SEPTEMBER 2011

virus BULLETIN

Fighting malware and spam

SEPTEMBER 2011 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

Looking purely at the numbers, the difference between a spam catch rate of 99.90% and one of 99.70%, or between a false positive rate of 0.00% and one of 0.02%, may not seem very great. They indicate, however, a threefold increase in the amount of spam in one's inbox and the difference between being able to ignore one's spam folder and having to look there occasionally for a missed email.

In spam filtering, the devil is in the details. In this month's VBSpam test we have added some more of these details: firstly by increasing the size of the ham corpus to over 4,300 emails, and secondly by the introduction of a new corpus consisting of newsletters.

Some prefer the content of their inboxes to consist solely of personal email conversations and are happy with spam filters taking a tough stance on newsletters. Many others, however, would be upset if they missed out on a great offer, an interesting event or a thought-provoking article as a result of the newsletters they subscribed to being blocked by their spam filter. Hence, while the newsletters do not count towards the final score, we believe their inclusion is a valuable addition to the VBSpam tests, and they will provide some more insight into the participating products.

This month there were 23 products on the test bench, 21 of which were full solutions – a record for our tests. The remaining two were partial solutions (DNS blacklists) which are designed to be used in conjunction with other products to provide a complete anti-spam solution. All full solutions achieved a VBSpam award but their performance still differed greatly in the details.

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 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:

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

THE EMAIL CORPUS

The test ran for 19 consecutive days, from 12am GMT on Thursday 11 August 2011 until 12am GMT on Tuesday 29 August 2011.

The corpus contained 176,485 emails, 171,963 of which were spam. Of these, 87,462 were provided by *Project Honey Pot* and 84,501 were provided by *Abusix*; they were all relayed in real time, as were the 4,315 legitimate emails ('ham'). The remaining 207 emails were all newsletters, more on which below.

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

Twice, the hourly average dipped below 99%: in the morning of 14 August products had some difficulty with a malicious spam campaign claiming to come from *UPS*; a little more

ISSN 1749-7027

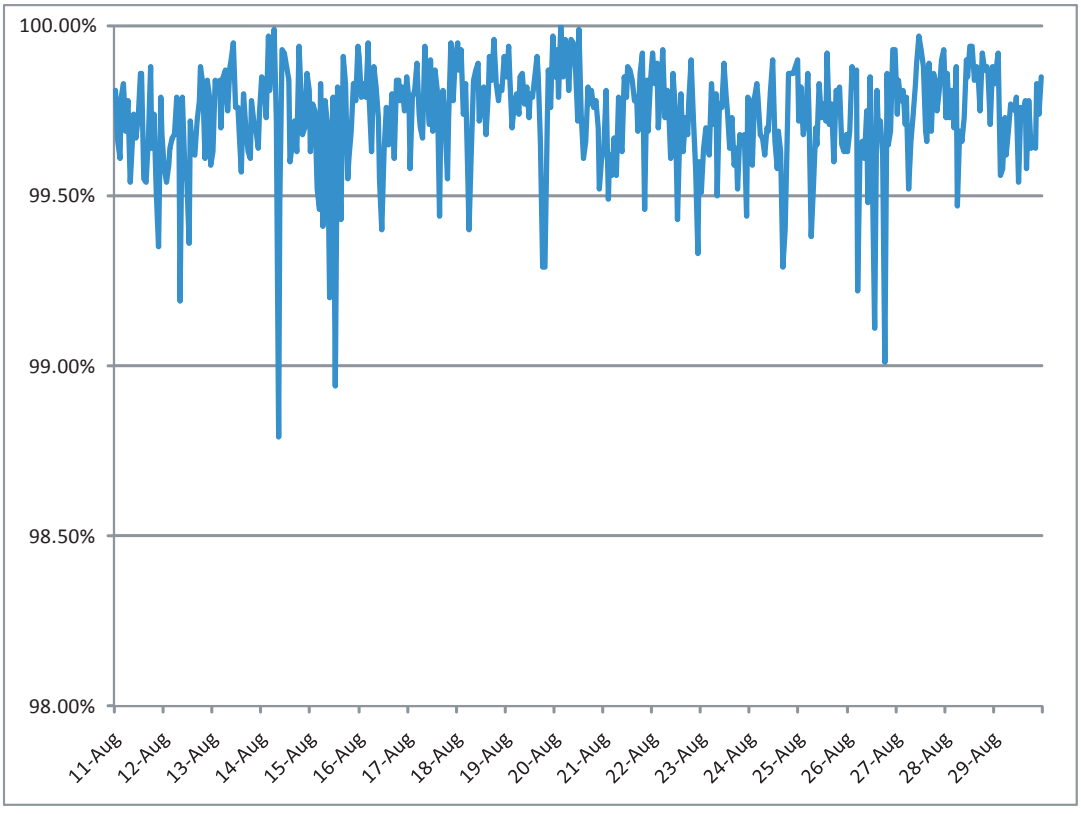


Figure 1: Catch rate of all full solutions throughout the test period.

than a day later it was a German casino spam campaign that caused more problems for products than usual.

The *UPS* spam was an example of something we observed throughout the test: a spam message with a ZIP file attached to it, with the ZIP containing a malicious .exe file. The same attachment was used for about a day in emails with related, but not identical, subjects. Immediately after one attachment stopped appearing in emails, a new one popped up. Subject lines suggested the attachment contained information about lost parcels, an 'End of July statement', a *Xerox* scan, credit card details or, rather mysteriously, a 'changelog'.

The VBSpam test is not designed to measure products' anti-malware capabilities, hence there is no requirement to block or quarantine the attachments. However, since the email messages themselves are spam, they should of course be blocked. Most products coped reasonably well with these emails, although the average catch rate on them was slightly lower than on other kinds of spam.

The remarkable recent increase in the proportion of spam messages containing malicious attachments[1] – reaching similar numbers to those seen several years ago – demonstrates that spammers regularly recycle tricks from the past. Thus, while it is important for spam filters to keep up to date with current technologies, it is equally important for them not to forget old spammers' tricks.

NEWSLETTERS

For the first time, this test contained a small corpus of 'newsletters': non-personal emails that are sent with certain regularity after the recipient has subscribed to them. The corpus was generated by manually subscribing to a large number of newsletters, in a number of different languages and on various topics.

Not surprisingly, this type of email presents some problems for anti-spam solutions: the fact that the messages are sent in bulk, are non-personal and tend to have a commercial nature means that they share some important characteristics with spam.

Recipients' opinions on newsletters vary greatly, as do the newsletters themselves. Some contain information that the recipient really wouldn't want to miss out on and thus they would be frustrated if a spam filter decided the email

[1] See 'Explosive growth of malicious spam': http://www.virusbtn.com/news/2011/08_17.xml.

was not legitimate. On the other hand, some newsletters elicit the same response as spam when they arrive in the recipient's inbox: frustration at the time and inbox space wasted. The fact that the users originally subscribed to these emails, and that many have a working unsubscribe button, does not always help[2].

Because of this, we understand that some products will block the occasional newsletter – and we are willing to assume this may have happened at the implicit or explicit request of their customers. Therefore, performance on the corpus of newsletters does not count towards the final score or have a bearing on the VBSpam awards. Still, with only small differences between products' performance in recent tests, the introduction of this corpus should provide some extra details on each product, which may be valuable to customers.

We set two restrictions on the newsletter corpus: no newsletter is included more than five times (to avoid the results being skewed by performance on a few daily newsletters), and subscription to all newsletters in the corpus must have been confirmed via email.

This subscription method, usually called 'confirmed opt-in' (COI), is considered good practice among senders of email[3]: it avoids unwanted subscriptions due to typos, pranks or bots filling in email addresses en masse. It also helps prevent the newsletters being sent to spam traps, which could greatly reduce their delivery rates. Anti-spam laws in many countries specify confirmed opt-in as a requirement for sending bulk email.

Still, a great many newsletters we signed up for did not ask to confirm the subscription via email. Some took measures to avoid unwanted subscriptions (e.g. using CAPTCHAs, or requiring the email address to be entered twice), but such measures do not eliminate all the aforementioned problems.

Although we did not use these newsletters (generally called 'single opt-in' or 'SOI') in the test, we did send them through the products like the COI newsletters; after all, when signing up for a newsletter it is rarely clear if the subscription will need to be confirmed[4]. Again limiting the SOI corpus to no more than five inclusions per newsletter, we ended up with a corpus of 321 SOI newsletters.

We noticed that, on average, products performed worse on the SOI newsletters than on the COI ones, as can be seen in Figure 2. While well over 70% of COI newsletters were not blocked by any solution, almost half of the SOI newsletters were blocked by at least one solution. Being blocked by three or more products was rare among COI newsletters, but was the case for almost 10% of SOI newsletters. On average, a spam filter was twice as likely to block an SOI newsletter as a COI one.

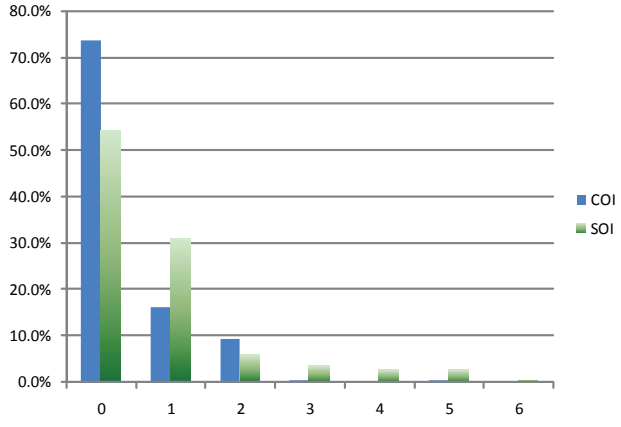


Figure 2: Percentage of newsletters blocked.

This is unlikely to be a coincidence: using some statistics we were able to show with over 99% significance that COI newsletters are indeed less likely to be blocked than SOI ones. Of course, correlation does not imply causation and it may well be that the increased delivery rate is a consequence of the fact that the subscription was confirmed. Still, this may be something email service providers and marketeers may want to keep in mind.

As an aside, during the test we noticed a few newsletters being blocked by all products. Upon further inspection, it turned out that these messages were spam, sent to four tagged addresses, all of which could be linked to the same ESP. We notified the ESP of the suspected data breach.

Of course, fixing the breach does not remove the addresses from the spammers' lists and they are likely to continue to receive spam ad infinitum. This is unfortunate for the owners of those email addresses, but for us it created some spam traps that we will be monitoring carefully. Using these emails we were also able to confirm that none of the products were gaming the test by 'guessing' the tagged addresses used for newsletter subscriptions.

RESULTS

In the text that follows, unless otherwise specified, 'ham' or 'legitimate email' refers to email in the ham corpus – which excludes the newsletters – and a 'false positive' is a message in that corpus erroneously marked by a product as spam.

[2] The advice given in the early days of spam – that you should never click the 'unsubscribe' link, as this would only confirm your address to the spammer – does not help here either.

[3] See http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2.pdf.

[4] One exception we found was that all newsletters from Germany required confirmed subscription; we thought this was a fact worth mentioning.

Because the size of the newsletter corpus is significantly smaller than that of the ham corpus, a missed newsletter will have a much greater effect on the newsletter false positive rate than a missed legitimate email will have on the FP rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of 0.02%, while one missed email in the newsletter corpus results in an FP rate of 0.5%).

AnubisNetworks Mail Protection Service

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.94
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.5%

AnubisNetworks returns to the test after having been absent last month – and what a comeback it is. The hosted solution, which has always performed well, caught more spam than all but two other products and, unlike those products, missed no legitimate email. The highest final score of this test and the company's seventh VBSpam award in as many tests will be good news for the team in Lisbon.

BitDefender Security for Mail Servers 3.0.2

SC rate: 99.82%
FP rate: 0.07%
Final score: 99.47
Project Honey Pot SC rate: 99.79%
Abusix SC rate: 99.85%
Newsletters FP rate: 1.4%

BitDefender continues to be the only product to have won a VBSpam award in every test to date, and this month sees the Romanian product win its 15th award. Its developers will no doubt be a little disappointed with the three false positives, but with a slightly improved final score, the VBSpam award was never in danger.

Fortinet FortiMail

SC rate: 99.74%
FP rate: 0.02%
Final score: 99.63
Project Honey Pot SC rate: 99.59%
Abusix SC rate: 99.91%
Newsletters FP rate: 3.4%

With just one false positive in over 4,300 legitimate emails, *FortiMail* stays well below the average, and its spam catch rate also improved a little. There were more than a handful of missed newsletters, which the developers might want to look into, but this month's performance easily earns the product its 14th consecutive VBSpam award.

GFI MailEssentials

SC rate: 99.68%
FP rate: 0.19%
Final score: 98.75
Project Honey Pot SC rate: 99.45%
Abusix SC rate: 99.91%
Newsletters FP rate: 1.9%

GFI had the joint highest number of false positives in this test. That is not something to be proud of, but it is good to know that still fewer than one in 500 legitimate emails were missed. A small increase in the product's spam catch rate means that the Maltese anti-spam solution wins its third VBSpam award in as many tests.

Halon Mail Security

SC rate: 99.72%
FP rate: 0.07%
Final score: 99.37
Project Honey Pot SC rate: 99.62%
Abusix SC rate: 99.81%
Newsletters FP rate: 1.4%

Halon Mail Security missed three legitimate emails – three times as many as in the product's first three tests put together. That will probably be the cause of some disappointment, but with an increased final score and the product's fourth VBSpam award, *Halon*'s developers will no doubt be eager to get on with proving they were just a little unlucky this time.

IBM Lotus Protector for Mail Security

SC rate: 99.90%
FP rate: 0.07%
Final score: 99.55
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.00%

This spring, *IBM* celebrated its 100th birthday. In an industry where ten years

is old and 25 years gives you Methuselah status, that is an incredibly long time. If anything, it shows how the company constantly adapts to new developments and challenges. Spam is one of these challenges – certainly not the easiest to deal with, and it is no surprise that in *Lotus Protector*, *IBM* offers its own anti-spam solution.

The solution works with various platforms including *Microsoft Exchange* and *Lotus Notes*; we ran it as a virtual machine on an *ESXi* server. Set-up was easy and straightforward and the product was up and running almost immediately. An extensive web interface has a large number of bells and whistles for system administrators to play with – which would certainly help to fine-tune the product to a customer's needs.

As usual, we concentrated on the product's performance – which was good: an impressive 99.90% of all spam emails were blocked, while there were only three false positives. It will be interesting to see if the developers can reduce that number in the next test; the lack of missed newsletters shows that filtering legitimate email is certainly not a major issue for the product. A very well deserved VBSpam award goes to the industry's grandfather on its debut.

Kaspersky Anti-Spam 3.0

SC rate: 99.12%
FP rate: 0.00%
Final score: 99.12
Project Honey Pot SC rate: 99.25%
Abusix SC rate: 98.98%
Newsletters FP rate: 0.00%

Kaspersky's anti-spam solution has not missed a legitimate email in the last three tests, and none of the over 4,300 ham emails were blocked this time either. The product also correctly identified all newsletters as legitimate, and while the product's spam catch rate dropped a little, it remains very decent. The company's 13th VBSpam award is well deserved.

Libra Esva 2.0

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.89%
Abusix SC rate: 99.96%
SC rate pre-DATA: 98.50%
Newsletters FP rate: 0.5%

If the VBSpam test were a competition to achieve the highest final score, *Libra Esva* would be rather disappointed – having come in second place for the fourth time. However, we cannot stress strongly enough the importance of a product demonstrating a solid performance in multiple tests over time – as such, *Libra Esva*'s record is evidence of just how good a product it is. With no false positives and the fourth highest spam catch rate this month, the Italian product wins its ninth consecutive VBSpam award.

Mailshell Anti-Spam SDK

SC rate: 99.89%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.83%
Abusix SC rate: 99.95%
Newsletters FP rate: 0.00%

To say that *Mailshell* debuts in this test is perhaps not quite true. The product itself has not been tested before, but the company offers security solutions for OEMs, including DNS security, URL filtering and an anti-spam SDK. The latter has implicitly been tested through a number of other products that make use of it – but now it debuts on its own.

Mailshell Anti-Spam SDK was set up on a *Linux* server on our premises and plugged into *sendmail* as a 'milter'– this is one of several ways in which OEMs can use the product. It worked quickly and easily; in fact, we had more issues with setting up *sendmail* than with plugging *Mailshell* into it.

The product's performance was very good. *Mailshell* blocked an impressive 99.89% of spam. That, of course, is only half of the picture but the other half was equally good, if not better: no legitimate emails were missed, and no newsletters were missed either. With this month's fourth highest final score *Mailshell* earns its first VBSpam award as a product in its own right.

McAfee Email Gateway (formerly IronMail)

SC rate: 99.92%
FP rate: 0.19%
Final score: 99.00
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.97%
Newsletters FP rate: 3.4%

As is the case with all *McAfee* products, the spam catch rate of the *Email Gateway* appliance is very high, with the product missing fewer than one in 1,300 spam emails on this occasion. The downside is that the solution missed eight legitimate emails, and while

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
AnubisNetworks	4315	0	0.00%	97	171866	99.94%	99.94
BitDefender	4312	3	0.07%	311	171652	99.82%	99.47
FortiMail	4314	1	0.02%	439	171524	99.74%	99.63
GFI MailEssentials	4307	8	0.19%	557	171406	99.68%	98.75
Halon Security	4312	3	0.07%	488	171475	99.72%	99.37
IBM Lotus Protector	4312	3	0.07%	180	171783	99.90%	99.55
Kaspersky Anti-Spam 3.0	4315	0	0.00%	1515	170448	99.12%	99.12
Libra Esva	4315	0	0.00%	128	171835	99.93%	99.93
Mailshell	4315	0	0.00%	193	171770	99.89%	99.89
McAfee Email Gateway	4307	8	0.19%	129	171834	99.92%	99.00
McAfee EWS	4314	1	0.02%	177	171786	99.90%	99.78
McAfee SaaS	4310	5	0.12%	41	171922	99.98%	99.40
OnlyMyEmail	4313	2	0.05%	1	171962	100.00%	99.77
Sophos Email Appliance	4315	0	0.00%	177	171786	99.90%	99.90
SPAMfighter	4313	2	0.05%	884	171079	99.49%	99.25
SpamTitan	4313	2	0.05%	118	171845	99.93%	99.70
Spider Antispam	4315	0	0.00%	280	171683	99.84%	99.84
Symantec Messaging Gateway	4314	1	0.02%	247	171716	99.86%	99.74
The Email Laundry	4313	1	0.02%	272	171691	99.84%	99.72
Vade Retro	4312	3	0.07%	1027	170936	99.40%	99.06
Vamsoft ORF	4313	2	0.05%	1291	170672	99.25%	99.02
Spamhaus ZEN+DBL*	4315	0	0.00%	1858	170105	98.92%	98.92
SURBL*	4315	0	0.00%	62578	109385	63.61%	63.61

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

(Please refer to the text for full product names.)

that does not stop it from winning a VBSpam award, it does leave some room for improvement.

McAfee Email and Web Security Appliance

SC rate: 99.90%
FP rate: 0.02%
Final score: 99.78
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.96%
Newsletters FP rate: 3.9%

After skipping the previous test, *McAfee*'s *EWS* appliance returned this month and made sure its return did not go unnoticed: a spam catch rate of 99.90% was combined with missing just a single legitimate email. More than an average number of newsletters were missed, which is something the developers might want to look into, but with another VBSpam award in the bag, I'm sure they will be happy to do so.

McAfee SaaS Email Protection

SC rate: 99.98%
FP rate: 0.12%
Final score: 99.40
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.99%
Newsletters FP rate: 2.9%

McAfee's *SaaS* solution debuted in the previous test with a decent performance, but one which left some room for improvement. Happily, the product's performance did improve, with the spam catch rate (which was already high) increasing to the point where the product missed just 41 spam messages – fewer than all but one other product. It did miss five legitimate emails (and some newsletters too), so some improvement is still possible, but that is already a big leap forward from the previous test. The product earns its second VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.05%
Final score: 99.77
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 3.9%

In the previous test, *OnlyMyEmail*'s hosted solution missed just two out of more than 291,000 spam messages – an incredible performance, especially since it did not miss a single legitimate email. If possible, the product's spam catch rate was even better in this test with just one of more than 171,000 spam messages missed. Unlike the previous test, however, there were two missed legitimate emails and also eight newsletters that were blocked. This sees the product drop slightly in the final score table, but it was still a stunning performance and the product easily earns its sixth VBSpam award.

Sophos Email Appliance

SC rate: 99.90%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 99.83%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.00%

The significantly improved spam catch rate achieved by *Sophos*'s *Email Appliance* in the last test was not a one-off – this month the product managed to equal its last performance. What is more, the product missed no legitimate emails or newsletters, giving it the third highest final score this month and earning the company its 10th consecutive VBSpam award.

SPAMfighter Mail Gateway

SC rate: 99.49%
FP rate: 0.05%
Final score: 99.25
Project Honey Pot SC rate: 99.24%
Abusix SC rate: 99.75%
Newsletters FP rate: 7.2%

SPAMfighter missed 15 newsletters in this test – which is more than any other product. It is for the vendor's customers to decide whether or not that causes a problem – after all, several companies have a policy of blocking newsletters. What it does show is an area where the developers might want to focus their efforts. Meanwhile, the false positive rate decreased slightly and although the spam catch rate also dropped, the product's final score was well within the range to earn *SPAMfighter* its 12th consecutive VBSpam award.

SpamTitan

SC rate: 99.93%
FP rate: 0.05%
Final score: 99.70

	Newsletters		Project Honey Pot		Abusix		pre-DATA[§]		
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate			STDev[‡]
AnubisNetworks	1	0.5%	79	99.91%	18	99.98%			0.01
BitDefender	3	1.4%	185	99.79%	126	99.85%			0.31
FortiMail	7	3.4%	360	99.59%	79	99.91%			0.36
GFI MailEssentials	4	1.9%	480	99.45%	77	99.91%			0.36
Halon Security	3	1.4%	330	99.62%	158	99.81%			0.40
IBM Lotus Protector	0	0.0%	163	99.81%	17	99.98%			0.19
Kaspersky Anti-Spam	0	0.0%	653	99.25%	862	98.98%			1.56
Libra Esva	1	0.5%	93	99.89%	35	99.96%	2,585	98.50%	0.17
Mailshell	0	0.0%	148	99.83%	45	99.95%			0.19
McAfee Email Gateway	7	3.4%	105	99.88%	24	99.97%			0.18
McAfee EWS	8	3.9%	139	99.84%	38	99.96%			0.22
McAfee SaaS	6	2.9%	30	99.97%	11	99.99%			0.07
OnlyMyEmail	8	3.9%	1	100.00%	0	100.00%			0.01
Sophos Email Appliance	0	0.0%	148	99.83%	29	99.97%			0.18
SPAMfighter	15	7.2%	669	99.24%	215	99.75%			1.68
SpamTitan	6	2.9%	85	99.90%	33	99.96%			0.16
Spider Antispam	0	0.0%	237	99.73%	43	99.95%			0.33
Symantec Messaging Gateway	5	2.4%	119	99.86%	128	99.85%			0.32
The Email Laundry	3	1.4%	212	99.76%	60	99.93%	1,775	98.97%	0.26
Vade Retro	1	0.5%	880	98.99%	147	99.83%			0.75
Vamsoft ORF	2	1.0%	1051	98.80%	240	99.72%			0.63
Spamhaus ZEN+DBL[*]	0	0.0%	1313	98.50%	545	99.36%	2,975	98.27%	0.89
SURBL[*]	1	0.5%	53166	39.21%	9412	88.86%			16.85

[*] *Spamhaus and SURBL are both partial solutions and their performance is not to be compared to 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 except 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 the text for full product names.)

SpamTitan contd.

Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.96%
Newsletters FP rate: 2.9%

With minuscule improvements to both the spam catch rate and the false positive rate – and thus a small improvement to the final score as well – *SpamTitan*'s virtual solution put in an excellent performance. However, it is interesting to note that the product missed six newsletters – which is about the average, but is no doubt something the developers will want to improve. The product earns its 12th VBSpam award.

Spider Antispam

SC rate: 99.84%
FP rate: 0.00%
Final score: 99.84
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.95%
Newsletters FP rate: 0.00%

I like seeing new products join the test, but I look forward just as much to the second test for each new product, to see whether the developers have managed to improve their product's score based on the feedback we have given them. *Spider Antispam* did just that: the Czech product had no false positives in this test, missed no newsletters and also saw a significant improvement in its spam catch rate.

This all resulted in the fifth highest final score, a second VBSpam award, and good reason for the developers to celebrate.

Symantec Messaging Gateway 9.5 powered by Brightmail

SC rate: 99.86%
FP rate: 0.02%
Final score: 99.74
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.85%
Newsletters FP rate: 2.4%

As in the previous test, *Symantec Messaging Gateway* missed a single legitimate email, but the increased size of the ham corpus on this occasion means that its FP rate has dropped. With a spam catch rate almost equal to its last, it has a slightly improved final score and, with the handful of missed newsletters something for the developers to look into, another VBSpam award is added to *Symantec*'s tally, which now stands at 11.

The Email Laundry

SC rate: 99.84%
FP rate: 0.02%
Final score: 99.72
Project Honey Pot SC rate: 99.76%
Abusix SC rate: 99.93%
SC rate pre-DATA: 98.97%
Newsletters FP rate: 1.4%

In this test, *The Email Laundry* saw its spam catch rate improve and the details show that most of this improvement occurred pre-DATA, based on the IP address and domain of the sender. Moreover, the product also improved its false positive rate and with a significantly improved final score it wins its eighth consecutive VBSpam award.

Vade Retro Center

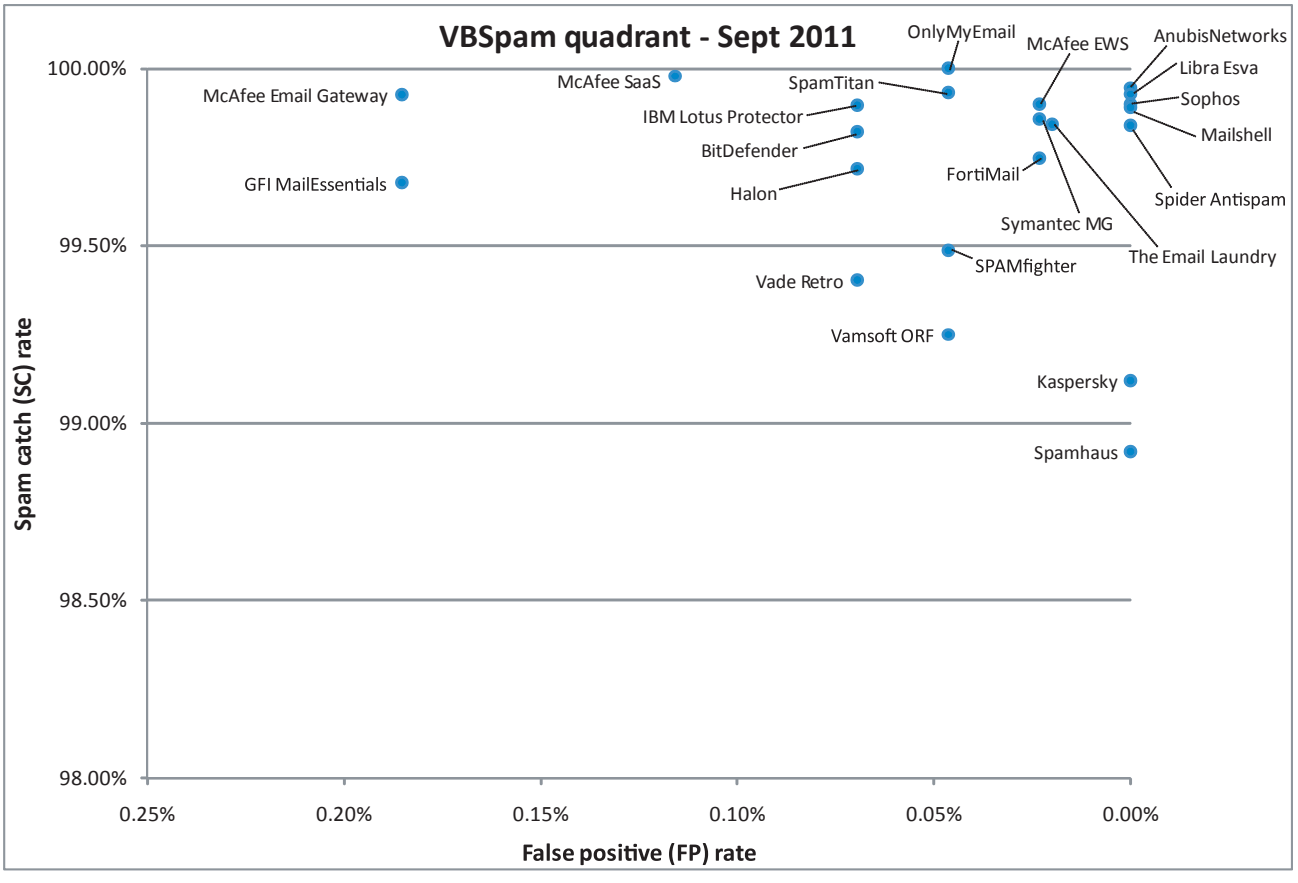
SC rate: 99.40%
FP rate: 0.07%
Final score: 99.06
Project Honey Pot SC rate: 98.99%
Abusix SC rate: 99.83%
Newsletters FP rate: 0.5%

Compared with the previous test, *Vade Retro* improved both its spam catch rate and its false positive rate. It missed only one newsletter and a significantly improved final score demonstrates that the product's developers are continuing to make improvements to their solution.

Vamsoft ORF

SC rate: 99.25%
FP rate: 0.05%
Final score: 99.02
Project Honey Pot SC rate: 98.80%
Abusix SC rate: 99.72%
Newsletters FP rate: 1.0%

Vamsoft prides itself on having very few false positives, and no doubt its developers will consider the two legitimate emails missed this month to be two too many. We like this attitude, and with a higher final score than last time (as both the FP rate



and the SC rate improved), and the product's ninth VBSpam award in as many tests, they will be motivated to make further improvements.

Spamhaus ZEN+DBL

SC rate: 98.92%
FP rate: 0.00%
Final score: 98.92
Project Honey Pot SC rate: 98.50%
Abusix SC rate: 99.36%
SC rate pre-DATA: 98.27%
Newsletters FP rate: 0.00%

In the previous test, one legitimate sender had found its IP address on *Spamhaus*'s blacklists, causing a number of false positives not just for the reputation list, but also for a number of products using it. I was pleased to see that this was not repeated – no legitimate emails or newsletters were missed in this test. On top of that, almost 99% of spam emails were blocked – a record for the product – and another VBSpam award is well deserved.

SURBL

SC rate: 63.61%
FP rate: 0.00%
Final score: 63.61
Project Honey Pot SC rate: 39.21%
Abusix SC rate: 88.86%
Newsletters FP rate: 0.5%

SURBL's performance depends not only on the quality of the URI blacklist itself, but also on the relative occurrence of emails with (detectable) URLs. With the proportion of those kind of emails increased in this month's spam corpus, it is not surprising that SURBL's spam catch rate improved. However, it was good to note that its catch rate also improved (by more than 2%) within the sub-category of emails containing URLs. No legitimate emails were misclassified, but one newsletter was blocked since it contained a URL on a blacklisted domain.

CONCLUSION

All participating full solutions achieved a VBSpam award, which means we handed out a record number of 22 awards

Products ranked by final score*	
AnubisNetworks	99.94
Libra Esva	99.93
Sophos Email Appliance	99.90
Mailshell	99.89
Spider Antispam	99.84
McAfee EWS	99.78
OnlyMyEmail	99.77
Symantec Messaging Gateway	99.74
The Email Laundry	99.72
SpamTitan	99.70
FortiMail	99.63
IBM Lotus Protector	99.55
BitDefender	99.47
McAfee SaaS	99.40
Halon Security	99.37
SPAMfighter	99.25
Kaspersky Anti-Spam 3.0	99.12
Vade Retro	99.06
Vamsoft ORF	99.02
McAfee Email Gateway	99.00
GFI MailEssentials	98.75

* *Full solutions only.*

(Please refer to the text for full product names.)

this month. This is good news and shows that there are many solutions available that prevent the vast majority of spam from entering organizations' networks, while blocking very few legitimate emails along the way.

Of course, that is only part of the story: the results show that products' performance can differ greatly in the details. The addition of the newsletter corpus provides some extra details that we are rather excited about. We will work hard on increasing the size of this corpus, even if that means many more hours of performing the rather tedious task of finding newsletters and subscribing to them.

The increased size of the ham corpus means that performance on this test set has gained some statistical significance. We are considering adding some extra weight to this corpus in the final score.

The next VBSpam test will run in October 2011, with the results scheduled for publication in November. 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/

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.