SEPTEMBER 2013

virus BULLETIN

Covering the global threat landscape

SEPTEMBER 2013 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

While I promise not to make a habit of using references to the British royal family in VBSpam introductions, I couldn't help but see a similarity between anti-spam testing and two events that occurred at Buckingham Palace earlier this month.

On 2 September, a man was found trespassing in the grounds of the supposedly well-guarded home of HRH Queen Elizabeth II[1]. Two days later, a man was apprehended by the police in the gardens of Buckingham Palace on suspicion of the same activity – in this case, however, it turned out to be the second son of the main residents of the palace, Prince Andrew, who had gone out for a stroll[2]. Both incidents caused significant public outcry.

It seems you can't have it both ways in protecting a palace – you can't make sure that no unauthorized people are able to come close to the queen's private quarters while at the same time always allowing those who have a legitimate reason for being there to walk around uninterrupted.

It's the same in spam filtering: you can't block all phishing emails and at the same time have all legitimate correspondence from financial institutions arrive in the user's inbox. You can't make sure that all genuine correspondence of a medical nature is sent to the intended recipient, while all *Viagra* spam is blocked.

Of course, a good palace guard is one that gets it right almost all of the time. Likewise, a good spam filter blocks almost all spam, while stopping very few legitimate emails.

In this VBSpam test, all but one of the 18 full solutions we tested achieved a VBSpam award for combining a high spam catch rate with a low false positive rate. Five of them stepped things up a notch, with a catch rate of more than 99.50% and no false positives at all, thus earning a VBSpam+ award.

[1] http://www.bbc.co.uk/news/uk-23999047
[2] http://www.bbc.co.uk/news/uk-24005811

THE TEST SET-UP

The VBSpam test methodology can be found at http://www.virusbtn.com/vbspam/methodology/. As usual, emails were sent to the products in parallel and in real time, and products were given the option to block email pre-DATA (that is, based on the SMTP envelope and before the actual email was sent). Three products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. As different products have different hardware requirements – not to mention those running on their own hardware, or those running in the cloud – there is little point comparing the memory, processing power or hardware the products were provided with; we followed the developers' requirements and note that the amount of email we receive is representative of that received by a smaller organization.

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 98:

$$SC - (5 \times FP) \geq 98$$

Meanwhile, those products that combine a spam catch rate of 99.50% or higher with a lack of false positives earn a VBSpam+ award.

As always, we stress that there is no objective justification for using the weight of 5 in the calculation of the final score: the spam catch and false positive rates are two distinct metrics of a spam filter and any way in which they are combined into a one-dimensional metric is arbitrary. We use the weight of 5 to highlight the importance of false positives, without false positives becoming the single metric that makes products pass or fail. Readers who prefer to use a different weight – or a different formula altogether – are

ISSN 1749-7027

encouraged to do so given the numbers presented in this report.

THE EMAIL CORPUS

Late summer is traditionally a busy time for the *Virus Bulletin* team, with our annual conference looming on the calendar in the early autumn. This year, we will be in Berlin, and I'm looking forward to a lot of the presentations on current threats. A number of those presentations will be on spam, or on threats for which email is the main delivery mechanism – highlighting the fact that stopping threats that are delivered through email remains an important part of an organization's defence.

However, not all threats are delivered by email, and of those that are, not all are successfully blocked by the spam filter. With this in mind, we have also been busy working on a web filter test, soon to be added to *Virus Bulletin*'s suite of security tests (the 'VBWeb' test). The test looks at products' abilities to block badness of various kinds delivered through HTTP, primarily at a network gateway. We are currently running a free trial, and developers of web filter solutions are encouraged to contact us if they are interested in submitting their product either for this trial or for the subsequent tests.

Back to the VBSpam test. Running a larger network isn't always a straightforward task, and a planned power outage on the last day of August took more time to recover from than expected (though both the IT team and the participating vendors were helpful in getting things back on track). In anticipation of the power outage, the test ran for 14 consecutive days rather than the usual 16 consecutive days. It started at 12am on Saturday 17 August and ended at the same time on Saturday 31 August. No network issues or other external factors impacted the test.

A total of 84,326 emails were sent as part of the test, 72,181 of which were spam. 60,565 of these were provided by *Project Honey Pot*, with the remaining 11,616 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 11,805 legitimate emails ('ham') and 340 newsletters.

As usual, we added a number of new sources of legitimate email to the test covering subjects ranging from open source computing to singer-songwriters – and as a result, despite the shorter test period, we had a slightly bigger ham corpus.

We also subscribed our test addresses to various new newsletters. Although not counting towards the final score, we see products struggling to filter these messages – each full solution incorrectly blocked at least one of the 340 legitimate newsletters.

We also made a small change to the rules regarding what is included in the VBSpam corpus.

Until now, we have always included everything that is delivered to us by the spam feed providers in the spam feed. After all, these are emails sent to addresses that aren't used by anyone, which means that the emails are not wanted by anyone. The ideal spam filter blocks exactly these – emails that are unwanted.

In practice, however, things are a little more complicated. People make typos. Spammers abuse social network invitations by having them sent to spam traps. Sloppy sender practices mean that emails that end up in spam traps may really be wanted by some of their recipients.

Following feedback both from a number of VBSpam participants and from readers of these reports, we decided to exclude some emails from the test. In particular, we have decided to exclude spam emails that are missed (i.e. marked as legitimate) by at least half the participating full solutions *and* which are not obviously spam. (The former rule means we use the wisdom of the crowd, while also making this workable for the testers, who don't have the manpower to verify tens of thousands of emails.)

Following the introduction of this rule, we took about a dozen emails out of the test. Its impact is thus minimal – yet

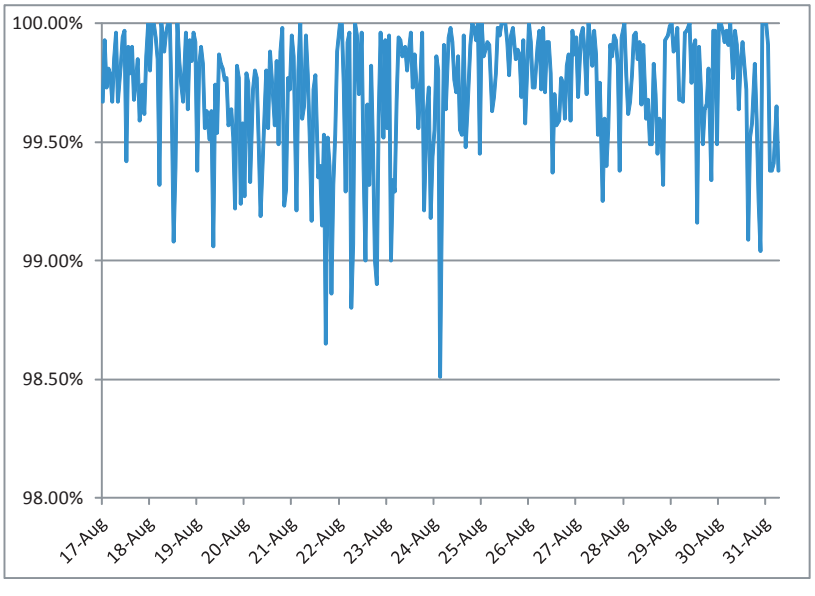


Figure 1: Spam catch rate of all complete solutions throughout the test period.

it means that participants are less likely to be 'punished' for decisions they make at their users' request.

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 rates have been excluded for each hour.

The fact that on several occasions, this 'corrected' average was 100% may in part be explained by the aforementioned new rule. Average catch rates were slightly higher during the second week, but spam remains volatile and there is no single campaign visible in the graph.

RESULTS

In the text that follows, '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 that has been erroneously marked by a product as spam.

Because the size of the newsletter corpus is significantly smaller than that of the ham corpus, a missed newsletter has a much greater effect on the newsletter false positive rate than a missed legitimate email has on the false positive rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of less than 0.01%, while one missed email in the newsletter corpus results in an FP rate of almost 0.3%).

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.94%
Newsletters FP rate: 2.1%

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Bitdefender	11805	0	0.00%	51	72125	99.93%	99.93
ESET	11803	2	0.02%	149	72027	99.79%	99.71
FortiMail	11805	0	0.00%	116	72060	99.84%	99.84
GFI	11801	4	0.03%	196	71980	99.73%	99.56
Halon Security	11793	12	0.10%	443	71733	99.39%	98.88
IBM	11801	2	0.02%	507	71669	99.30%	99.21
Kaspersky LMS	11802	3	0.03%	75	72101	99.90%	99.77
Libra Esva	11805	0	0.00%	53	72123	99.93%	99.93
Mailshell	11803	2	0.02%	120	72056	99.83%	99.75
McAfee Email Gateway	11799	6	0.05%	325	71851	99.55%	99.30
McAfee SaaS	11799	6	0.05%	151	72025	99.79%	99.54
Netmail Secure	11799	5	0.04%	151	72025	99.79%	99.58
OnlyMyEmail	11805	0	0.00%	0	72176	100.00%	100.00
Scrollout	11764	41	0.35%	222	71954	99.69%	97.96
Sophos	11803	2	0.02%	223	71953	99.69%	99.61
SpamTitan	11803	2	0.02%	325	71851	99.55%	99.47
Symantec	11802	3	0.03%	294	71882	99.59%	99.47
ZEROSPAM	11805	0	0.00%	135	72041	99.81%	99.81
Spamhaus ZEN+DBL*	11805	0	0.00%	5670	66506	92.14%	92.14
SURBL*	11805	0	0.00%	40015	32161	44.56%	44.56

* *Spamhaus* and *SURBL* are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

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

Never change a winning team or formula. *Bitdefender* has participated in every single VBSpam test since they started back in 2009, and we have been testing version 3.1.2 of the company's anti-spam solution since May 2012. The product has always performed well, achieving a VBSpam award in each of the last 26 tests, with an unbroken string of VBSpam+ awards throughout 2013.

Its run of success continues in this test, where the product achieves its fifth consecutive VBSpam+ award. *Bitdefender* missed just 51 spam emails in this month's spam corpus, with no false positives. There were a handful of false positives among the newsletters, including one email each from *LinkedIn* and *Twitter*, but even here the product did better than many others.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.79%
FP rate: 0.02%
Final score: 99.71
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.89%
Newsletters FP rate: 1.8%

In three of its last six test entries, *ESET* has achieved a VBSpam+ award, but on this occasion the product blocked two legitimate emails (from a new source), meaning that a fourth VBSpam+ award was not forthcoming.

Nevertheless, the product easily earns a standard VBSpam award with a performance that is not one to be ashamed of: *ESET* missed significantly fewer spam emails this time (those that were missed were mostly emails in Latin script) and saw a small increase in its final score. That fourth VBSpam+ award may be in the bag next time around.

Fortinet FortiMail

SC rate: 99.84%
FP rate: 0.00%
Final score: 99.84
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.5%

The last test was the 25th time that *Fortinet* had submitted its *FortiMail* appliance, and although it saw the product achieve its 25th VBSpam award, there was a slight glitch in its performance.

The results of this month's test demonstrate that the glitch was a one-off occurrence: not only did the catch rate increase to a pleasing 99.84%, but the appliance didn't block any of the more than 11,000 legitimate emails either. With the fourth highest final score this month, *FortiMail* wins its second VBSpam+ award.

GFI MailEssentials

SC rate: 99.73%
FP rate: 0.03%
Final score: 99.56
Project Honey Pot SC rate: 99.69%
Abusix SC rate: 99.91%
Newsletters FP rate: 1.8%

Going through the almost 200 spam emails missed by *GFI MailEssentials* in this test, I couldn't help but laugh at some of the gross misspellings in a few phishing emails. While such emails are unlikely to trick recipients, they still don't belong in inboxes. It is therefore good to know that these were the exceptions: *MailEssentials* missed only one in 368 spam emails in this test – about the same ratio as in the previous test.

There were four false positives, all of which were emails from sources that were added for this test, while the FP rate on the newsletter corpus was relatively low. In all, a decent performance from *GFI*, earning it its 15th consecutive VBSpam award.

Halon Security

SC rate: 99.39%
FP rate: 0.10%
Final score: 98.88
Project Honey Pot SC rate: 99.55%
Abusix SC rate: 98.51%
Newsletters FP rate: 3.8%

Halon's final score has been gradually falling in the past year – a trend that sadly continued in this test. Although the product's catch rate was higher than it has been since January, the virtual appliance missed more spam than most other products – many of the false negatives were messages in Japanese, Chinese and Russian. *Halon* also missed 12 legitimate emails – all of which were in English.

With a final score of just under 99, I think it's fair to say that *Halon*'s performance on this occasion doesn't live up to the excellent reputation the product has earned in previous VBSpam tests. However, it did achieve another VBSpam award – and *Halon*'s developers should be motivated to get their product climbing back up the ranks.

	Newsletters		Project Honey Pot		Abusix		Web hosts		pre-DATA†		STDev‡
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender	7	2.1%	44	99.93%	34	99.94%	30	99.86%			0.19
ESET	6	1.8%	136	99.78%	75	99.89%	83	99.69%			0.47
FortiMail	5	1.5%	114	99.81%	97	99.98%	102	99.60%			0.35
GFI	6	1.8%	186	99.69%	134	99.91%	115	99.44%			0.45
Halon Security	13	3.8%	270	99.55%	152	98.51%	245	99.37%			0.81
IBM	16	4.7%	497	99.18%	216	99.91%	423	99.10%			6.28
Kaspersky LMS	1	0.3%	62	99.90%	33	99.89%	403	99.86%			2.24
Libra Esva	8	2.4%	52	99.91%	36	99.99%	51	99.85%	7107	90.15%	0.35
Mailshell	7	2.1%	118	99.81%	67	99.98%	31	99.72%			0.26
McAfee Email Gateway	4	1.2%	283	99.53%	190	99.64%	62	99.21%			0.36
McAfee SaaS	90	26.5%	130	99.79%	51	99.82%	156	99.79%			0.57
Netmail Secure	7	2.1%	141	99.77%	104	99.91%	119	99.57%	7138	90.11%	0.63
OnlyMyEmail	29	8.5%	0	100.00%	0	100.00%	89	100.00%			0.38
Scrollout	46	13.5%	200	99.67%	160	99.81%	627	99.33%			1.32
Sophos	3	0.9%	221	99.64%	137	99.98%	0	99.43%			0.03
SpamTitan	6	1.8%	320	99.47%	253	99.96%	212	98.95%			0.61
Symantec	2	0.6%	285	99.53%	191	99.92%	186	99.21%			0.66
ZEROSPAM	13	3.8%	130	99.79%	107	99.96%	154	99.55%			0.52
Spamhaus ZEN+DBL*	0	0.0%	2715	95.52%	3960	74.56%	3794	83.52%	7375	89.78%	4.23
SURBL*	0	0.0%	33581	44.55%	15918	44.61%	18229	33.76%			17.48

* *Spamhaus* and *SURBL* are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

† pre-DATA filtering was optional and was applied on the full corpus. All of the false positives occurred post-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.*)

IBM Lotus Protector for Mail Security

SC rate: 99.30%
FP rate: 0.02%
Final score: 99.21
Project Honey Pot SC rate: 99.18%
Abusix SC rate: 99.91%
Newsletters FP rate: 4.7%

After missing out on a VBSpam award in July, the developers of *IBM Lotus Protector for Mail Security* have worked hard to make sure this wouldn't happen again. They were more than successful, as the product saw its false negative rate drop by more than half – many of the 500-odd emails that were missed were in foreign character sets. The false positive rate went down too and *IBM* only missed two legitimate emails, one in German and one in (Brazilian) Portuguese.

Both rates could certainly be improved upon a little further, but for now *IBM* lives up to its reputation of a trustworthy Internet company once again, and a VBSpam award is evidence of that.

Kaspersky Linux Mail Security 8.0

SC rate: 99.90%
FP rate: 0.03%

Kaspersky Linux Mail Security 8.0 contd.

Final score: 99.77
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.89%
Newsletters FP rate: 0.3%

Kaspersky's *Linux Mail Security* product missed only 75 spam emails in this test – fewer than most other products. Indeed, missing fewer than one in 950 spam emails, the product did even better than it has done in most previous tests.

On this occasion, however, the product incorrectly blocked three legitimate emails, so we weren't able to give *Kaspersky* another VBSpam+ award. A final score of 99.77 is nothing to be ashamed of, though. With just a single newsletter false positive (fewer than any other full solution) the product's eighth VBSpam award is well deserved.

Libra Esva 3.0.1

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.99%
SC rate pre-DATA: 90.15%
Newsletters FP rate: 2.4%

Only 53 spam emails slipped through *Libra Esva*'s grasp in this test, each of which was also missed by many other products – showing that there is very little room for improvement for the virtual solution. There certainly isn't any room for improvement when it comes to false positives, as once again there weren't any.

While one could be forgiven for thinking that developers at a company whose offices are located near Lake Como in Italy would spend a lot of their time enjoying the views, yet another stunning performance shows that they certainly don't. With another top-three performance, *Libra Esva* achieves its fourth VBSpam+ award.

Mailshell Mail Agent

SC rate: 99.83%
FP rate: 0.02%
Final score: 99.75
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.98%
Newsletters FP rate: 2.1%

Mailshell has submitted its SDK to half a dozen VBSpam tests, but the product the company submitted for this test is a new, soon to be released, hosted platform, where filtering takes place before the emails are delivered to the recipient's inbound mail server.

Different customers have different needs and there will be many for whom a hosted solution works best. What matters to us is how well the product blocks spam. *Mailshell Mail Agent* certainly does it well: it missed fewer than one in 600 spam emails. There were two false positives, both from the same (new) source, so there was no VBSpam+ award in the bag this time – but a final score of 99.75 shows that *Mailshell* continues to do a very good job.

McAfee Email Gateway 7.0

SC rate: 99.55%
FP rate: 0.05%
Final score: 99.30
Project Honey Pot SC rate: 99.53%
Abusix SC rate: 99.64%
Newsletters FP rate: 1.2%

I met a member of *McAfee*'s anti-spam team recently at an event in Vienna, so I was amused to see two spam emails missed by their *Email Gateway* appliance that advertised cruises in the Austrian capital. Against these two, and the 323 other missed spam emails, stood tens of thousands of emails that were blocked and that will have kept the security giant's customers protected against various threats.

There were six false positives this time, from four different senders, and four false positives in the newsletter corpus. With a decent performance, *McAfee* easily wins another VBSpam award.

McAfee SaaS Email Protection

SC rate: 99.79%
FP rate: 0.05%
Final score: 99.54
Project Honey Pot SC rate: 99.79%
Abusix SC rate: 99.82%
Newsletters FP rate: 26.5%

While the spam catch rates of most products remained more or less stable compared to the last test, *McAfee*'s hosted solution saw quite an increase in its catch rate. Among the 151 emails that were missed were quite a few in Chinese that may not be easy to filter in a context such as ours that includes legitimate Chinese email as well.

Six false positives (from three different senders) prevent the product from winning a VBSpam+ award, but it easily wins another VBSpam award – though I was a little disappointed

Complete solutions sorted by final score	
OnlyMyEmail	100.00
Bitdefender	99.93
Libra Esva	99.93
FortiMail	99.84
ZEROSPAM	99.81
Kaspersky LMS	99.77
Mailshell	99.75
ESET	99.71
Sophos	99.61
Netmail Secure	99.58
GFI	99.56
McAfee SaaS	99.54
Symantec	99.47
SpamTitan	99.47
McAfee Email Gateway	99.30
IBM	99.21
Halon Security	98.88
Scrollout	97.96

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

by the fact that more than one in four newsletters were erroneously blocked.

Messaging Architects Netmail Secure

SC rate: 99.79%
FP rate: 0.04%
Final score: 99.58
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.91%
SC rate pre-DATA: 90.11%
Newsletters FP rate: 2.1%

'How about a 58 percent [*sic*] increase?' some of the spam emails missed by *Netmail Secure* ask. There was no such increase for the virtual appliance, but at 99.79% its catch rate was already very good. Unlike in the previous test, there were a handful of false positives, all but one of which were from newly added sources.

This meant that the product missed out on a VBSpam+ award, but another VBSpam award is well deserved.

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.00%
Final score: 100.00
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 8.5%

While every anti-spam solution makes mistakes on occasion, *OnlyMyEmail*'s *Corporate MX-Defender* tends to make *very* few of them. In this test, it didn't make a single mistake in either the ham corpus or the spam corpus. And as if that wasn't impressive enough, I should point out that it would have achieved this even without the new rule that excluded some emails from the spam corpus.

It did make the wrong decision on 29 newsletters, but with such a good performance overall, this can be considered nothing more than a small detail. Another VBSpam+ award is very well deserved.

Scrollout F1

SC rate: 99.69%
FP rate: 0.35%
Final score: 97.96
Project Honey Pot SC rate: 99.67%
Abusix SC rate: 99.81%
Newsletters FP rate: 13.5%

The free and open source solution *Scrollout* continues to block a lot of spam emails – in this test it stopped all but one in 325 spam emails. Among those that were missed were a lot of emails from just a few senders – so perhaps some additional rules could improve the performance even further.

A bigger concern is the high false positive rate. Even after counting only four FPs per sender (which has long been the rule in VBSpam tests), we counted 41 of them – almost equal to the total number of false positives of the other products combined. Although some of these can be explained by the product blocking URLs that end in .exe (which may be disproportionately represented in our corpus) that is certainly not the only reason. As a result of its very high FP rate, *Scrollout*'s final score falls below the VBSpam threshold of 98 and thus fails to earn the product a VBSpam award.

Sophos Email Appliance

SC rate: 99.69%
FP rate: 0.02%
Final score: 99.61
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.9%

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	Multiple MX-records	Multiple locations
McAfee SaaS	McAfee	√	√	√	√	√
Mailshell	Optional		√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	√	√
ZEROSPAM	ClamAV			√	√	√

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	Interface			
					CLI	Desktop GUI	Web GUI	API
Bitdefender	Bitdefender	√			√		√	
ESET	ESET Threatsense				√	√		
FortiMail	Fortinet	√	√	√	√		√	
GFI	Five anti-virus engines	√		√			√	
Halon Security	Commtouch; Kaspersky; ClamAV; HRPS	√	√	√			√	√
IBM	Sophos; IBM Remote Malware Detection			√	√		√	
Kaspersky LMS	Kaspersky	√		√	√		√	
Libra Esva	ClamAV; others optional		√	√	√		√	
McAfee Email Gateway	McAfee	√	√	√	√	√	√	
Netmail Secure	Proprietary	√	√	√	√		√	
Scrollout	ClamAV			√	√		√	
Sophos	Sophos						√	
SPAMfighter	VIRUSfighter (optional)	√	√	√			√	
SpamTitan	Kaspersky; ClamAV	√	√	√	√		√	√
Symantec	Symantec	√	√	√	√		√	

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

Sophos's *Email Appliance* saw its false positive number halve from four to two – and both of these were from the same sender. At the same time, there was a significant increase in the product's spam catch rate, which reached 99.69%.

As a consequence, the product's final score increased significantly too and it easily earned another VBSpam award. The product also stood out as having one of the lowest false positive rates in the newsletter corpus.

SpamTitan 5.11

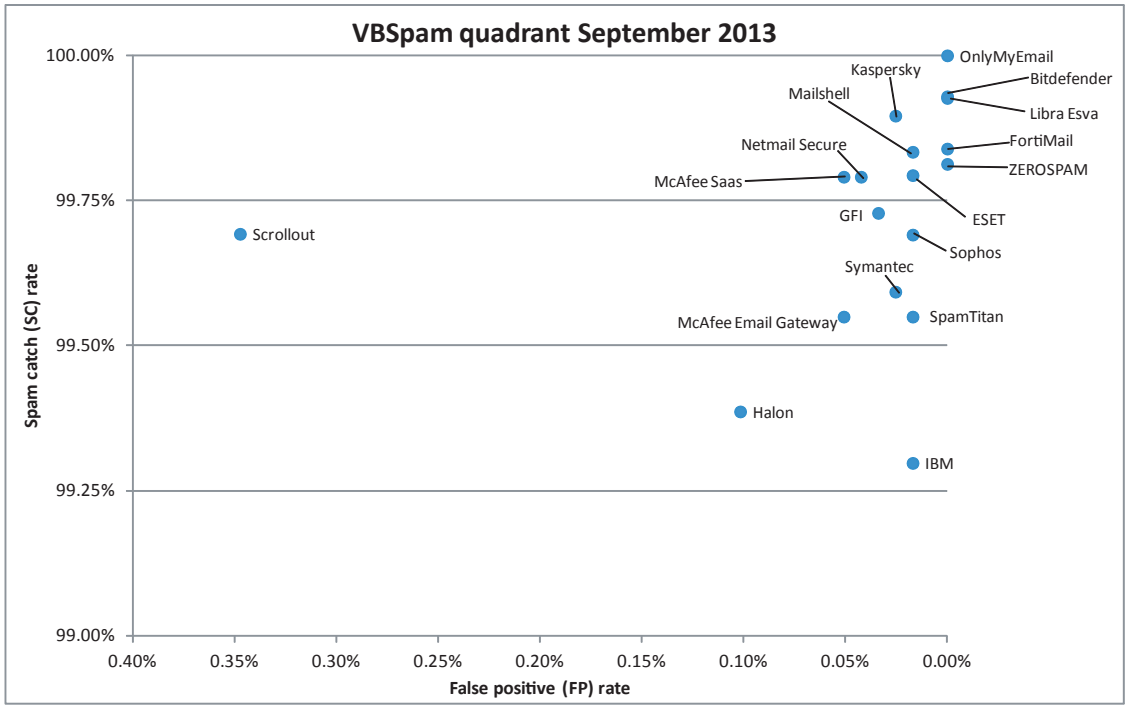
SC rate: 99.55%
FP rate: 0.02%
Final score: 99.47
Project Honey Pot SC rate: 99.47%
Abusix SC rate: 99.96%
Newsletters FP rate: 1.8%

With a catch rate of 99.55% there's little reason for customers of *SpamTitan* to be unhappy with the product's performance, but the appliance (we tested the virtual version) has seen a slow and steady decline in its performance throughout the year. Of course we hope to see this trend reversed – and the fact that a lot of the missed spam was in Romance languages like French or Spanish may help the developers achieve that.

Thankfully, the false positive rate remained low (there were only two false positives) and thus the product's final score was sufficient for it to achieve another VBSpam award – it now has two dozen.

Symantec Messaging Gateway 10.0

SC rate: 99.59%
FP rate: 0.03%
Final score: 99.47



(Please refer to text for full product names.)

Symantec Messaging Gateway 10.0 contd.

Project Honey Pot SC rate: 99.53%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.6%

Unlike in the last test, there were some false positives for *Symantec Messaging Gateway* this time – though their number (three) remained low. The number of false positives among newsletters was also low – lower than all but one other full solution.

The product's catch rate remained stable at just above 99.5% – among the spam that was missed were a fair number of emails from Latin America. The false positives prevented *Symantec* from earning a VBSpam+ award this time, but it achieved a VBSpam award without difficulty.

ZEROSPAM

SC rate: 99.81%
FP rate: 0.00%
Final score: 99.81
Project Honey Pot SC rate: 99.79%
Abusix SC rate: 99.96%
Newsletters FP rate: 3.8%

At 99.81%, *ZEROSPAM*'s spam catch rate is already higher than that of many other products, but looking at the missed spam it may be that a little less tolerance for email from certain hosting providers could be an easy means of increasing it further.

There is no room for improvement on the false positive side of things though, as there were none – and with the fifth highest final score this month it wins its second VBSpam+ award.

Spamhaus ZEN+DBL

SC rate: 92.14%
FP rate: 0.00%
Final score: 92.14
Project Honey Pot SC rate: 95.52%
Abusix SC rate: 74.56%
SC rate pre-DATA: 89.78%
Newsletters FP rate: 0.0%

Although we saw a decline in *Spamhaus*'s catch rate starting about a year ago, it now seems to have stabilized at a little above 90 per cent. This suggests that, while spammers may have had some success avoiding blacklisted (or blacklist-able) IP addresses and domains, they can

only do so to a certain extent, and *Spamhaus*'s service continues to block well over 90% of spam.

False positives were absent in this test, even among the newsletters, and again may provide a reality check for email marketers, some of whom believe that *Spamhaus* is unfairly strict against them.

SURBL

SC rate: 44.56%
FP rate: 0.00%
Final score: 44.56
Project Honey Pot SC rate: 44.55%
Abusix SC rate: 44.61%
Newsletters FP rate: 0.0%

Decreases in *SURBL*'s spam catch rate have been explained in the past by the fact that spammers are doing a better job at using legitimate domains in the emails they send. This trend may have been reversed a little, as *SURBL*'s catch rate increased by more than 13 percentage points this month.

This shows that blocking bad domains remains an effective way to stop a significant chunk of spam – especially since yet again there were no false positives. It also shows that the members of *SURBL*'s team haven't given up trying to distinguish the good from the bad domains – and they deserve praise for that.

CONCLUSION

The VBSpam tests remain proof of the fact that spam is generally dealt with rather well – after all, we won't even consider a product that doesn't block at least 98% of spam for the VBSpam stamp of approval. However, the devil remains in the details: if email security products didn't block such a high percentage of spam, email would be unusable. The difference between a spam catch rate of 99%, 99.5% and 99.9% is therefore bigger than the numbers might suggest.

This test mostly showed that trends we have seen in previous tests have continued and that, at least for now, filters' catch rates have generally stabilized. We will, of course, continue to look at how these trends develop. At the same time, we're working on some new additions to the tests, to enhance the picture they give even further.

The next VBSpam test will run in October 2013, 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: Dr Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Scott James

Sales Executive: Allison Sketchley

Perl Developer: Tom Gracey

Consulting Editors:
Nick FitzGerald, *AVG, NZ*
Ian Whalley, *Google, USA*
Dr Richard Ford, *Florida Institute of Technology, USA*

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/