JANUARY 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW JANUARY 2015 – SUMMARY

INTRODUCTION

In this short version of the January 2015 VBSpam report, we provide a summary of the results of the 35th VBSpam test as well as some information on 'the state of spam'. The main point of note from the test results is that most products performed very well and showed an improvement compared with the last (November 2014) test – but there were a few exceptions.

THE VBSPAM TESTS

The VBSpam tests started in May 2009 and have been running every two months since then. They use a number of live email streams (the spam feeds are provided by *Project Honey Pot* and *Abusix*) which are sent to participating solutions in parallel to measure their ability to block spam and to correctly identify various kinds of legitimate emails. Products that combine a high spam catch rate with a low false positive rate (the percentage of legitimate emails that are blocked) achieve a VBSpam award, while those that do this exceptionally well earn a VBSpam+ award.

vb VERIFIED SPAM virusbtn.com

vb VERIFIED SPAM + virusbtn.com

This month's VBSpam test saw 16 full anti-spam solutions and a number of DNS-based blacklists on the test bench. Filtering more than 140,000 emails over an 18-day period, all but three full solutions performed well enough to achieve a VBSpam award[1] – and six of them achieved a VBSpam+ award. These results demonstrate once again that, while spam remains a problem that cannot be ignored, there are many solutions that do a very good job of mitigating it.

THE RESULTS

Many products ended 2014 on a low note, with a relatively poor performance in the November 2014 test[2] – although in all but one case, that performance was still sufficient to achieve a VBSpam award.

In the first test of 2015, most products bounced back. No fewer than eight solutions blocked more than 99.90% of spam, while nine full solutions didn't block any of the more than 8,500 legitimate emails.

There were exceptions though, and two products failed to achieve a VBSpam award, while for a number of products the newsletter feed turned out to be surprisingly difficult to filter; a high false positive rate on this feed prevented three products from achieving a VBSpam+ award.

In the end, six full solutions – *ESET*, *GFI*¸ *Kaspersky*, *Libra Esva*, *OnlyMyEmail* and *ZEROSPAM* – achieved VBSpam+ awards for blocking more than 99.5% of spam, while blocking no legitimate emails and very few newsletters.

OnlyMyEmail once again achieved the highest spam catch rate (the hosted solution missed just two spam emails out of more than 131,000), closely followed by *Libra Esva*, while *Kaspersky*'s *Linux Mail Security* product was the third that kept a 'clean sheet', with no false positives in either the ham corpus or the newsletters.

[1] Given that DNS blacklists are supposed to be included in an anti-spam solution rather than run on their own, it is not reasonable to expect such products to meet our strict thresholds. Thus, while the DNS blacklist solutions included in the test did not achieve a VBSpam award, they certainly didn't 'fail' the test.

[2] https://www.virusbtn.com/virusbulletin/archive/2014/11/vb201411-vbspam-comparative.

ISSN 1749-7027

NEWSLETTERS

Since May 2011, we have included a feed of 'newsletters' in the test corpus; since March last year, the newsletter false positive rate has counted towards VBSpam certification.

This feed includes any kind of legitimate bulk email, ranging from emails from a shop advertising its current offers to updates on a charity's campaigns. Senders vary from small local organizations to large multinationals. What the emails have in common is that they were all explicitly subscribed to.

In some cases, the subscription was also explicitly confirmed. We think this is a good idea – and have shown in the past that confirmed opt-in subscriptions are half as likely to be blocked as those that do not follow this practice[3]. We have also shown that the use of DKIM has a small positive effect on email delivery rates[4].

In this test, the products' performance on the feed of newsletters was poorer than it has been in previous tests. Interestingly, this didn't seem to be the fault of the newsletters: no newsletter was blocked by more than three products, and even among those that were blocked, there were none for which, at first glance, it seemed understandable – no pharmaceutical mailings or emails from banks.

But then, most spam filtering takes place under the hood. Incorrect blocking may be due to the way the email is constructed, which might be unusual or even share methods with those of spammers. It is also possible that an email service provider hired to send an organization's email hasn't succeeded in keeping spammers off its services, resulting in its legitimate emails being blocked as well.

Correctly classifying newsletters is probably the most difficult part of maintaining a spam filter. It is also an area in which it is understandable when the wrong choices are made. Indeed, aside from the incorrectly blocked newsletters, there are always a number of spam emails that look very much like legitimate newsletters – and perhaps to some recipients, they are.

Many recipients won't mind too much if the odd newsletter is sent to the spam folder – and for that reason we don't punish participating products too harshly if they have blocked the odd one. But there will be other recipients who do mind – and for that reason we will continue to look at how well products classify them.

TABLES AND GRAPHS

Note that in the table on page 3, products are ranked by their 'final score'. This score combines the spam catch rate, false positive rate and newsletter false positive rate in a single metric. However, readers are encouraged to consult the in-depth report for the full details and, if deemed appropriate, use their own formulas to compare products.

In the VBSpam quadrant, the products' spam catch rates are set against their 'weighted false positive rates', the latter being a combination of the two false positive rates, with extra weight on the ham feed. An ideal product would be placed in the top right corner of the quadrant.

The next VBSpam test will run in February 2015, with the results scheduled for publication in March. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

[3] https://www.virusbtn.com/blog/2011/09_19.xml.

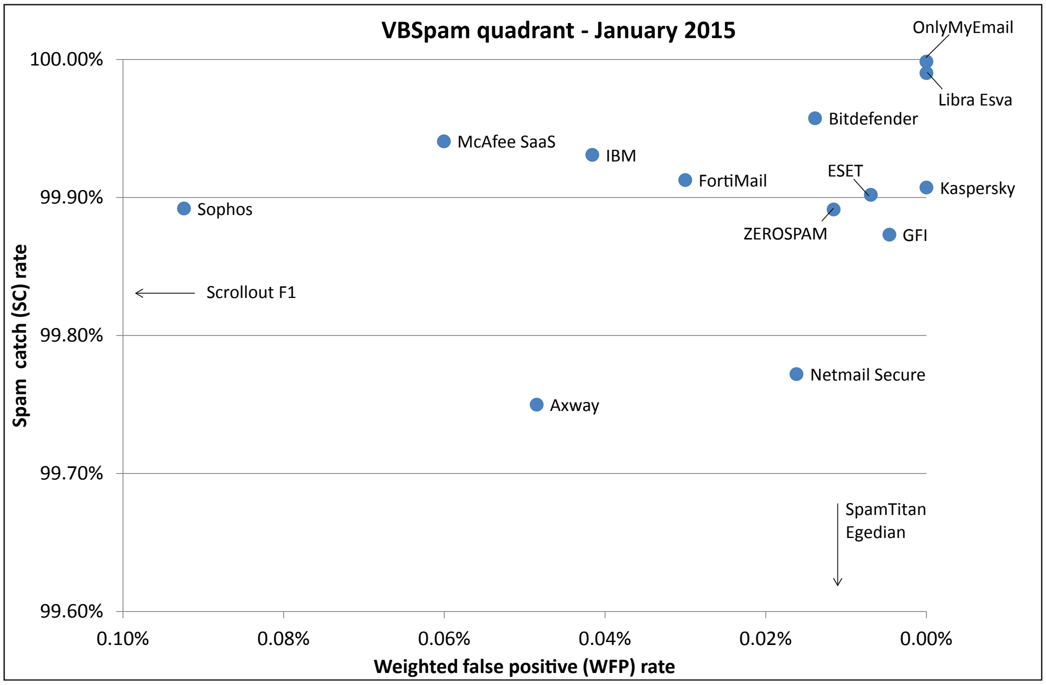
[4] https://www.virusbtn.com/virusbulletin/archive/2011/07/vb201107-vbspam-comparative.

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

© 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/

Product name	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
OnlyMyEmail	8603	0	0.00%	2	131553	99.998%	99.998
Libra Esva	8603	0	0.00%	13	131542	99.99%	99.99
Kaspersky LMS	8603	0	0.00%	122	131433	99.91%	99.91
Bitdefender	8602	1	0.01%	56	131499	99.96%	99.89
ESET	8603	0	0.00%	129	131426	99.90%	99.87
GFI	8603	0	0.00%	167	131388	99.87%	99.85
ZEROSPAM	8603	0	0.00%	143	131412	99.89%	99.83
FortiMail	8603	0	0.00%	115	131440	99.91%	99.76
IBM	8600	3	0.03%	91	131464	99.93%	99.72
Netmail Secure	8603	0	0.00%	300	131255	99.77%	99.69
McAfee SaaS	8600	3	0.03%	78	131477	99.94%	99.64
Axway	8603	0	0.00%	329	131226	99.75%	99.51
Sophos	8595	8	0.09%	142	131413	99.89%	99.43
Scrollout	8576	27	0.31%	455	131100	99.65%	97.46
SpamTitan	8601	2	0.02%	4192	127363	96.81%	96.65
Egedian	8599	4	0.05%	4334	127221	96.71%	96.46
Spamhaus ZEN+DBL*	8598	5	0.06%	4623	126932	96.49%	96.20
Spamhaus ZEN*	8603	0	0.00%	10693	120862	91.87%	91.87
Spamhaus DBL*	8598	5	0.06%	80521	51034	38.79%	38.50

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



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