JULY 2011

virus BULLETIN

Fighting malware and spam

JULY 2011 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

Those who follow the security news will have seen reports[1] of a significant drop in spam levels over recent months. This, of course, is very good news for users and system administrators alike, but in the VBSpam tests we look at a different aspect of spam, and consider not the quantity but, if you like, the 'quality' of spam: what percentage of it makes it through to users' inboxes and which anti-spam solutions do the best job of blocking those spam messages, ideally without blocking legitimate ones too.

The corpus for this month's test was actually several times larger than that used in previous months. The reason for this was not that we received more spam but that we solved some network issues that had been troubling us for several months (the issues proved to have been caused by a router that was not able to deal with the amount of traffic used in the tests). With the issues resolved we could finally open the tap and send almost 20,000 spam messages a day through each of the products.

To give an idea how much traffic that is, it amounts to more than a dozen messages per minute – far too many to deal with manually, in case anyone still thinks that it is possible to deal with spam in that way. Of course, many organizations receive far greater volumes of email than this.

Apart from the increased volume of spam, we also intended to introduce a new stream in this test: legitimate newsletters. We subscribed to a large number of these, aiming to report on products' performance against this corpus as some additional information in the test. Unfortunately, while subscribing to newsletters turned out to be easy (in many cases probably too easy, as the majority did not check whether the subscription request came from the actual user of the address) it was difficult to obtain a large corpus of newsletters without having it dominated by a handful of 'daily newsletters'.

In the end it was decided that the number of newsletters successfully subscribed to (154 if we restrict it to those that required confirmed opt-in and included up to five newsletters of each kind) was too small to draw upon for meaningful conclusions.

What we did look at was whether, for example, using confirmed opt-in and/or DKIM increased the likelihood of a newsletter being delivered. While results suggested that this was the case, it could not be shown with sufficient statistical significance. Hopefully, in the next test (by which time we intend to have increased the number of newsletters subscribed to) we will have a clearer picture.

We also hope to be able to report on individual products' performance on filtering newsletters (although this will not count towards the final score or VBSpam certification).

This month's test – the 14th VBSpam test – included 17 full solutions (two of which were new to the *VB* test bench) and two DNS blacklists. All of the full solutions achieved a VBSpam award, but only a handful of products did so without blocking any legitimate email.

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. Three 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

[1] Such as http://www.virusbtn.com/virusbulletin/archive/2011/07/vb201107-news1.

ISSN 1749-7027

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

SC - (5 x FP) ≥ 97

THE EMAIL CORPUS

The test ran for 16 consecutive days, from 12am GMT on Saturday 18 June 2011 until 12am GMT on Monday 4 July 2011.

The corpus contained 293,757 emails, 291,304 of which were spam. Of these, 186,284 were provided by *Project Honey Pot* and 105,020 were provided by *Abusix*; in both cases, the messages were relayed in real time, as were the 2,453 legitimate emails.

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

Those comparing this month's results with those of previous tests will notice an increase in the number of false positives seen this month, with just four full solutions avoiding them altogether. This is largely because of one sender in the ham corpus that for several days found itself listed on a number of blacklists – allegedly because the sender's server had been abused and used for sending spam.

No one will deny that blacklisting an IP address that is also used for sending legitimate email will cause problems for the latter. The anti-spam community is divided over when (and whether) blocking is justified in such a case. We take the conservative approach and count legitimate emails missed in this manner as false positives.

Of course, we also understand the view that by blacklisting an IP, the system administrator is forced to fix their problems and therefore the total damage incurred may actually be less than if the IP were left unblocked. To avoid results being excessively skewed by a single blacklisted

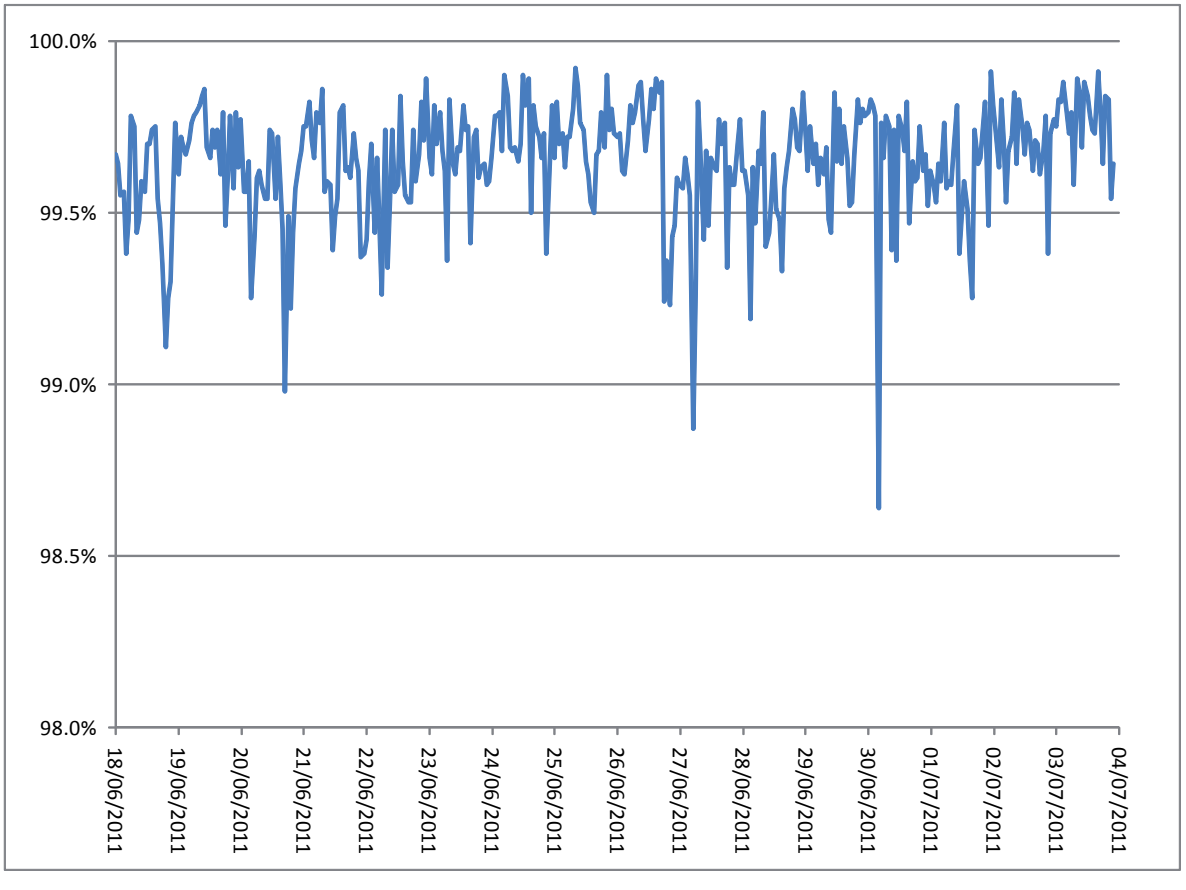


Figure 1: Average catch rate of all full solutions over the test period.

sender, we count no more than four false positives per IP address per product.

RESULTS

BitDefender Security for Mail Servers 3.0.2

SC rate: 99.88%
FP rate: 0.00%
Final score: 99.88
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.90%

BitDefender's anti-spam solution continues to be the only product to have won a VBSpam award in all 14 of our tests. This month's results show that this is more than just a matter of the developers being brave enough to submit their product every time – thanks in part to a total lack of false positives, the product achieved this month's second highest final score.

Fortinet FortiMail

SC rate: 99.79%
FP rate: 0.00%
Final score: 99.79
Project Honey Pot SC rate: 99.74%
Abusix SC rate: 99.88%

It seems that 13 is no unlucky number for *Fortinet,* as this month the company's *FortiMail* appliance achieved its 13th VBSpam award in as many entries – and with the third highest final score. Moreover, it was one of just four products that did not block any legitimate emails.

GFI MailEssentials

SC rate: 99.61%
FP rate: 0.16%
Final score: 98.79
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.82%

On several occasions we have seen a product suffer from a number of false positives in its debut test, but significantly reduce that number in the next test – probably because its developers found settings that were more suited to our test set-up. This was certainly the case with *GFI*'s *MailEssentials*, which on this occasion only misclassified legitimate emails from the aforementioned heavily blacklisted IP address. Thus, with four false positives and a good spam catch rate, *MailEssentials* easily wins its second VBSpam award.

Halon Mail Security

SC rate: 99.57%
FP rate: 0.04%
Final score: 99.36
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.28%

In its third VBSpam test, *Halon* almost equalled its spam catch rate from the last test, but did so while incurring a single false positive – the product's first since it joined the tests. That is still fewer than the average product, though, and with a decent final score the virtual appliance achieves its third VBSpam award.

Kaspersky Anti-Spam 3.0

SC rate: 99.48%
FP rate: 0.00%
Final score: 99.48
Project Honey Pot SC rate: 99.41%
Abusix SC rate: 99.60%

During the running of this test, *Kaspersky Lab* celebrated its 14th birthday – no small achievement in an industry where things seem to change daily. The Russian company receives another VBSpam award as a belated birthday present, albeit one that was worked hard for. A slightly improved spam catch rate and the fact that this was one of only a small number of products without false positives should give the developers something to be pleased about.

Libra Esva 2.0

SC rate: 99.97%
FP rate: 0.16%
Final score: 99.15
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.99%
SC rate pre-DATA: 97.95%

For the second time in a row, *Libra Esva* caught more spam than all but one other product, missing fewer than 100 out of more than 290,000 spam messages. Unfortunately for the Italian product's developers, it blocked the same legitimate emails as many other products, which saw its final score drop to a slightly lower position in the league tables. The company's eighth VBSpam award in as many tests should keep the developers motivated to improve this again though.

McAfee Email Gateway (formerly IronMail)

SC rate: 99.88%
FP rate: 0.12%
Final score: 99.27
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.88%

As in previous tests, *McAfee*'s *Email Gateway* appliance demonstrated an excellent spam catch rate, missing fewer than one in 800 spam messages. There were three false positives this time – all from the same IP address (though not 'that' IP address) – but that didn't stop the product from achieving its 12th consecutive VBSpam award

McAfee SaaS Email Protection

SC rate: 99.91%
FP rate: 0.33%
Final score: 98.28
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.93%

The fact that email security is not a one-size-fits-all business is demonstrated by the different kinds of products in our tests, and the fact that even a single company such as *McAfee* offers a variety of solutions to protect the inboxes of various types and sizes of organizations.

McAfee SaaS Email Protection is the third product from the security giant to participate in the VBSpam tests. As the name suggests, this is a hosted solution that receives email 'in the cloud' and then relays only the filtered email to the customer. If done well, this can save the customer valuable time and resources. Many customers will also be interested in the product's numerous additional features, varying from malware scanning to email encryption and other kinds of policy-based controls on outbound email.

In our tests, we only looked at the product's inbound spam-filtering capabilities. The spam catch rate was certainly impressive, with fewer than one in 1,000 spam messages missed. There were eight false positives (from two different email addresses), which means that users may occasionally have to search the product's quarantine for legitimate email, but this may partly be because it was the product's first VBSpam test. In any case, the final score was high enough to win the product a VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%
Final score: 100.00
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%

With only two missed spam messages and no false positives in the last test, *OnlyMyEmail's MX-Defender* had set the bar extremely high for this time around. Despite this, the hosted solution managed to match its last performance – once again avoiding false positives altogether and missing just two spam emails, making this the fifth time in a row that the product has achieved the highest spam catch rate. With such a stunning result and a final score rounded to 100.00, *MX-Defender* ensures that the bar remains very high not just for itself, but for all products in all tests to come.

Sophos Email Appliance

SC rate: 99.90%
FP rate: 0.24%
Final score: 98.67
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.94%

Despite a significantly improved spam catch rate, six false positives caused the final score for *Sophos*'s *Email Appliance* to drop to a mid-table position. No doubt this will cause some disappointment among the product's developers but it wasn't enough to deny the product its 10th VBSpam award and it should motivate the developers to work on improving the final score for next time.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
BitDefender	2453	0	0.00%	339	290965	99.88%	99.88
FortiMail	2453	0	0.00%	613	290691	99.79%	99.79
GFI MailEssentials	2449	4	0.16%	1148	290156	99.61%	98.79
Halon Security	2452	1	0.04%	1261	290043	99.57%	99.36
Kaspersky Anti-Spam	2453	0	0.00%	1521	289783	99.48%	99.48
Libra Esva	2449	4	0.16%	99	291205	99.97%	99.15
McAfee Email Gateway	2450	3	0.12%	342	290962	99.88%	99.27
McAfee SaaS	2445	8	0.33%	257	291047	99.91%	98.28
OnlyMyEmail	2453	0	0.00%	2	291302	99.999%	100.00
Sophos Email Appliance	2447	6	0.24%	302	291002	99.90%	98.67
SPAMfighter	2451	2	0.08%	633	290671	99.78%	99.38
SpamTitan	2452	1	0.04%	189	291115	99.94%	99.73
Spider Antispam	2445	8	0.33%	1076	290228	99.63%	98.00
Symantec Messaging Gateway	2452	1	0.04%	365	290939	99.87%	99.67
The Email Laundry	2447	6	0.24%	570	290734	99.80%	98.58
Vade Retro	2448	5	0.20%	2827	288477	99.03%	98.01
Vamsoft ORF	2449	4	0.16%	3781	287523	98.70%	97.89
Spamhaus ZEN+DBL*	2449	4	0.16%	3977	287327	98.63%	97.82
SURBL*	2453	0	0.00%	124465	166839	57.27%	57.27

**Spamhaus* and *SURBL* are partial solutions and their performance is not to be compared with that of other products – nor should their mutual performances be compared.

(Please refer to text for full product names.)

SPAMfighter Mail Gateway

SC rate: 99.78%

FP rate: 0.08%

Final score: 99.38

Project Honey Pot SC rate: 99.78%

Abusix SC rate: 99.79%

For the third time in a row *SPAMfighter* sees both its false positive rate decrease (just two legitimate emails were missed this time) and its spam catch rate improve. This shows that the product's developers are working hard and an 11th consecutive VBSpam award is their reward.

SpamTitan

SC rate: 99.94%

FP rate: 0.04%

Final score: 99.73

Project Honey Pot SC rate: 99.94%

Abusix SC rate: 99.93%

Unlike many other products in this test, *SpamTitan* saw its false positive rate reduced – on this occasion the virtual appliance missed just one legitimate email. The product's spam catch rate equalled that of the previous test and was outdone by just two other products on

	Project Honey Pot		Abusix		pre-DATA†		STDev‡
	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
BitDefender	230	99.88%	109	99.90%			0.22
FortiMail	483	99.74%	130	99.88%			0.24
GFI MailEssentials	954	99.49%	194	99.82%			0.35
Halon Security	509	99.73%	752	99.28%			0.64
Kaspersky Anti-Spam	1099	99.41%	422	99.60%			0.62
Libra Esva	85	99.95%	14	99.99%	5967	97.95%	0.08
McAfee Email Gateway	216	99.88%	126	99.88%			0.22
McAfee SaaS	188	99.90%	69	99.93%			0.15
OnlyMyEmail	2	99.999%	0	100.00%			0.01
Sophos Email Appliance	244	99.87%	58	99.94%			0.19
SPAMfighter	415	99.78%	218	99.79%			0.26
SpamTitan	115	99.94%	74	99.93%			0.11
Spider Antispam	475	99.75%	601	99.43%			0.30
Symantec Messaging Gateway	261	99.86%	104	99.90%			0.23
The Email Laundry	509	99.73%	61	99.94%	3714	98.73%	0.23
Vade Retro	2023	98.91%	804	99.23%			1.34
Vamsoft ORF	2165	98.84%	1616	98.46%			0.99
Spamhaus ZEN+DBL*	2619	98.59%	1358	98.71%	7308	97.49%	0.95
SURBL*	107117	42.50%	17348	83.48%			12.68

*_Spamhaus_ and _SURBL_ are partial solutions and their performance is not to be compared with that of other products – nor should their mutual performances be compared.

† pre-DATA filtering was optional and was applied on the full spam corpus. All false positives for the relevant products bar three from _The Email Laundry_ occurred pre-DATA.

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

(Please refer to text for full product names.)

the test bench. As a result, the Irish product easily achieves another VBSpam award – its 11th in as many tests.

Spider Antispam

SC rate: 99.63%

FP rate: 0.33%

Final score: 98.00

Project Honey Pot SC rate: 99.75%

Abusix SC rate: 99.43%

The Czech Republic is home to a number of security companies and *Amenit*, the developer of *Spider Antispam*, is one of them. The company offers a number of email security solutions. We tested its standard anti-spam solution *Spider Antispam*, but the company also offers *Spider Mail Protection*, which combines spam filtering with two anti-malware engines.

Both products are hosted solutions, where the bad messages are filtered out remotely, away from the customer's premises – in this case the filtering is performed in a number of different data centres spread throughout Europe. Like most software-as-a-service solutions, *Spider Antispam* keeps email even when your mail server is down and it can also be used for outbound spam filtering, as well as adding

DKIM-signatures to outgoing email. With the growing importance of sender reputation, this could certainly help delivery rates of outgoing email.

In our test, we only looked at the product's inbound spam-filtering capabilities. These were certainly good, with 99.63% of all spam caught by the product. There were eight false positives, which lowered the final score a little (and gives the developers something to work on), but this was not enough to prevent the product from winning a VBSpam award in its first test.

Symantec Messaging Gateway 9.5 powered by Brightmail

SC rate: 99.87%
FP rate: 0.04%
Final score: 99.67
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.90%

Symantec Messaging Gateway is one of those products to have combined a high spam catch rate with almost no false positives. It missed one legitimate email this time (fewer than most), which gave it the fifth highest final score and a VBSpam award to add to its collection.

The Email Laundry

SC rate: 99.80%
FP rate: 0.24%
Final score: 98.58
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.94%
SC rate pre-DATA: 98.73%

I continue to be amazed by the fact that *The Email Laundry* manages to block close to 99% of all spam during the SMTP transaction before it has even seen the content of the email. This occasionally comes at a price though, as three of the six legitimate emails the hosted solution missed in this test were blocked at this stage of the transaction as well (although it is fair to say that this would also have increased the likelihood of the sender receiving a bounce message). After the content filtering fewer than one in 500 emails were missed – meaning that the product is worthy of its eighth consecutive VBSpam award.

Vade Retro Center

SC rate: 99.03%
FP rate: 0.20%
Final score: 98.01
Project Honey Pot SC rate: 98.91%
Abusix SC rate: 99.23%

In the previous review, we reported that *Vade Retro Center* had some problems filtering spam from the *Abusix* feed. The developers must have taken that feedback to heart as the product performed significantly better on that feed and, as a result, almost halved the percentage of missed spam. Hopefully, in the next test the product will see its false positive rate reduced (it missed five legitimate emails this time), but for now it wins its eighth VBSpam award with a slightly improved final score.

Vamsoft ORF

SC rate: 98.70%
FP rate: 0.16%
Final score: 97.89
Project Honey Pot SC rate: 98.84%
Abusix SC rate: 98.46%

Products ranked by final score*	
OnlyMyEmail	100.00
BitDefender	99.88
FortiMail	99.79
SpamTitan	99.73
Symantec Messaging Gateway	99.67
Kaspersky Anti-Spam	99.48
SPAMfighter	99.38
Halon Security	99.36
McAfee Email Gateway	99.27
Libra Esva	99.15
GFI MailEssentials	98.79
Sophos Email Appliance	98.67
The Email Laundry	98.58
McAfee SaaS	98.28
Vade Retro	98.01
Spider Antispam	98.00
Vamsoft ORF	97.89

*Full solutions only.
(Please refer to text for full product names.)

ORF had not missed a single legitimate email in the last three tests, so no doubt the product's developers will be a little disappointed to find that they missed four legitimate emails on this occasion, even if they came from the same heavily blacklisted sender that pestered many other products. Thankfully, this did not get in the way of the product earning an eighth consecutive VBSpam award.

Spamhaus ZEN+DBL

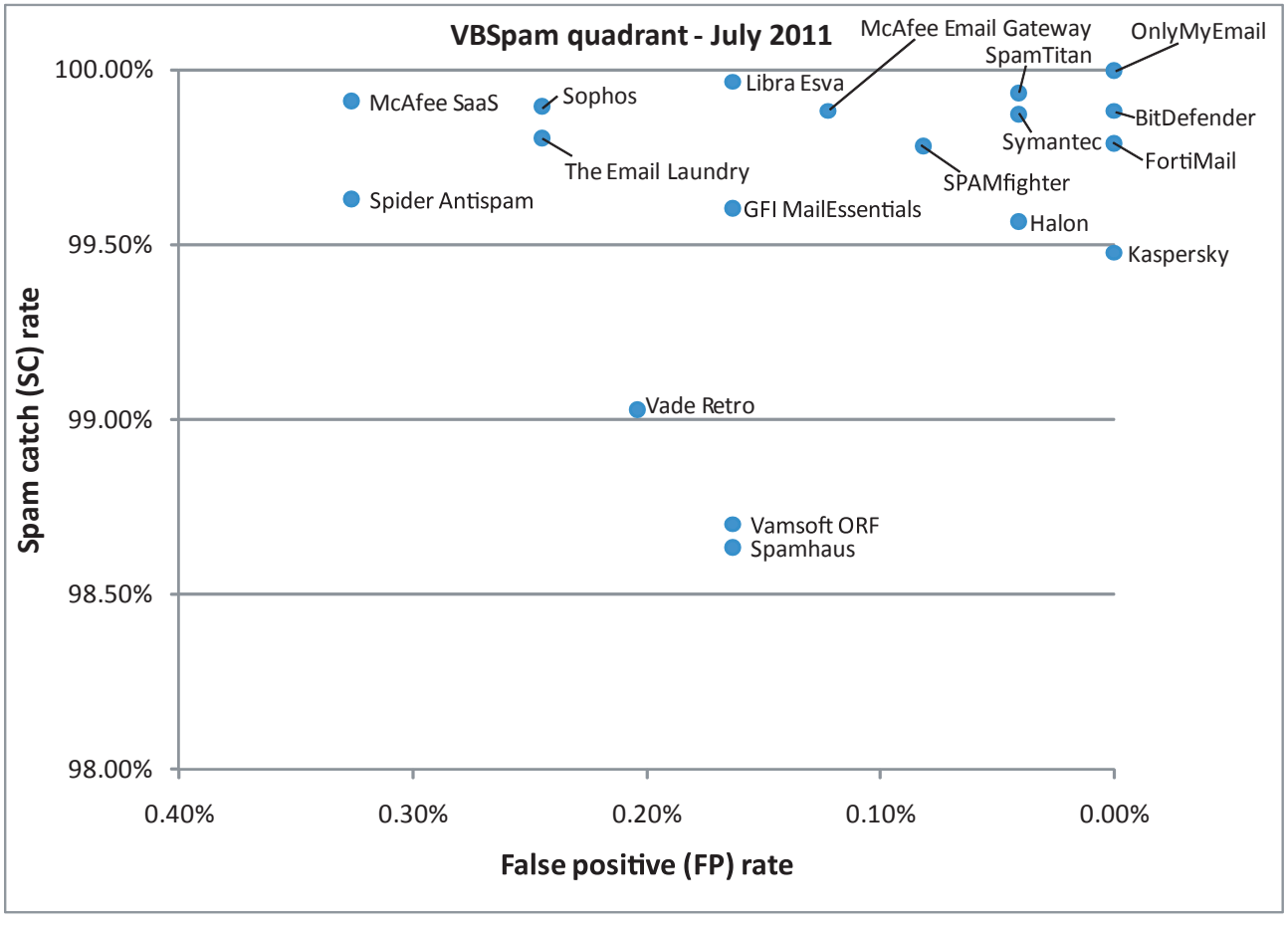
SC rate: 98.63%
FP rate: 0.16%
Final score: 97.89
Project Honey Pot SC rate: 98.59%
Abusix SC rate: 98.71%
SC rate pre-DATA: 97.49%

The ten previous VBSpam tests have shown that *Spamhaus* makes a concerted effort to keep its reputation blacklists from causing false positives. This, the product's eleventh test, marked only the second time some legitimate senders in our ham corpus were blacklisted. However, it may well be that the overall damage was lessened by blacklisting the senders – and this should act as a warning to users of DNS blacklists that using them is no guarantee that only spam will be blocked.

SURBL

SC rate: 57.27%
FP rate: 0.00%
Final score: 57.27
Project Honey Pot SC rate: 42.50%
Abusix SC rate: 83.48%

SURBL, which stands for 'Spam URI Realtime Blocklist', is a blacklist of domains used (solely) for spamming purposes. Like most blacklists, it uses the DNS protocol to allow for quick look-ups of domain names against the blacklist and thus can be used for real-time scanning of spam messages.



SURBL was included in a few VBSpam tests last year as part of the *MXTools* suite but now returns on its own. As before, a slightly modified version of the 'uribl' plug-in for qpsmtpd was used to detect URLs in emails and to perform the look-ups. Users implementing *SURBL* may improve its performance by, for instance, following redirects in URLs and looking for URLs in emails that in some way or another are encoded. Of course, this will require more processor and/or network resources.

It should be noted that *SURBL* is a partial solution that ought to be used as part of a full solution rather than on its own. Its performance should not be compared with that of any of the full solutions in this test or with that of *Spamhaus*, another partial solution, but one that acts on different parts of the email. While the nature of the product means its final score did not come close to the VBSpam award threshold, it certainly did not 'fail' the test.

With more than 57% of messages blocked, *SURBL* does a good job of getting rid of a lot of unwanted email, and no legitimate email was blocked. More telling perhaps, and certainly more impressive, is the fact that of all spam messages in which our plug-in detected at least one URL (not necessarily a malicious one), 83.60% of spam was blocked.

CONCLUSION

Having spent a great many hours trying to solve increasing network problems – which, in the end, proved to be caused by an incompetent router – and then having spent a lot of time subscribing to what turned out to be an insufficient number of newsletters, from the tester's point of view this felt like the test of wasted time.

Of course, that was not the case and the results show both a number of excellent performances (of which, *OnlyMyEmail*'s final score of 100.00 is worth repeating) as well as a number of others that leave some room for improvement. The large number of products with false positives was a bit of a disappointment – even if this was largely caused by a small number of senders – but it is good to see products notching up a sufficiently high spam catch rate to make up for such glitches.

Having been unable to include results on newsletter filtering in this report, we will work hard to ensure that we have enough data available for the next test to enable us to present some interesting results on filtering, both for individual products and more generically.

The next VBSpam test will run in August 2011, with the results scheduled for publication in September. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Web Developer: Paul Hettler

Consulting Editors:

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, US*

SUBSCRIPTION RATES

Subscription price for Virus Bulletin magazine (including comparative reviews) 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.

Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):

- Comparative subscription: $100

See http://www.virusbtn.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@virusbtn.com Web: http://www.virusbtn.com/