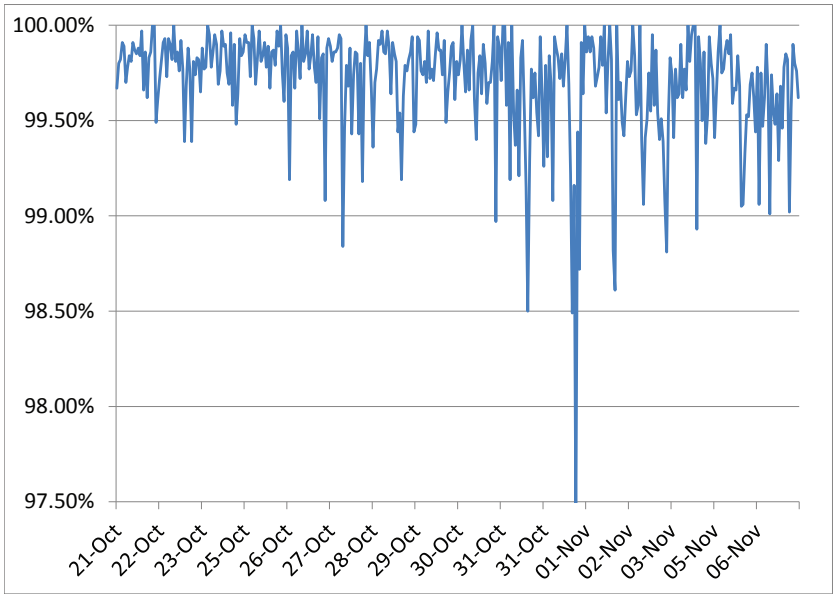


Figure 1: Spam catch rate of all full solutions throughout the test period.

provided by *spamfeed.me*, a product from *Abusix*[1]. They were all relayed in real time, as were the 11,152 legitimate emails ('ham') and 340 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.

This graph shows that the overall performance of products was worse than in the previous test – something which affected most participating products. On several occasions the average hourly catch rate dropped below 99% – and once even well below 97%, when a number of emails spamming hotels were found hard to filter.

These emails weren't the hardest to block in this month's corpus though. That qualification goes to a 419 spam email, followed by an email offering a job and one promoting (supposedly) cheap loans.

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.

[1] The relatively small size of the *Abusix* corpus is due to a technicality on our side.

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 almost 0.3%).

Axway MailGate 5.3.1

SC rate: 99.67%
FP rate: 0.10%
Final score: 99.03
Project Honey Pot SC rate: 99.58%
Abusix SC rate: 99.95%
Newsletters FP rate: 5.0%

Axway's *MailGate* first entered the VBSpam test a year ago. The product from the Phoenix, Arizona-based company had a slightly slow start, which may have been due to some issues adjusting to our test environment, but has since performed steadily, with its performance improving a little in each test.

This month, the product increased its catch rate further to 99.67%. Against that stood an increase in the false positive rates in both the ham and the newsletter corpus. This meant the product's final score was a bit lower than it was in the last test, but *Axway MailGate* still easily achieves its fifth VBSpam award.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.0%

The *Linux*-based product from *Bitdefender* has participated in each of the 34 VBSpam tests we have run so far, and has never failed to achieve a VBSpam award. Moreover, since January 2013, *Bitdefender* has had an unbroken run of VBSpam+ awards. Against that, all concerns are pretty minor, but we have noticed a small drop in the product's catch rate in recent months.

It was therefore nice to see that, in a test in which the performance of most products dropped, *Bitdefender*'s catch rate increased to more than 99.9%. On top of that, the product yet again didn't block a single legitimate email and didn't even block a newsletter, thus making 2014 another golden VBSpam+ year for the Romanian company.

Egedian Mail Security

SC rate: 98.95%
FP rate: 0.25%
Final score: 97.61
Project Honey Pot SC rate: 98.74%
Abusix SC rate: 99.58%
Newsletters FP rate: 2.9%

Egedian Mail Security was first submitted to our VBSpam lab in the spring of this year. The French product, developed by *Profil Technology*, achieved a VBSpam award on its first entry in May, and repeated its success in the next two tests.

Unfortunately, there was no VBSpam award for *Egedian* this time: the product saw a sharp drop in its catch rate – there was a lot of Asian spam among the more than 700 missed spam emails – and also saw its false positive rate increase. This was a shame, of course, and we hope that the product will be back to its usual form in the next test.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.31%
FP rate: 0.00%
Final score: 99.30
Project Honey Pot SC rate: 99.14%
Abusix SC rate: 99.82%
Newsletters FP rate: 0.3%

ESET prides itself on its excellent performance in our VB100 anti-malware tests, so when the company first submitted its *Mail Security* product to the VBSpam tests back in 2012, the bar was already set high. It is thus perhaps little surprise that in each of the 14 tests since then (including this one), *ESET* has easily achieved a VBSpam award, and in six of those tests it has even earned a VBSpam+ award.

In this test, the only false positive for the product was a newsletter that, somewhat frustratingly for those working in anti-spam, addressed the recipient in a generic way. That alone wouldn't have prevented *ESET* from achieving another VBSpam+ award, but unfortunately for its developers, the product's spam catch rate dropped below 99.5%, almost entirely due to spam in east-Asian character sets. They will thus have to be satisfied with another standard VBSpam award on this occasion.

Fortinet FortiMail

SC rate: 99.79%
FP rate: 0.00%
Final score: 99.77
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.6%

Fortinet's *FortiMail* appliance is another product that goes back a long way in our tests, to the second ever VBSpam test back in June 2009. It achieved a VBSpam award on that occasion and has done so in every test since, regularly finding itself among the top performers, while the very same box that was first submitted to us is still humming along nicely in our test lab.

The product's 33rd test was a good one: although the spam catch rate dropped slightly, that was the case for most products this month, and at 99.79% it was still pretty good. More importantly, *FortiMail* didn't miss any email in the ham corpus, and missed just two newsletters. It thus wins its fifth VBSpam+ award.

GFI MailEssentials

SC rate: 99.09%
FP rate: 0.00%
Final score: 99.09
Project Honey Pot SC rate: 98.89%

Product name	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	11141	11	0.10%	223	68319	99.67%	99.03
Bitdefender	11152	0	0.00%	63	68479	99.91%	99.91
Egedian	11124	28	0.25%	722	67820	98.95%	97.61
ESET	11152	0	0.00%	472	68070	99.31%	99.30
FortiMail	11152	0	0.00%	143	68399	99.79%	99.77
GFI	11152	0	0.00%	623	67919	99.09%	99.09
IBM	11152	0	0.00%	201	68341	99.71%	99.70
Kaspersky LMS	11152	0	0.00%	25	68517	99.96%	99.96
Libra Esva	11146	6	0.05%	38	68504	99.94%	99.62
Netmail Secure	11146	6	0.05%	244	68298	99.64%	99.36
OnlyMyEmail	11152	0	0.00%	1	68541	99.999%	99.96
Scrollout	11140	12	0.11%	49	68493	99.93%	98.95
Sophos	11147	5	0.04%	202	68340	99.71%	99.48
SpamTitan	11150	2	0.02%	478	68064	99.30%	99.20
ZEROSPAM	11136	16	0.14%	380	68162	99.45%	98.70
Spamhaus DBL*	11152	0	0.00%	42744	25798	37.64%	37.64
Spamhaus ZEN*	11146	6	0.05%	11210	57332	83.65%	83.38

**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.)*

GFI MailEssentials contd.

Abusix SC rate: 99.68%
Newsletters FP rate: 0.0%

It has been quite a good year for *GFI MailEssentials*: the product performed steadily and has not missed a VBSpam award (in fact, it has not missed one since it started participating in our tests in 2011), and it earned its fourth VBSpam+ award in the last test.

Yet again, the *Windows* solution had no false positives (this time there weren't even any missed newsletters). However, this time the spam catch rate was quite a bit lower than in previous tests – too low to merit another VBSpam+ award. Noting that *GFI* also had issues with spam in east-Asian character sets, we are still able to award the vendor another VBSpam certification.

IBM Lotus Protector for Mail Security

SC rate: 99.71%
FP rate: 0.00%
Final score: 99.70
Project Honey Pot SC rate: 99.61%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%

There is hardly any IT-related subject in which *IBM* isn't involved in some way, and thus it is hardly surprising that the industry giant has its own anti-spam solution. *IBM Lotus Protector for Mail Security* has been included in our tests since September 2011, and 2014 has been a pretty good year for it, easily achieving a VBSpam award in every test.

That good year ends on a high note, as with a good catch rate, no false positives and just a single newsletter misclassified, *IBM* achieves its first VBSpam+ award, thus rewarding the hard work of its developers.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.96

	Newsletters		Project Honey Pot		Abusix		pre-DATA‡		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway	17	5.0%	214	99.58%	9	99.95%			0.64
Bitdefender	0	0.0%	53	99.90%	10	99.94%			0.32
Egedian	10	2.9%	650	98.74%	72	99.58%			1.75
ESET	1	0.3%	441	99.14%	31	99.82%			0.88
FortiMail	2	0.6%	131	99.75%	12	99.93%			0.45
GFI	0	0.0%	569	98.89%	54	99.68%			1.02
IBM	1	0.3%	200	99.61%	1	99.99%			0.53
Kaspersky LMS	0	0.0%	15	99.97%	10	99.94%			0.19
Libra Esva	6	1.8%	34	99.93%	4	99.98%	58073	84.73%	0.23
Netmail Secure	2	0.6%	242	99.53%	2	99.99%	57805	84.34%	0.61
OnlyMyEmail	4	1.2%	1	99.999%	0	100.00%			0.02
Scrollout	50	14.7%	45	99.91%	4	99.98%			0.28
Sophos	0	0.0%	201	99.61%	1	99.99%			0.63
SpamTitan	2	0.6%	467	99.09%	11	99.94%			1.36
ZEROSPAM	4	1.2%	376	99.27%	4	99.98%			1.25
Spamhaus DBL*	0	0.0%	26785	47.96%	15959	6.51%			13.16
Spamhaus ZEN*	0	0.0%	10919	78.79%	291	98.30%			8.16

*Spamhaus is a partial solution and its performance is not to be compared with that of other products.

‡pre-DATA filtering was optional and was applied on the full corpus. All *Libra Esva* and *Netmail Secure FPs* occurred pre-data; other FPs occurred post-DATA.

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

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

Kaspersky Security 8 for Linux Mail Server contd.

Project Honey Pot SC rate: 99.97%

Abusix SC rate: 99.94%

Newsletters FP rate: 0.0%

Kaspersky publishes a lot of research on spam trends – its quarterly reports are a must-read for anyone working in the field – and of course, the company has its own anti-spam solutions. *Kaspersky Security 8 for Linux Mail Server* was first submitted to our tests in the summer of 2012, after a previous *Kaspersky* product had performed well in earlier tests. *Kaspersky LMS* has never failed to achieve a VBSpam award and has already won half a dozen VBSpam+ awards, three of which were earned this year.

This final test of 2014 sees the product win yet another VBSpam+ award. This was one of only two products that didn't see its performance on at least one of the three corpora decrease, and its spam catch rate of 99.96% is certainly impressive. The product's 7th VBSpam+ award thus couldn't be any more greatly deserved.

Libra Esva 3.3.2.0

SC rate: 99.94%

FP rate: 0.05%

Final score: 99.62

Project Honey Pot SC rate: 99.93%

Abusix SC rate: 99.98%

Pre-DATA SC rate: 84.73%

Newsletters FP rate: 1.8%

At a security fair I attended earlier this year, *Libra Esva* displayed a poster in its booth showing its past performance in VBSpam tests and showing that the virtual product always finishes among the top few as measured by final

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	√				√		√	√
ESET	ESET Threatsense					√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Netmail Secure	Proprietary	√	√	√		√		√	
Profil	Bitdefender	√				√		√	√
Scrollout	ClamAV			√		√		√	
Sophos	Sophos							√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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

score. Indeed, *Libra Esva*, which first joined the test in May 2010, has not missed a single VBSpam award since it joined, and has enjoyed an unbroken run of VBSpam+ awards since July last year.

Unfortunately, that run was broken this month thanks to six false positives, four of which were sent by the same sender and all of which had found themselves on various blacklists. It may well be that the senders are partly to blame here, but ultimately the filtering decision is made by the product. Fingers crossed this will be a one-off glitch and, noting that *Libra Esva*'s spam catch rate of 99.94% remains impressive, we can at least send the product's developers another VBSpam award.

Netmail Secure

SC rate: 99.64%
FP rate: 0.05%
Final score: 99.36
Project Honey Pot SC rate: 99.53%
Abusix SC rate: 99.99%
Pre-DATA SC rate: 84.34%
Newsletters FP rate: 0.6%

Netmail Secure topped the rankings in the very first VBSpam test back in May 2009, albeit under a different name, and has been a regular participant in recent years, achieving a VBSpam+ award roughly every second test.

Unfortunately, there was no VBSpam+ award for *Netmail* in this test as it too had issues with six legitimate emails whose senders had ended up on blacklists. Other than that, performance remained good and yet another VBSpam award was never in question.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%

Products ranked by final score (full solutions only)	
Kaspersky LMS	99.96
OnlyMyEmail	99.96
Bitdefender	99.91
FortiMail	99.77
IBM	99.70
Libra Esva	99.62
Sophos	99.48
Netmail Secure	99.36
ESET	99.30
SpamTitan	99.20
GFI	99.09
Axway	99.03
Scrollout	98.95
ZEROSPAM	98.70
Egedian	97.61

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

OnlyMyEmail's Corporate MX-Defender contd.

Final score: 99.96
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 1.2%

VBSpam test histories don't get any more impressive than that of *OnlyMyEmail*. The Michigan-based hosted solution has been included in our tests for four years and has never missed more than 0.02% of spam. This year, things were even more impressive as the product didn't miss any legitimate email and very few newsletters, and the product achieved a VBSpam+ award in each of the last five tests.

This month, we are pleased to be able to increase that run of VBSpam+ awards to six in a row – the product missed just a single spam email out of more than 68,000, it didn't block any of the more than 11,000 legitimate emails, and it only blocked four newsletters. It won't be easy for *OnlyMyEmail* to repeat in 2015 what it achieved in 2014, but with this product one never knows.

Scrollout F1

SC rate: 99.93%
FP rate: 0.11%
Final score: 98.95
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.98%
Newsletters FP rate: 14.7%

Virus Bulletin in general, and the VBSpam tests in particular, make a lot of use of open-source products and thus we were rather pleased when almost two years ago, we were contacted by the developers of *Scrollout F1* who were interested in submitting their product.

Although a free product like *Scrollout* might require more adjustments from a systems administrator than a paid-for product, it has performed reasonably well (even straight out of the box) in nearly two years' worth of testing, picking up several VBSpam awards along the way.

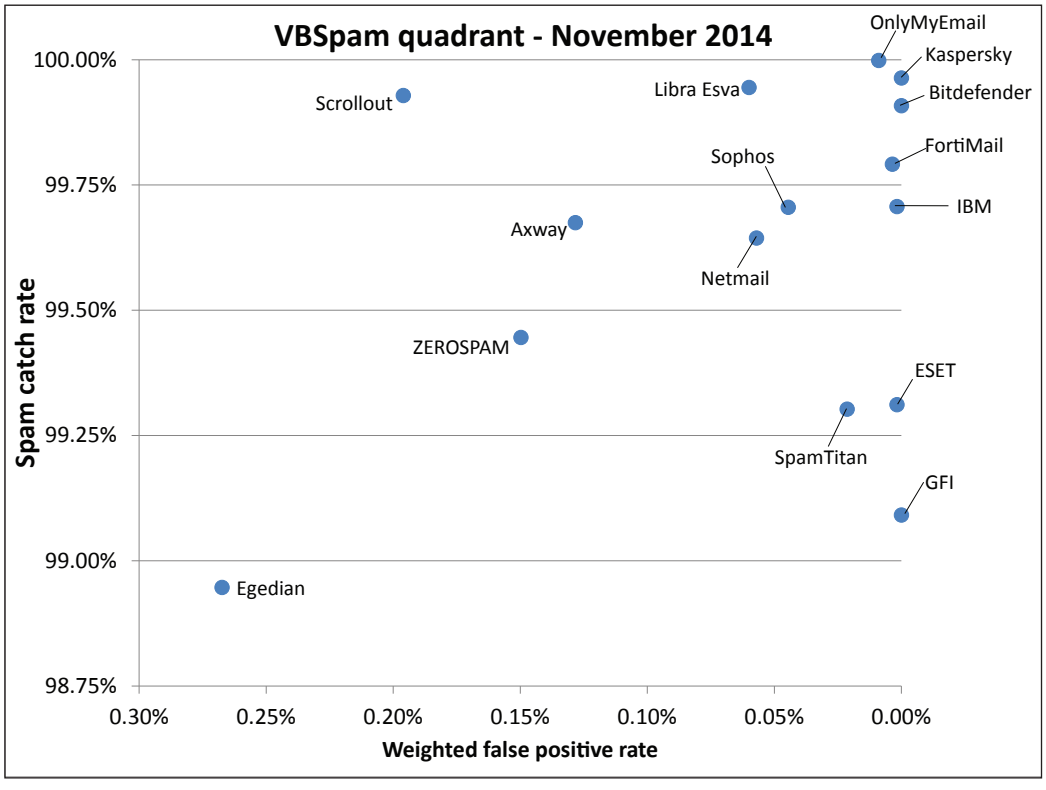
The last test was the first time this year that *Scrollout* failed to achieve a VBSpam award, so we were pleased to see that its performance had improved significantly in this test. The spam catch rate of 99.93% was particularly good to see. Of course, that is only half of the story and *Scrollout* did block more legitimate emails than all but two other products. Still, that wasn't enough to deny the virtual appliance another VBSpam award.

Sophos Email Appliance

SC rate: 99.71%
FP rate: 0.04%
Final score: 99.48
Project Honey Pot SC rate: 99.61%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%

Sophos's *Email Appliance* started 2014 on a high note with a VBSpam+ award, and while its performance has been pretty good since then, there have always been a few false positives standing in the way of it earning another such award.

Unfortunately, this test was no different as *Sophos* missed five legitimate emails – four of which were from the same Malawi-based sender. Note that the appliance didn't block any newsletters, which is not surprising as *Sophos* has historically had little problem with this difficult feed. While the developers may be disappointed to have missed out on another VBSpam+ award, their 28th VBSpam award in as many tests is still something to be proud of.



(Please refer to text for full product names.)

SpamTitan 6.00

SC rate: 99.30%
FP rate: 0.02%
Final score: 99.20
Project Honey Pot SC rate: 99.09%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.6%

SpamTitan is another product whose VBSpam participation goes back to 2009, the very first year we ran these tests, and which has not missed a single test since, earning a VBSpam award on each occasion. 2014 has been a fairly good year for the product, with one VBSpam+ award and very few false positives.

In the final test of the year, *SpamTitan* blocked just two legitimate emails – both from the same sender in Africa – but it was also one of several products that saw quite a drop in its spam catch rate. Interestingly, almost all of the missed spam was written in English and, rather worryingly, there were quite a few phishing emails among them.

Of course, a catch rate of 99.3% is still pretty good, and the product's 31st VBSpam award is on its way to its developers on the west coast of Ireland.

ZEROSPAM

SC rate: 99.45%
FP rate: 0.14%
Final score: 98.70
Project Honey Pot SC rate: 99.27%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.2%

ZEROSPAM, a hosted solution which first joined the tests in 2012, has had a good year, never failing to win a VBSpam award and picking up VBSpam+ awards in January and July.

This was one of several products for which the last test of the year proved to be the worst, with its catch rate falling and its false positive rate increasing to the second highest this month – the product blocked more legitimate emails in this test than it has done in the previous five tests together. The final score of 98.70 is still well above the VBSpam threshold though, and thus the product adds another

VBSpam award to its tally, but we're looking forward to the next test to see if *ZEROSPAM* can show that this was a one-time glitch.

Spamhaus DBL

SC rate: 37.64%
FP rate: 0.00%
Final score: 37.64
Project Honey Pot SC rate: 47.96%
Abusix SC rate: 6.51%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 83.65%
FP rate: 0.05%
Final score: 83.38
Project Honey Pot SC rate: 78.79%
Abusix SC rate: 98.30%
Newsletters FP rate: 0.0%

Most spam filters make use of IP- and/or domain-based blacklists, and we are pleased to have been testing one of the best known among them in our VBSpam tests for many years. *Spamhaus ZEN* combines several IP-based blacklists, while *DBL* (Domain Block List) is a self-describing acronym. Because these lists are designed to be used by spam filters, rather than on their own, their performance is not to be compared with that of the other participants, and though clearly falling well short of the VBSpam threshold, the products did not 'fail' the test.

We have been testing *ZEN* and *DBL* separately since May this year and, interestingly, the performance of the former is now lower than it has been since then, while on this occasion the *DBL* performed better than it has done before – though in both cases this may partially be explained by the relative sizes of the two spam feeds in this test.

While both lists continue to show their value, the six false positives the *ZEN* IP-blacklist gave us this time – the same six that were blocked by several other products – were a bit of a concern, as previous tests have always shown that *Spamhaus* tends to err on the side of caution.

CONCLUSION

This test, in which many products saw their performance drop, finished an otherwise good year for spam filters.

If there's one thing we've learned over all our years of running anti-spam tests it's that spam is very volatile: this month's drop in performance may be part of a larger trend, and it may also be a one-off thing. We hope it's the latter, but we will report on it either way.

Stay tuned for another year's worth of anti-spam testing. See you all in 2015!

The next VBSpam test will run in December 2014 and January 2015, with the results scheduled for publication in January. Developers interested in submitting their products should email martijn.grooten@virusbtn.com.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Consultant Technical Editors: Dr Morton Swimmer, Ian Whalley

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