JULY 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW JULY 2015 – SUMMARY

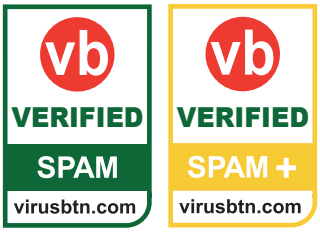
INTRODUCTION

In this short version of the July 2015 VBSpam report (published in August), we provide a summary of the results of the 38th VBSpam test as well as some information on 'the state of spam'. The main point of note from the test results is that, at an average of 99.87%, spam catch rates were not only very high in absolute terms (as they have always been in recent years) but also significantly higher than in the last (May 2015) test.

Note: Later this month, a full report will be published covering the same set of results, but with details of each product's individual performance and with full results tables.

THE VBSPAM TESTS

The VBSpam tests started in May 2009 and have been running every two months since. 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 the products' 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.



This month's VBSpam test saw 15 anti-spam solutions and three DNS blacklists on the test bench. Filtering more than 165,000 emails over a 16-day period (23 June to 8 July 2015), all but one full solution performed well enough to achieve a VBSpam award, and five of them achieved a VBSpam+ award. These results demonstrate that, while spam remains a problem that cannot be ignored, there are many solutions that do a very good job of mitigating it.

Note: 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. These DNS blacklists are not included in the averages mentioned in this report summary.

THE RESULTS

In July, security firm *Symantec* reported that, for the first time in 12 years, less than half of all email traffic was spam[1]. While this is a clear sign that we aren't losing the fight against spam, the consequences for spam filters are mixed. While on the one hand they are less likely to be deluged by spam, and can thus use more resources to determine the status of each individual email, on the other hand as the size of spam campaigns decreases, spam becomes more difficult to spot and more likely to stay under the radar.

In this test, we noticed little of the latter affect. Spam catch rates, which dropped significantly in the May 2015 test, more than bounced back and at an average of 99.87% were impressively high. Every product we tested missed fewer than one in 200 spam emails.

The picture was more varied when it came to false positives, with some products performing a little better than in the last test, and others performing less well. Overall, though, it is

[1] http://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015.en-us.pdf

ISSN 1749-7027

clear that the increase in the spam catch rates wasn't a result of products using stricter settings, which would have caused more false positives.

The picture among newsletters – various kinds of legitimate bulk emails that were subscribed to explicitly – was the same: a mixed bag, but there was certainly no overall decline in performance.

The 15 spam filters use different techniques and sources to determine which emails are spam, hence it is not surprising to find quite a lot of variation in the emails they missed. There were only six emails (SEO spam, job spam, religious spam and a test message) that were missed by at least half of the 15 participating full solutions, and each spam email was blocked by at least six products.

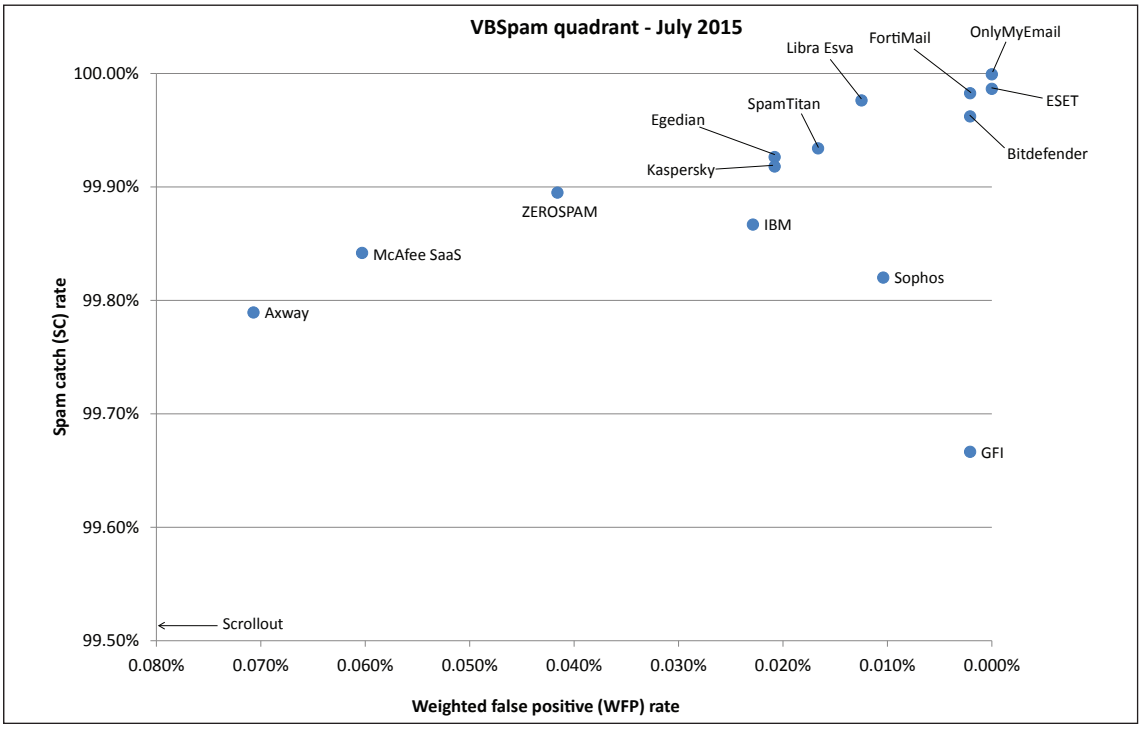
A whopping 98.4% of spam was blocked by all solutions, showing that spam filters not only do a good job of keeping users' inboxes clean, they also do serious damage to spam as a whole.

WINNERS

With spam catch rates as high as they were in this test, and false positive rates yet again fairly low, the big winners are the end-users and systems administrators. Many security experts don't like the idea of 'just putting a box in front of it'. When it comes to spam, a box – whether it's a physical box, a virtual box, or one based in the cloud – makes a huge difference.

Product name	False positives	FP rate	False negatives	SC rate	Newsletter false positives	Newsletter FP rate	Final score
OnlyMyEmail's Corporate MX-Defender	0	0.00%	1	99.999%	0	0.00%	99.999
ESET Mail Security for Microsoft Exchange Server	0	0.00%	21	99.99%	0	0.00%	99.99
Fortinet FortiMail	0	0.00%	27	99.98%	1	0.31%	99.97
Bitdefender Security for Mail Servers 3.1.2	0	0.00%	59	99.96%	1	0.31%	99.95
Libra Esva 3.4.1.0	1	0.01%	37	99.98%	1	0.31%	99.91
SpamTitan 6.00	1	0.01%	103	99.93%	3	0.92%	99.85
Egedian Mail Security	1	0.01%	115	99.93%	5	1.53%	99.82
Kaspersky Security 8 for Linux Mail Server	2	0.02%	128	99.92%	0	0.00%	99.81
Sophos Email Appliance	1	0.01%	281	99.82%	0	0.00%	99.77
IBM Lotus Protector for Mail Security	2	0.02%	208	99.87%	1	0.31%	99.75
ZEROSPAM	3	0.03%	164	99.90%	5	1.53%	99.69
GFI MailEssentials	0	0.00%	521	99.67%	1	0.31%	99.66
McAfee SaaS Email Protection	5	0.05%	247	99.84%	4	1.22%	99.54
Axway MailGate 5.3.1	5	0.05%	329	99.79%	9	2.75%	99.44
Scrollout F1	228	2.39%	777	99.50%	167	51.07%	86.97
Spamhaus DBL*	4	0.04%	108059	30.84%	0	0.00%	30.63
Spamhaus ZEN*	0	0.00%	11393	92.71%	0	0.00%	92.71
Spamhaus ZEN+DBL*	4	0.04%	7147	95.43%	0	0.00%	95.22

**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.)

Of the 15 participating solutions, 14 easily earned a VBSpam award. The highest spam catch rates were achieved by *OnlyMyEmail* (which missed only one spam email), *ESET* and *FortiMail*, each of which blocked more than 99.98% of spam.

These three products also didn't block a single email in the feed of more than 9,500 legitimate emails, and blocked very few newsletters, thus earning them a VBSpam+ award. *Bitdefender* and *GFI* joined them in achieving a VBSpam+ award.

TABLES AND GRAPHS

Note that in the table opposite, 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 (to be published later this month) for the full details and, if deemed appropriate, use their own formulas to compare products.

The spam corpus contained 156,250 emails; the ham corpus contained 9,552 emails; and the newsletter corpus contained 327 emails.

In the VBSpam quadrant above, 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 August 2015 and will start in the middle of the month. The full results are scheduled for publication in September. Developers interested in submitting products for VBSpam testing 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

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: http://www.virusbtn.com/