

COMPARATIVE REVIEW

VBSPAM COMPARATIVE REVIEW MARCH 2011

Martijn Grooten

Those who are familiar with our VB100 tests, where the criteria to pass the test are to have a 100% catch rate combined with zero false positives, may wonder why we don't have similar criteria for the VBSpam tests. The reason goes deeper than the simple fact that no product has ever achieved this.

All of the tens of thousands of spam messages sent as part of this test were originally sent to fictional addresses that have never belonged to a real person or organization (spam traps). Messages sent to these addresses are, by definition, unwanted: there is no one to have wanted them in the first place.

However, that does not mean that a handful of messages in the spam corpus may not appear rather legitimate: for instance, this month's spam corpus contained a genuine invite to join *Facebook*, and a newsletter that looks as if it will be of genuine interest to some recipients.

So while the *right* thing to do with these messages would be to block them (as, ultimately, a spam filter should block what is unwanted), this may not be the *best* thing to do. Blocking *Facebook* invitations – the vast majority of which are legitimate and wanted – will likely lead to false positives. Blocking a newsletter, even if its sender did not adhere to best practices, may also lead to complaints from end-users.

We have always believed that avoiding false positives is more important than blocking as much spam as possible,

and it is good to see there were no false positives for any of the products with the top seven final scores.

Still, we acknowledge that false positives may occur from time to time, and sometimes for a good reason. Some of the legitimate emails that were missed during this test contained URLs on domains frequently used by spammers. And while the best thing to do with such messages would be to allow them through to the user's inbox, marking them as spam is certainly understandable. As long as it does not occur frequently, this should not prevent a product from winning a VBSpam award.

In this test 18 out of 19 full solutions (hailing from 13 different countries – a nice record showing the global nature of the fight against spam) achieved VBSpam certification, eight of which had no false positives.

THE TEST SET-UP

The VBSpam test methodology can be found at <http://www.virusbtn.com/vbspam/methodology/>. As usual, email was sent to the products in parallel and in real time, and products were given the option to block email pre-DATA. Four products chose to make use of this option.

As in previous tests, 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', which is defined as the spam catch (SC) rate minus five times

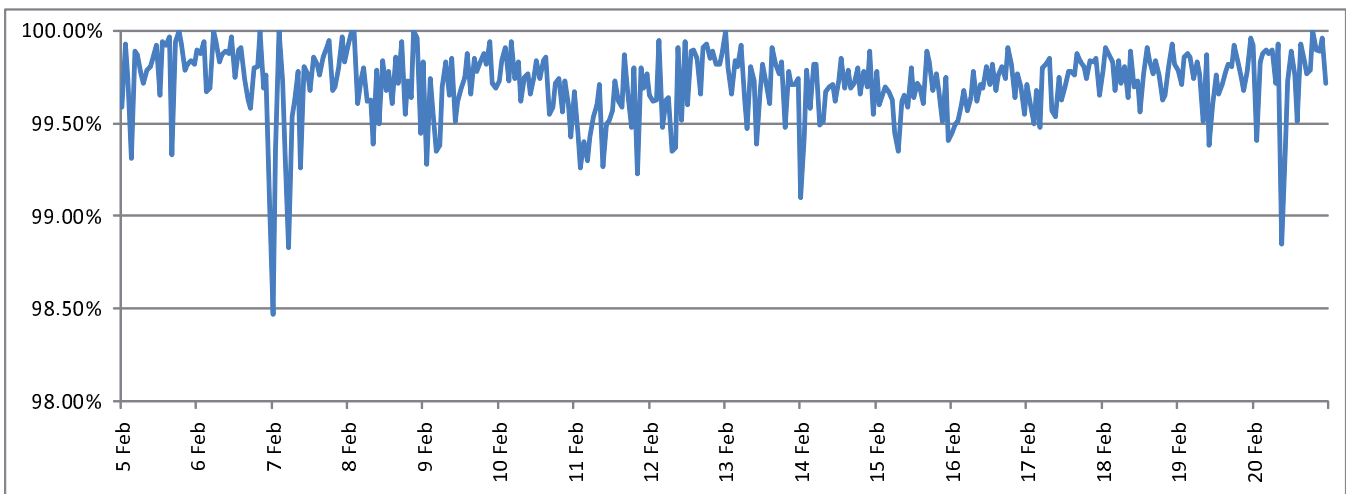


Figure 1: Average catch rate of all full solutions throughout the test.

the false positive (FP) rate. Products earn VBSpam certification if this value is at least 97:

$$SC - (5 \times FP) \geq 97$$

THE EMAIL CORPUS

The test ran for 16 consecutive days, from around 12am GMT on Saturday 5 February 2011 until 12am GMT on Monday 21 February 2011.

The corpus contained 140,800 emails, 137,899 of which were spam. Of these, 80,755 were provided by *Project Honey Pot* and 57,144 were provided by *Abusix*; in both cases, the messages were relayed in real time, as were the 2,901 legitimate emails – a record number for our tests. As before, the legitimate emails were sent in a number of languages to represent an international mail stream.

Figure 1 shows the average catch rate of all full solutions throughout the test. As before, to avoid the average being skewed by a poorly performing product, we excluded the highest and lowest catch rate for each hour.

In the previous test we noticed the somewhat surprising fact that spam sent in plain text appeared to be significantly more difficult to filter than spam with both HTML and text in the body or with a pure HTML body. This month's results showed that this was still the case – though, again, we stress that this does not necessarily mean that the messages are difficult to filter *because* of the plain text body. Still, developers looking into ways to improve their products' performance may want to have a look at whether the filtering of text-only emails can be improved upon.

In this test, we again looked at the overall spam corpus and compared it with the sub-corpus of 'difficult' spam – defined as those messages missed by at least two different filters; the latter concerned slightly more than 1 in 42 messages.

This time we looked at the size of the emails (header plus body; in bytes) and how the distribution of sizes differed between the two corpora. Ordering the emails in both corpora by size, Figure 2 shows how quickly emails get bigger in each corpus.

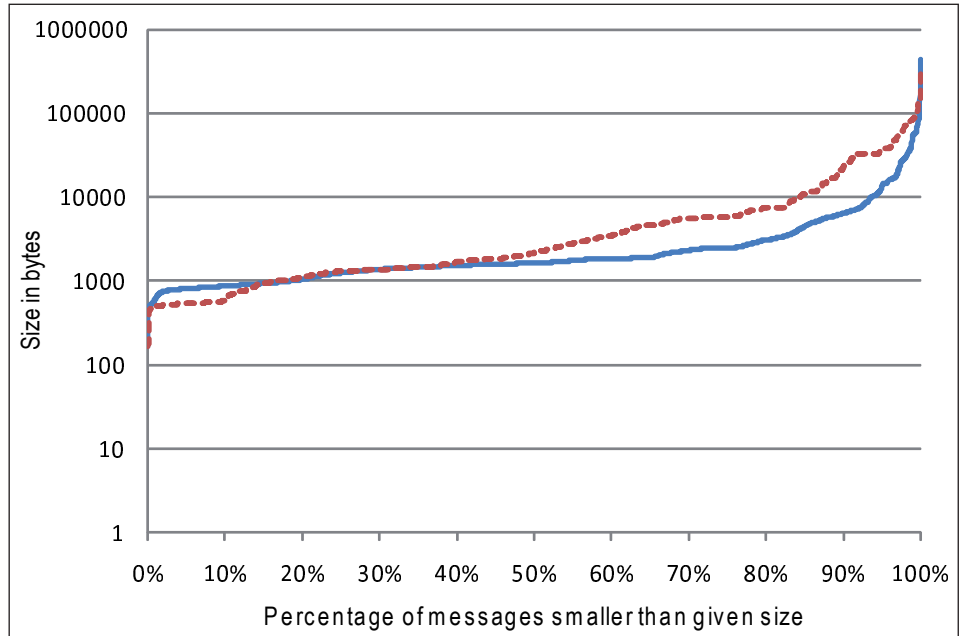


Figure 2: Size of spam emails.

The blue line corresponds to the full corpus, the red one to that of more difficult spam. The graph, with the bytes shown on the vertical axis in logarithmic scale should be read as follows: (exactly) 80% of all spam (blue line) was less than 3,072 bytes in size, while 80% of the difficult spam had a size of less than 7,222 bytes. In the latter corpus, just 57% was smaller than 3,072 bytes.

What the graph shows is that both very small and very large spam messages are harder to filter. It would be wrong to conclude that this difficulty in filtering is a consequence of the message size, but it is nevertheless something developers may want to keep in mind when trying to improve their products.

RESULTS

AnubisNetworks Mail Protection Service

SC rate: 99.83%

FP rate: 0.00%

Final score: 99.83

Project Honey Pot SC rate: 99.84%

Abusix SC rate: 99.82%

The increase in the global volume of spam that was seen just after the beginning of the year would not have been felt by the customers of



AnubisNetworks, as the product's spam catch rate improved significantly too. Thankfully, this improvement was without any false positives, and with the third highest final score the product wins its fifth consecutive VBSpam award.

BitDefender Security for Mail Servers 3.0.2

SC rate: 99.78%

FP rate: 0.00%

Final score: 99.78

Project Honey Pot SC rate: 99.78%

Abusix SC rate: 99.78%

A participant since the very first test, *BitDefender* continues to be the only product to have won a VBSpam award in every test. Despite the product's impressive track record, its developers are not ones for resting on their laurels, as was demonstrated by an improvement in the product's final score for the third time in a row. With no false positives, the product achieved the fifth highest final score and another well deserved VBSpam award.



eleven eXpurgate Managed Service 3.2

SC rate: 99.62%

FP rate: 0.00%

Final score: 99.62

Project Honey Pot SC rate: 99.43%

Abusix SC rate: 99.89%

I was pleased to see *eleven's eXpurgate* return to the test, having been absent since July 2010. Its developers explained that, for them, reducing false positives is an absolute priority and they try to achieve this, among other things, by classifying email into several categories: ham, spam, bulk, almost empty etc. Our test only distinguishes between ham and spam – as do many end-users – but this was not a problem for the product. It did not miss a single legitimate email and it won a VBSpam award with a very decent and improved final score.



Fortinet FortiMail

SC rate: 99.82%

FP rate: 0.00%

Final score: 99.82

Project Honey Pot SC rate: 99.81%

Abusix SC rate: 99.85%

It is a good thing if a product performs well several tests in a row, and even better when it also manages to improve its performance. In this test, *FortiMail* both increased its spam catch rate slightly and eliminated false positives. The appliance saw its final score improve for the third time in a row and easily wins its 11th VBSpam award.



Halon Mail Security

SC rate: 99.71%

FP rate: 0.00%

Final score: 99.71

Project Honey Pot SC rate: 99.72%

Abusix SC rate: 99.69%

Halon, a Swedish company, offers three spam-filtering solutions: a hosted solution, a hardware appliance and a virtual appliance; we tested the latter.

The product was installed easily on *VMware* and setting it up was equally straightforward. A nice, intuitive web interface lets the administrator change settings where necessary and I was particularly charmed by the fact that the product uses its own scripting language that can be used to fine-tune its performance. This will give more tech-savvy sysadmins the possibility to add their own rules to tailor the product specifically for their organization's particular needs.

Of course, a user-friendly interface is only meaningful if the product itself performs well, but that was certainly the case here. With a good spam catch rate and no false positives at all, *Halon Mail Security's* final score is among the highest in this test and earns the product a well-deserved VBSpam award.



Kaspersky Anti-Spam 3.0

SC rate: 98.32%

FP rate: 0.00%

Final score: 98.32

Project Honey Pot SC rate: 98.75%

Abusix SC rate: 97.73%

Kaspersky's spam catch rate was significantly lower this month than in the previous test thanks to a run of bad days during the test, when the product's performance dropped quite a bit (as can



be seen from the high standard deviation in the table on p.21). Thankfully, there was room for this, and as there were no false positives, the product ended up winning its tenth VBSpam award.

Libra Esva 2.0

SC rate: 99.89%
SC rate pre-DATA: 98.34%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.95%

Libra Esva achieved the second highest final score in the previous test – and managed to repeat the achievement this month, once again combining a very high spam catch rate with a zero false positive rate. The Italian company earns its sixth VBSpam award in as many tests.



McAfee Email Gateway (formerly IronMail)

SC rate: 99.92%
FP rate: 0.21%
Final score: 98.88
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.99%

As in the previous test, *McAfee's Email Gateway* appliance achieved the second highest spam catch rate. Unfortunately, some of the domains that were seen in legitimate emails but which are also frequently used in spam messages, caused the product to generate a handful of false positives. Still, with a decent final score, the product earns its tenth consecutive VBSpam award.



McAfee Email and Web Security Appliance

SC rate: 99.20%
FP rate: 0.48%
Final score: 96.79
Project Honey Pot SC rate: 99.16%
Abusix SC rate: 99.27%

With 14 false positives, *McAfee's* second appliance had the joint highest false positive rate. This would not automatically have denied the product a VBSpam award, but with a spam catch rate that was slightly below average,

the product's final score fell below the threshold of 97 and no certification can be awarded.

MessageStream

SC rate: 99.70%
FP rate: 0.48%
Final score: 97.29
Project Honey Pot SC rate: 99.63%
Abusix SC rate: 99.81%

MessageStream's hosted solution missed a relatively high number of legitimate emails, but its spam catch rate was high enough to make up for that. There is certainly room for improvement, but in the meantime, *MessageStream* wins its 11th VBSpam award.



OnlyMyEmail's Corporate MX-Defender

SC rate: 99.99%
FP rate: 0.14%
Final score: 99.30
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.98%

OnlyMyEmail's MX-Defender continues to amaze me with its spam catch rate, which this time saw it miss less than one in 8,500 spam emails. Unlike in the previous test, there were a few false positives this time, which reduced the final score, but it was still a very decent score and wins the product its third VBSpam award.



Sophos Email Appliance

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.97%

Sophos's previous test result contains a lesson for all users of spam filters. The product was set up to tag spam emails with an 'X-Spam: yes' header. What looked like and counted as its single false positive in the previous test was actually an email that already contained this header – probably added by an



	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Anubis Networks	2901	0	0.00%	230	137669	99.83%	99.83
BitDefender	2901	0	0.00%	305	137594	99.78%	99.78
eleven	2901	0	0.00%	521	137378	99.62%	99.62
FortiMail	2901	0	0.00%	244	137655	99.82%	99.82
Halon Mail Security	2901	0	0.00%	400	137499	99.71%	99.71
Kaspersky Anti-Spam	2901	0	0.00%	2311	135588	98.32%	98.32
Libra Esva	2901	0	0.00%	155	137744	99.89%	99.89
McAfee Email Gateway	2895	6	0.21%	113	137786	99.92%	98.88
McAfee EWS	2887	14	0.48%	1097	136802	99.20%	96.79
MessageStream	2887	14	0.48%	408	137491	99.70%	97.29
OnlyMyEmail	2897	4	0.14%	16	137883	99.99%	99.30
Sophos Email Appliance	2901	0	0.00%	122	137777	99.91%	99.91
SPAMfighter	2895	6	0.21%	2179	135720	98.42%	97.39
SpamTitan	2894	7	0.24%	143	137756	99.90%	98.69
Symantec Brightmail Gateway	2899	2	0.07%	183	137716	99.87%	99.52
The Email Laundry	2895	6	0.21%	413	137486	99.70%	98.67
Vade Retro	2896	5	0.17%	240	137659	99.83%	98.96
Vamsoft ORF	2901	0	0.00%	1245	136654	99.10%	99.10
Webroot	2893	8	0.28%	185	137714	99.87%	98.49
Spamhaus ZEN+DBL*	2901	0	0.00%	1768	136131	98.72%	98.72

*As the only partial solution in this test, the results for Spamhaus are listed separately from the full solutions.

over-zealous outbound filter. While for products in our tests it shows the importance of adding more unique headers, all users of spam filters should know that even a very good spam filter can perform suboptimally because of a minor tweak in its settings.

And *Sophos Email Appliance* is a very good spam filter, as demonstrated in the current test. The third highest spam catch rate combined with no false positives at all gave it the highest final score and the product’s developers in the UK and Canada should consider themselves the winners of this test.

SPAMfighter Mail Gateway

SC rate: 98.42%
FP rate: 0.21%
Final score: 97.39
Project Honey Pot SC rate: 99.06%
Abusix SC rate: 97.52%



SPAMfighter’s developers will be keen to learn the reason for their product’s reduced spam catch rate – which they no doubt will be a little disappointed with. This was mostly due to a large number of missed spam in the *Abusix* corpus. Ultimately, they will be pleased to learn that the spam catch rate was still high enough that even a handful of false positives did not get in the way of them winning their ninth VBSpam award.

SpamTitan

SC rate: 99.90%
FP rate: 0.24%
Final score: 98.69
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.83%

SpamTitan continues to score one of the highest spam catch rates in the tests, and users of the virtual appliance will



	Project Honey Pot		Abusix		pre-DATA [†]		STDev [‡]
	FN	SC Rate	FN	SC Rate	FN	SC Rate	
Anubis Networks	128	99.84%	102	99.82%	N/A	N/A	0.54
BitDefender	179	99.78%	126	99.78%	N/A	N/A	0.58
eleven	460	99.43%	61	99.89%	N/A	N/A	1.18
FortiMail	156	99.81%	88	99.85%	N/A	N/A	0.47
Halon Mail Security	224	99.72%	176	99.69%	N/A	N/A	0.39
Kaspersky Anti-Spam	1013	98.75%	1298	97.73%	N/A	N/A	4.79
Libra Esva	128	99.84%	27	99.95%	2285	98.34%	0.23
McAfee Email Gateway	105	99.87%	8	99.99%	N/A	N/A	0.20
McAfee EWS	681	99.16%	416	99.27%	N/A	N/A	1.07
MessageStream	302	99.63%	106	99.81%	N/A	N/A	0.45
OnlyMyEmail	6	99.99%	10	99.98%	N/A	N/A	0.05
Sophos Email Appliance	104	99.87%	18	99.97%	N/A	N/A	0.24
SPAMfighter	759	99.06%	1420	97.52%	N/A	N/A	3.01
SpamTitan	48	99.94%	95	99.83%	N/A	N/A	0.19
Symantec Brightmail Gateway	130	99.84%	53	99.91%	N/A	N/A	0.33
The Email Laundry	332	99.59%	81	99.86%	1177	99.15%	0.45
Vade Retro	195	99.76%	45	99.92%	N/A	N/A	0.42
Vamsoft ORF	914	98.87%	331	99.42%	N/A	N/A	0.72
Webroot	84	99.90%	101	99.82%	32948	76.11%	0.22
Spamhaus ZEN+DBL*	1113	98.62%	655	98.85%	2805	97.97%	0.94

*As the only partial solution in this test, the results for Spamhaus are listed separately from the full solutions.

[†] pre-DATA filtering was optional and was applied on the full spam corpus. All of The Email Laundry's false positives occurred pre-DATA; none of the other products had pre-DATA false positives.

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

find few spam emails in their inboxes. In this test, the high SC rate came at the expense of seven blocked legitimate emails. While these are seven too many, they were not enough to prevent the product from winning yet another VBSpam award.

appliance achieving an even better final score. The product's developers can console themselves with the fact that their final score was the highest among those products that had false positives, and they can add yet another VBSpam award to their unbroken series.

Symantec Brightmail Gateway 9.0

SC rate: 99.87%
FP rate: 0.07%
Final score: 99.52
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.91%



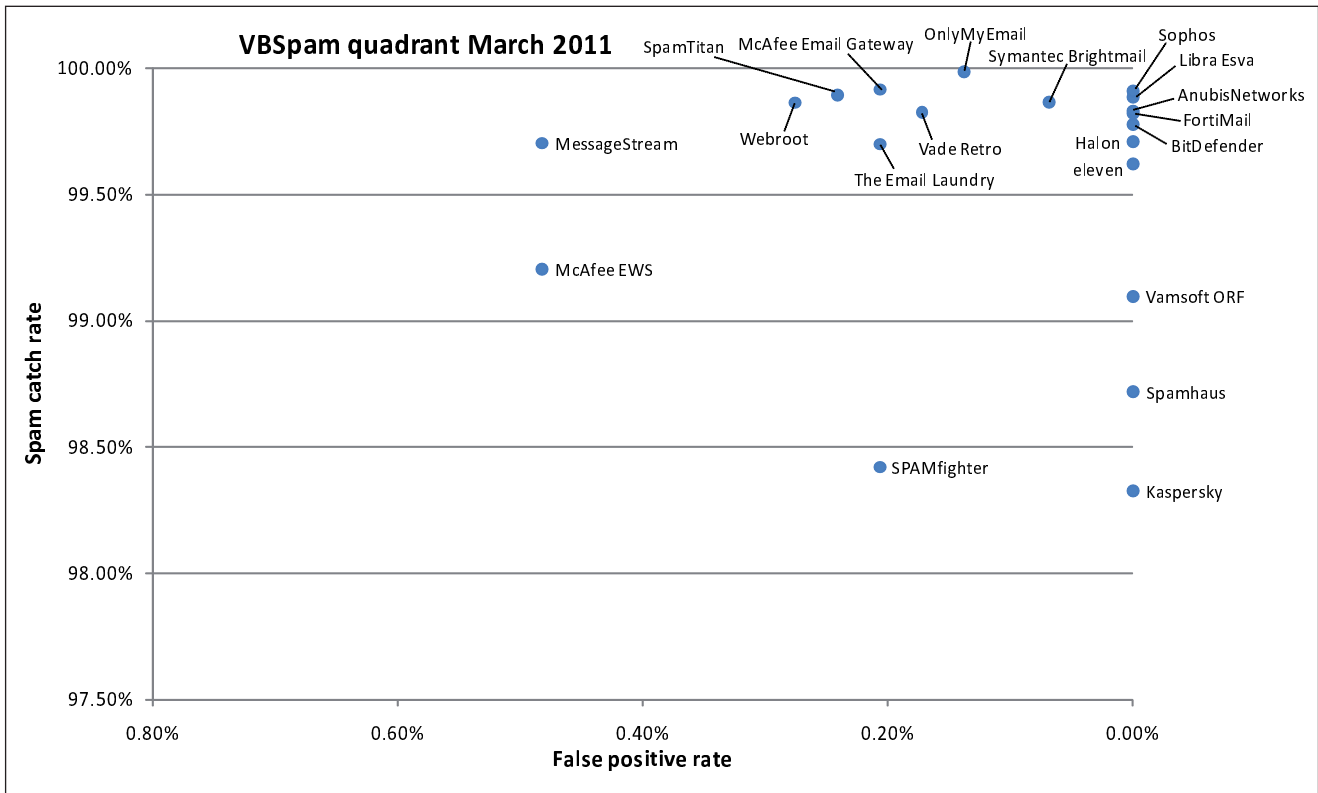
Two related legitimate emails were missed on the first day of the test and these got in the way of Symantec's virtual

The Email Laundry

SC rate: 99.70%
SC rate pre-DATA: 99.15%
FP rate: 0.21%
Final score: 98.67
Project Honey Pot SC rate: 99.59%
Abusix SC rate: 99.86%



One of the rules in this test is that we count no more than four false positives



per sending IP address. We believe that, in practice, multiple blocked messages from the same legitimate sender will either result in the sender finding a different way to communicate their message, or the recipient will adjust their filter – for instance by whitelisting the sender’s address.

This explains why *The Email Laundry*, which missed a few dozen legitimate emails from one sender, only scored six false positives in this test and thus easily won its sixth VBSpam award. More important was the fact that, well before the end of the test, and before we had had a chance to give the developers feedback on the product’s performance, emails from the sender in question were being accepted.

Vade Retro Center

- SC rate:** 99.83%
- FP rate:** 0.17%
- Final score:** 98.96
- Project Honey Pot SC rate:** 99.76%
- Abusix SC rate:** 99.92%

Vade Retro Center scored its highest spam catch rate to date, and while it was sad to see that the number of false



positives increased to five, a sixth consecutive VBSpam award was easily won by the product.

Vamsoft ORF

- SC rate:** 99.10%
- FP rate:** 0.00%
- Final score:** 99.10
- Project Honey Pot SC rate:** 98.87%
- Abusix SC rate:** 99.42%

For the fourth time in six tests, *ORF* did not miss a single legitimate email – a unique achievement among full solutions in this test. Even if the spam catch rate isn’t quite as high as that of some other products, the customers of the Hungarian-developed product will have little reason to look in their spam folders, and that may be just as important. A sixth VBSpam award is thus well deserved.



Webroot

- SC rate:** 99.87%
- SC rate pre-DATA:** 76.11%

Products ranked by final score	Final score
Sophos Email Appliance	99.91
Libra Esva	99.89
Anubis Networks	99.83
FortiMail	99.82
BitDefender	99.78
Halon Mail Security	99.71
eleven	99.62
Symantec Brightmail Gateway	99.52
OnlyMyEmail	99.30
Vamsoft ORF	99.10
Vade Retro	98.96
McAfee Email Gateway	98.88
Spamhaus ZEN+DBL	98.72
SpamTitan	98.69
The Email Laundry	98.67
Webroot	98.49
Kaspersky Anti-Spam	98.32
SPAMfighter	97.39
MessageStream	97.29
McAfee EWS	96.79

Webroot contd.

FP rate: 0.28%

Final score: 98.49

Project Honey Pot SC rate: 99.90%

Abusix SC rate: 99.82%

Once again, *Webroot's* hosted anti-spam solution blocked the vast majority of spam emails, significantly reducing its customers' need for bandwidth. Unfortunately, there were a number of false positives which meant the product achieved a slightly lower final score, but it still performed well enough to earn its 11th consecutive VBSpam award.



Spamhaus ZEN+DBL

SC rate: 98.72%

SC rate pre-DATA: 97.97%

FP rate: 0.00%

Final score: 98.72

Project Honey Pot SC rate: 98.62%

Abusix SC rate: 98.85%

It is hard to think of spam filtering without the use of DNS blacklists and, thinking about those, it is hard to ignore *Spamhaus*. Another good performance showed that there is a reason for this: the *ZEN* IP-based blacklist blocked just short of 98% of all spam, while subsequent scanning of email bodies against the *DBL* domain blacklist blocked over one third of the remaining emails. Both were without false positives and the product – which is only a partial solution – won its eighth VBSpam award in as many tests.



CONCLUSION

It was pleasing to award VBSpam certification to 19 products this month and to find out that the stricter threshold we introduced in the previous test does not pose too many difficulties for the products. A number of new products are expected to join the field for the next test and they will have their work cut out if they are to match the standards set by the current entrants.

In the introduction to this review, I mentioned the difference between the 'right' decision and the 'best' decision for a spam filter to make on a particular email, and how these two usually, but not always, coincide. To overcome this problem, users and system administrators might want to whitelist or blacklist certain senders, IP addresses and domains. In future tests, we hope to be able to verify whether products have this option available and whether it works.

Performance tables from this test, and each of the 11 previous tests can be viewed on the redesigned VBSpam website at <http://www.virusbtn.com/vbspam>.

Later in March I will be discussing the subject of testing messaging filters in a slightly broader context at the eCrime Researchers Sync-Up, organized by the Anti-Phishing Working Group. Details of the event, which will be held 14–15 March in Dublin, can be found at <http://www.ecrimeresearch.org/2011syncup/agenda.html>.

The next VBSpam test will run in April. Developers interested in submitting their products should contact me on martijn.grooten@virusbtn.com.

END NOTES & NEWS

The 12th annual CanSecWest conference will be held 9–11 March 2011 in Vancouver, Canada. See <http://cansecwest.com/>.

The 8th Annual Enterprise Security Conference will be held 14–15 March 2011 in Kuala Lumpur, Malaysia. For details see <http://www.acnergy.com/>.

Black Hat Europe takes place 15–18 March 2011 in Barcelona, Spain. For more information see <http://www.blackhat.com/>.

Infosecurity Europe will take place 19–21 April 2011 in London, UK. For more details see <http://www.infosec.co.uk/>.

SOURCE Boston 2011 will be held 20–22 April 2011 in Boston, MA, USA. For more details see <http://www.sourceconference.com/>.

The New York Computer Forensics Show will be held 26–27 April 2011 in New York, NY, USA. For more information see <http://www.computerforensicsshow.com/>.

The 5th International CARO Workshop will be held 5–6 May 2011 in Prague, Czech Republic. The main theme of the conference will be 'Hardening the net'. Details are available on the conference website at <http://www.caro2011.org/>.

The 20th Annual EICAR Conference will be held 9–10 May 2011 in Krems, Austria. This year's conference is named 'New trends in malware and anti-malware techniques: myths, reality and context'. A pre-conference programme will run 7–8 May. For full details see <http://www.eicar.org/conference/>.

The 6th International Conference on IT Security Incident Management & IT Forensics will be held 10–12 May 2011 in Stuttgart, Germany. See <http://www.imf-conference.org/>.

TakeDownCon takes place 14–19 May 2011 in Dallas, TX, USA. The event aims to bring together security researchers from corporate, government and academic sectors as well the underground to present and debate the latest security threats and disclose and scrutinize vulnerabilities. For more details see <http://www.takedowncon.com/>.

The 2nd VB 'Securing Your Organization in the Age of Cybercrime' Seminar takes place 24 May 2011 in Milton Keynes, UK. Held in association with the MCT Faculty of The Open University, the seminar gives IT professionals an opportunity to learn from and interact with security experts at the top of their field and take away invaluable advice and information on the latest threats, strategies and solutions for protecting their organizations. For details see <http://www.virusbntn.com/seminar/>.

The 2011 National Information Security Conference will be held 8–10 June 2011 in St Andrews, Scotland. Registration for the event is by qualification only – applications can be made at <http://www.nisc.org.uk/>.

The 23rd Annual FIRST Conference takes place 12–17 June 2011 in Vienna, Austria. The conference promotes worldwide coordination and cooperation among Computer Security Incident Response Teams. For more details see <http://conference.first.org/>.

SOURCE Seattle 2011 will be held 16–17 June 2011 in Seattle, WA, USA. For more details see <http://www.sourceconference.com/>.

Black Hat USA takes place 30 July to 4 August 2011 in Las Vegas, NV, USA. DEFCON 19 follows the Black Hat event, taking place 4–7 August, also in Las Vegas. For more information see <http://www.blackhat.com/> and <http://www.defcon.org/>.

The 20th USENIX Security Symposium will be held 10–12 August 2011 in San Francisco, CA, USA. See <http://usenix.org/>.

VB2011 takes place 5–7 October 2011 in Barcelona, Spain. VB is currently seeking submissions from those wishing to present at the conference. Full details of the call for papers are available at <http://www.virusbntn.com/conference/vb2011>. For details of sponsorship opportunities and any other queries relating to VB2011, please contact conference@virusbntn.com.

ADVISORY BOARD

Pavel Baudis, *Alwil Software, Czech Republic*
Dr Sarah Gordon, *Independent research scientist, USA*
Dr John Graham-Cumming, *Causata, UK*
Shimon Gruper, *NovaSpark, Israel*
Dmitry Gryaznov, *McAfee, USA*
Joe Hartmann, *Microsoft, USA*
Dr Jan Hruska, *Sophos, UK*
Jeannette Jarvis, *Independent researcher, USA*
Jakub Kaminski, *Microsoft, Australia*
Eugene Kaspersky, *Kaspersky Lab, Russia*
Jimmy Kuo, *Microsoft, USA*
Costin Raiu, *Kaspersky Lab, Russia*
Péter Ször, *Independent researcher, USA*
Roger Thompson, *AVG, USA*
Joseph Wells, *Independent research scientist, USA*

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

- Single user: \$175
- Corporate (turnover < \$10 million): \$500
- Corporate (turnover < \$100 million): \$1,000
- Corporate (turnover > \$100 million): \$2,000
- *Bona fide* charities and educational institutions: \$175
- Public libraries and government organizations: \$500

Corporate rates include a licence for intranet publication.

See <http://www.virusbntn.com/virusbulletin/subscriptions/> for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:

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@virusbntn.com Web: <http://www.virusbntn.com/>

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2011 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England.

Tel: +44 (0)1235 555139. /2011/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.