



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

The first VBSpam comparative review of the new decade saw 15 products on the test bench: 14 full anti-spam products and one partial solution.

THE TEST SET-UP

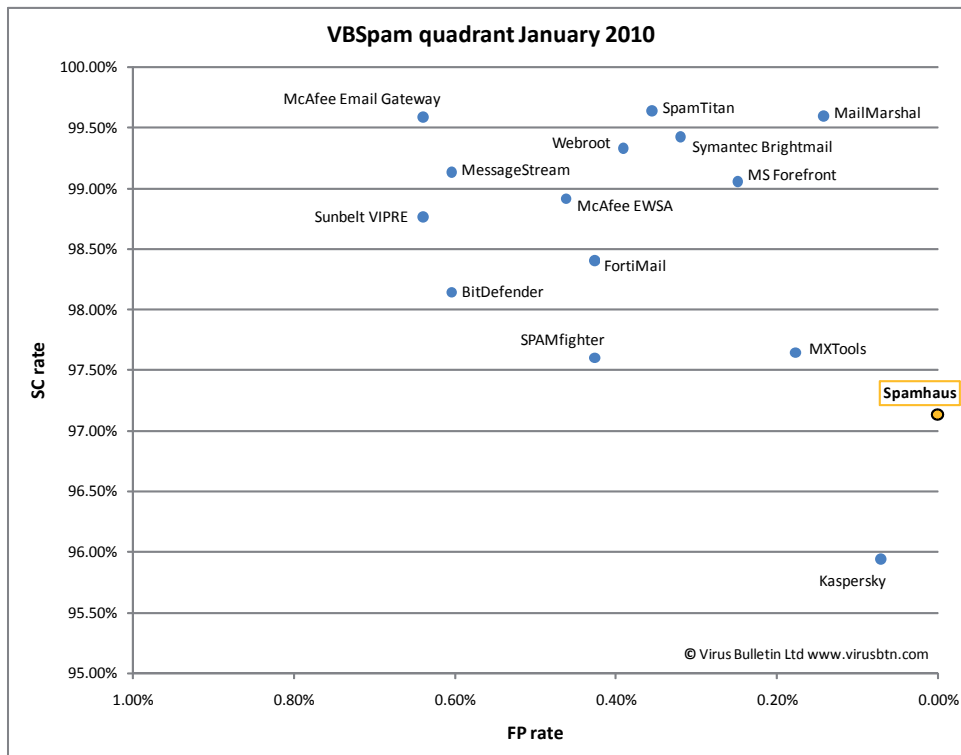
The full test methodology can be found at <http://www.virusbtn.com/vbspam/methodology/>.

A product's performance is measured based on the value of its spam catch (SC) rate minus three times its false positive (FP) rate. A product earns a VBSpam award if this value (referred to as the 'final score') is at least 96%:

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

This does not mean we believe there is no difference in performance between the various products, and end-users are encouraged to compare the performance figures shown in the tables and to look at the relative positions of the products plotted in the VBSpam results graph.

Our intention is not to give an absolute value to the performance measured by us: a 98% catch rate in our test does not necessarily indicate the same as a 98% catch rate in another test, and does not mean that the product will catch 98% of a customer's spam. However, the catch rates (or false positive rates) of two products in our test can be compared against each other.



The test ran from 1pm GMT on 14 December 2009 until 8am GMT on 4 January 2010 – a test period of almost three weeks, which included most of the Christmas holiday period (notorious for breaking spam records). The corpus contained 249,569 emails: 2,811 ham messages and 246,758 spam messages, where the latter consisted of 224,411 messages provided by Project Honey Pot and 22,347 messages sent to legitimate @virusbtn.com addresses.

The ham consisted of all legitimate messages sent to @virusbtn.com addresses, but with the senders of emails that regularly discuss spam- and malware-related topics (for example anti-spam discussion lists) excluded. To make up for



these exclusions, we added to the corpus a number of email discussion lists on a variety of other topics.

In an attempt to make the test results more realistic, no more than four false positives were counted per sender for each product. This should prevent a small mistake on a blacklist from having escalating effects if a certain sender sends many emails during a test period, but more importantly, it reflects a real situation where legitimate senders whose emails keep being blocked are eventually whitelisted.

Emails that claimed to have been sent from @virusbtn.com addresses were removed from the corpus: given the way our test is set up, products could have valid reasons for considering these emails to have been sent from a legitimate VB server.

RESULTS

In this test we make a distinction between full solutions and partial solutions. The latter are anti-spam products that are unlikely to be deployed on their own but are intended to work together with other solutions. As such, the performance of these products should not be compared directly to other solutions. This test contained one such solution (*Spamhaus Zen*).

Spamhaus ZEN plus DBL

SC rate (total): 97.14%

SC rate (Project Honey Pot corpus): 98.50%

SC rate (VB spam corpus): 83.47%

SC rate (image spam): 98.20%

SC rate (large spam): 94.64%

FP rate: 0.00%

Final score: 97.14%

Spamhaus (officially known as *The Spamhaus Project*) has been active for well over a decade and provides several DNS blacklists – databases of IP addresses known to be used by spammers. *Spamhaus ZEN* combines all three of the DNSBLs the

	True negative	False positive	FP rate	Total spam			Final score*
				False negative	True positive	SC rate	
BitDefender	2794	17	0.605%	4581	242177	98.14%	96.33%
Fortinet FortiMail	2796	12	0.427%	3937	242821	98.40%	97.12%
Kaspersky	2809	2	0.071%	10026	236732	95.94%	95.73%
M86 MailMarshal	2807	4	0.142%	987	245771	99.60%	99.17%
McAfee Email Gateway	2789	18	0.640%	1001	245757	99.59%	97.67%
McAfee EWSA	2795	13	0.462%	2667	244091	98.92%	97.53%
MessageStream	2782	17	0.605%	2130	244628	99.14%	97.33%
MS Forefront	2804	7	0.249%	2318	244440	99.06%	98.31%
MXTools	2804	5	0.178%	5803	240955	97.65%	97.12%
SPAMfighter	2797	12	0.427%	5920	240838	97.60%	96.32%
SpamTitan	2801	10	0.356%	873	245885	99.65%	98.58%
Sunbelt VIPRE	2793	18	0.640%	3043	243715	98.77%	96.85%
Symantec Brightmail	2798	9	0.320%	1404	245354	99.43%	98.47%
Webroot	2796	11	0.391%	1639	245119	99.34%	98.17%
Spamhaus	2811	0	0.000%	7064	239694	97.14%	97.14%

* Results listed alphabetically by product name.

organization provides and in this test, we combined it with *Spamhaus DBL*, which uses various heuristics to identify domains used by spammers. This DBL was checked for the domain part of every URL that appeared in the body of the emails – using the same method as used for *SURBL* and *Server Authority* – and also for the EHLO/HELO domain and the reverse DNS of the sending IP address.

Spamhaus has a rather conservative approach when it comes to adding IP addresses and domains to blacklists in order to minimize the number of false positives and, indeed, we did not see any false positives in this test. At the same time, the solution caught over 97% of the spam in this test, giving it a very good final score.

Still, the low catch rate for the *VB* spam corpus suggests that using *Spamhaus* on its own would lead to a fairly large number of spam messages reaching users' inboxes. This is why this is only a partial solution, the performance of which should not directly be compared to that of full solutions. Still, even as a partial solution, it easily earns a VBSpam award.



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