

virus

BULLETIN

EXCERPT FROM VBSPAM COMPARATIVE REVIEW, MARCH 2010: SPAMHAUS ZEN PLUS DBL

Building a spam filter is not rocket science. However, building a *good* spam filter is not a trivial task. And, with the email security market still growing and new products appearing every month, many customers will wonder whether a hitherto unknown product, with a shiny website and an impressive sales story, is actually any good.

The purpose of VBSpam testing is to provide an easy-to-recognize certification that tells potential customers that a product does what a good spam filter should do: i.e. block the vast majority of spam, with very few false positives. As such, we are delighted that all of the products in this month's test achieved a VBSpam award. This does not mean that no bad products exist – after all we only test products that have been submitted by their developers – but it does demonstrate that there is plenty of choice for customers, as well as a healthy amount of competition for product developers.

But in spam filtering, the devil is in the details. With recent reports suggesting that up to 95% of email traffic is spam, email can only be a viable form of communication for businesses if the vast majority of that spam is blocked – and blocking one or two per cent more will have a huge impact on users' inboxes. Similarly, a very low false positive rate is essential, and even a couple fewer false positives every month will significantly improve user experience. For this reason we provide detailed performance measurements for all of the products tested.

THE TEST SET-UP

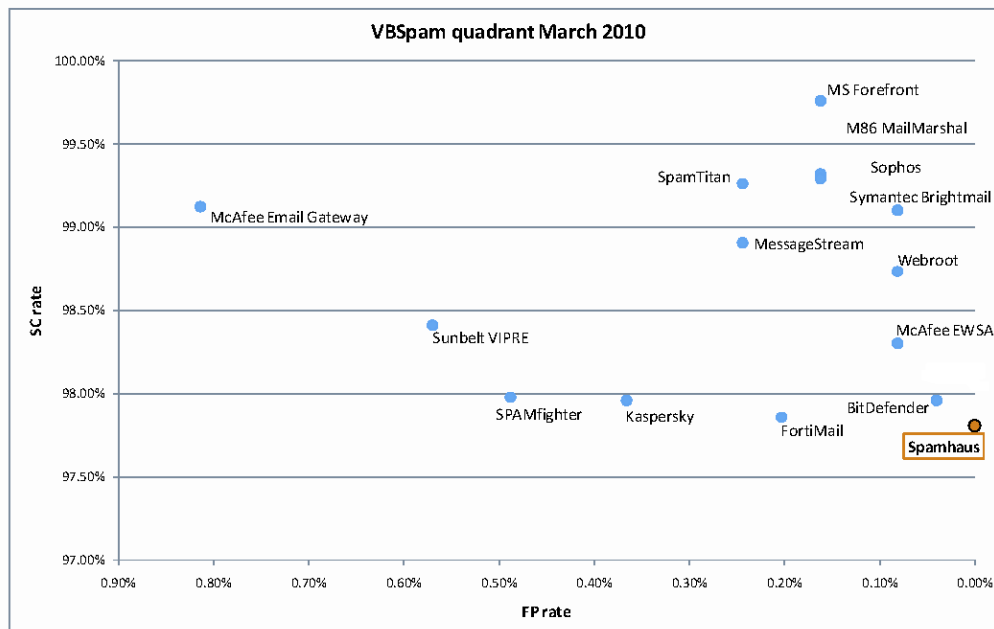
The full test methodology can be found online at <http://www.virusbtn.com/vbspam/methodology/>.

The products that needed to be installed on a server

were installed on a *Dell PowerEdge R200*, with a 3.0GHz dual core processor and 4GB of RAM. The *Linux* products ran on *SuSE Linux Enterprise Server 11*; the *Windows Server* products ran on either the 2003 or the 2008 version, depending on which was recommended by the vendor.

To compare the products, we calculate a 'final score', defined as the spam catch (SC) rate minus three times the false positive (FP) rate. Products earn VBSpam certification if this value is at least 96%:

$$SC - (3 \times FP) \geq 96\%$$



	True negative	False positive	FP rate	False negative	True positive	SC rate	Final score
BitDefender	2457	1	0.04%	5144	246805	97.96%	97.84%
FortiMail	2453	5	0.20%	5401	246548	97.86%	97.26%
Kaspersky	2449	9	0.37%	5148	246801	97.96%	96.85%
M86 MailMarshal	2454	4	0.16%	1717	250232	99.32%	98.84%
McAfee Email Gateway	2438	20	0.81%	2208	249741	99.12%	96.69%
McAfee EWSA	2456	2	0.08%	4281	247668	98.30%	98.06%
MessageStream	2452	6	0.24%	2762	249187	98.90%	98.18%
MS Forefront	2454	4	0.16%	602	251347	99.76%	99.28%
MXTools	2458	0	0.00%	4922	247027	98.05%	98.05%
Sophos	2454	4	0.16%	1787	250162	99.29%	98.81%
SPAMfighter	2446	12	0.49%	5099	246850	97.98%	96.51%
SpamTitan	2452	6	0.24%	1858	250091	99.26%	98.54%
Sunbelt VIPRE	2444	14	0.57%	4004	247945	98.41%	96.70%
Symantec Brightmail	2456	2	0.08%	2263	249686	99.10%	98.86%
Webroot	2456	2	0.08%	3192	248757	98.73%	98.49%
Spamhaus	2458	0	0.00%	5529	246420	97.81%	97.81%

THE EMAIL CORPUS

The corpus contained 254,407 emails: 2,458 ham messages and 251,949 spam messages, where the latter consisted of 237,783 messages provided by Project Honey Pot and 14,166 messages sent to legitimate @virusbtn.com addresses.

Some new email discussion lists were added to the ham set and emails that claimed to be sent from @virusbtn.com addresses were removed from the test set. (This check was only applied on the MAIL FROM, not on the email headers.)

For each product, no more than four false positives were counted per sender. The 'image spam' and 'large spam' categories referenced in the test results are, respectively, spam messages containing at least one inline image, and those with a body size of over 50,000 bytes.

Spamhaus ZEN plus DBL

SC rate (total): 97.81%

SC rate (Project Honey Pot corpus): 98.52%

SC rate (VB spam corpus): 85.89%

SC rate (image spam): 96.72%

SC rate (large spam): 92.91%

FP rate: 0.00%

Final score: 97.81%

As in the previous test, the IP address of every incoming email was checked against the *Spamhaus ZEN* DNS blacklist, while domain checks were performed against the new *Spamhaus DBL* blacklist.

Once again, this resulted in a very good spam catch rate and again there were no false positives. While it is probably not a good idea to use a DNS blacklist as a standalone spam filter, with *Spamhaus* one can at least be sure that the vast majority of spam is blocked at an early stage.



MX Tools
422 Richards Street, 3rd Floor
Vancouver, BC V6B 2Z3, Canada
Email: support@mxtools.com
Web: www.mxtools.com
Tel +1 778 330 1074 x237

