MAY 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MAY 2015

INTRODUCTION

At *Virus Bulletin*, we consider ourselves a serious company and we refrain from using sensationalist headlines despite knowing that they would draw more attention to the reports we publish. We also take the long view, regularly pointing out that it is the performance of products *over several tests* that really matters.

Bearing this in mind, I would like to warn against reading too much into the drop in the average spam catch rate this month from 99.82 to 99.60 per cent – or a 120% increase in the amount of spam missed.

Spam is notoriously volatile and so are spam filters, although the latter are orders of magnitude more reliable. It could be a simple matter of bad luck (or good luck, if you're a spammer) that caused the drop in this month's catch rates.

A 99.60% catch rate is still high, and the main takeaway from many years of running comparative spam filter tests – which is that spam filters are doing a pretty good job at mitigating the spam problem – remains true. The drop in catch rates is interesting nevertheless, and another reason to look forward to the next test to see whether the trend continues or reverses.

Despite the drop in catch rate, all but one of the 16 full solutions submitted this month achieved a VBSpam award, while four of them achieved a VBSpam+ award.

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). However, on this occasion no 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 small organization.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the weighted false positive (WFP) rate. The WFP rate is defined as the false positive rate of the ham and newsletter corpora taken together, with emails from the latter corpus having a weight of 0.2:

WFP rate = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #newsletters)

Products earn VBSpam certification if the value of the final score is at least 98:

SC - (5 x WFP) ≥ 98

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives and no more than 2.5% false positives among the newsletters earn a VBSpam+ award.

THE EMAIL CORPUS

The test started on Saturday 25 April at 12am and finished 16 days later, on Monday 11 May at 12am. On this occasion there were no serious issues affecting the test.

The test corpus consisted of 140,653 emails. 129,351 of these emails were spam, 65,007 of which were provided by *Project Honey Pot*, with the remaining 64,344 spam emails

ISSN 1749-7027

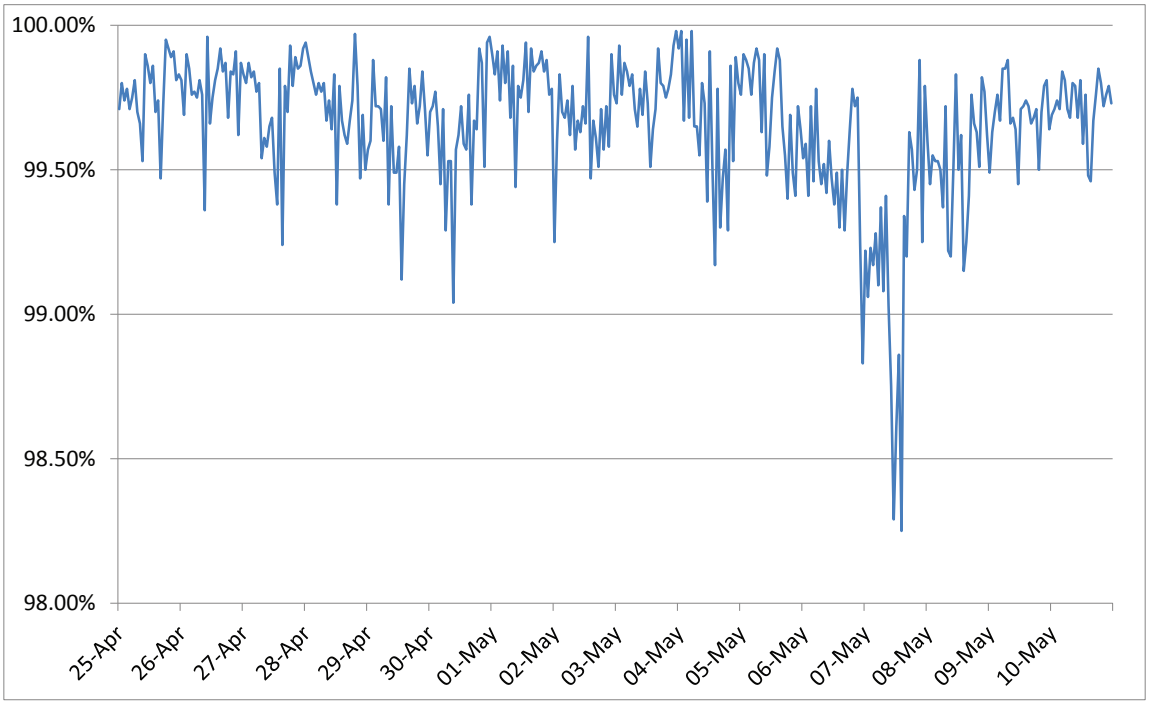


Figure 1: Spam catch rate of all full solutions throughout the test period.

provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 10,966 legitimate emails ('ham') and 336 newsletters.

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.

Two things are clear from this graph. The first is that the average catch rate was significantly lower on this occasion than in the last test. Indeed, the average false negative rate (the percentage of spam that was missed) was more than twice as high as it was two months ago: 0.40% compared with 0.18%. Many products contributed to this overall increase, with three products seeing their catch rate drop by more than 0.7 percentage points.

The second notable thing in the graph is the drop in the catch rate towards the end of the second week. Interestingly, on inspection of the spam emails that were causing problems for several filters at this time, many of them proved to be part of a campaign that seemed broken in a number of ways (e.g. including a single link going to a nonsensical *Google* search) and which attempted to push health-related products.

Sometimes spammers just get lucky, even if their spam is horribly broken. Thankfully, in this case the broken link would have meant that, despite getting their emails delivered, the spammers' luck didn't pay off.

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' refers to a message in that corpus that has been erroneously marked by a product as spam.

Axway MailGate 5.3.1

SC rate: 99.69%
FP rate: 0.21%
Final score: 98.47
Project Honey Pot SC rate: 99.45%
Abusix SC rate: 99.93%
Newsletters FP rate: 6.0%

While most products saw their spam catch rates decrease in this test, there was a small increase for *Axway*'s *MailGate* product, which blocked a little more spam than it did in March – and more than the average product in this test.

Unfortunately, the product's false positive rate also increased – from zero to 0.21%. This sharp increase was

the result of 23 erroneously blocked legitimate emails, most of which were in English with a couple in (Brazilian) Portuguese. The rise in FP rate meant that the product's final score dropped to well below 99. Nevertheless, it was still high enough for *Axway* to earn another VBSpam award.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.94%
FP rate: 0.04%
Final score: 99.76
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.0%

For *Bitdefender*, the spam that appeared to be more difficult for other products to block in this test wasn't an issue: the product (we run the *Linux* version) even increased its catch rate a little to 99.94%. Most of the spam that it did miss was pharma-spam.

However, the product wasn't able to retain a clean sheet: four legitimate emails were missed, all from the same sender and all discussing the same open-source project. This meant that, despite achieving the fifth highest final score, the product's developers had to be content with 'just' a standard VBSpam award this time – which continues an unbroken run of 37 such awards since the very first VBSpam test.

Egedian Mail Security

SC rate: 99.06%
FP rate: 0.00%
Final score: 99.02
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 98.27%
Newsletters FP rate: 1.2%

Like several other products this month, *Egedian* saw a fairly significant drop in its spam catch rate, although the product still blocked more than 99 out of every 100 spam emails.

What was nice, though, was that for the first time since joining the tests a year ago, the virtual solution didn't block a single legitimate email – which is no trivial achievement given the international corpus we use for that test. This is a nice step forward and might eventually lead to a VBSpam+ award. For now, the product earns its fifth VBSpam award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.69%
FP rate: 0.00%
Final score: 99.67
Project Honey Pot SC rate: 99.65%
Abusix SC rate: 99.72%
Newsletters FP rate: 0.6%

ESET saw a relatively big drop in its spam catch rate, mostly due to two spam campaigns in Japanese and English. Yet at 99.69%, the spam catch rate remains a little higher than average.

What is more, *ESET* once again didn't block a single email from the ham feed and only blocked two newsletters (which were in Finnish and Russian). This was enough to earn the product its ninth VBSpam+ award.

Fortinet FortiMail

SC rate: 99.94%
FP rate: 0.02%
Final score: 99.81
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.2%

Among the handful of products that saw their catch rates improve in this test, *Fortinet*'s increase was the largest. It also saw a small decrease in its false positive rate, with only two legitimate emails blocked this time.

This means that the appliance comes to the end of its sixth year of VBSpam testing with another VBSpam award and the third highest final score.

GFI MailEssentials

SC rate: 99.09%
FP rate: 0.03%
Final score: 98.89
Project Honey Pot SC rate: 98.75%
Abusix SC rate: 99.44%
Newsletters FP rate: 2.1%

After earning a VBSpam+ award in March, this test was a slight disappointment for *GFI*, which missed five times as many spam emails and also saw both its false positive rate and its newsletter false positive rate increase.

But then, spam is volatile and spam filters can have a bad day – or even a bad two-week period. And it's worth noting

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	10943	23	0.21%	399	128952	99.69%	98.47
Bitdefender	10962	4	0.04%	84	129267	99.94%	99.76
Egedian	10966	0	0.00%	1217	128134	99.06%	99.02
ESET	10966	0	0.00%	407	128944	99.69%	99.67
FortiMail	10964	2	0.02%	78	129273	99.94%	99.81
GFI	10963	3	0.03%	1178	128173	99.09%	98.89
IBM	10966	0	0.00%	237	129114	99.82%	99.82
Kaspersky LMS	10966	0	0.00%	181	129170	99.86%	99.86
Libra Esva	10961	5	0.05%	23	129328	99.98%	99.74
McAfee SaaS	10966	0	0.00%	1397	127954	98.92%	98.87
Netmail Secure	10966	0	0.00%	778	128573	99.40%	99.33
OnlyMyEmail	10962	4	0.04%	2	129349	99.998%	99.799
Scrollout	10940	26	0.24%	1404	127947	98.91%	97.12
Sophos	10965	1	0.01%	273	129078	99.79%	99.74
SpamTitan	10966	0	0.00%	559	128792	99.57%	99.55
ZEROSPAM	10963	3	0.03%	152	129199	99.88%	99.72
Spamhaus DBL*	10966	0	0.00%	112032	17319	13.39%	13.39
Spamhaus ZEN*	10966	0	0.00%	7204	122147	94.43%	94.43
Spamhaus ZEN+DBL*	10966	0	0.00%	5042	124309	96.10%	96.10

**The Spamhaus products are partial solutions and their performance should not be compared with that of other products. (Please refer to the text for full product names and details.)*

that the final score of the *Windows*-based product remained well above the VBSpam threshold, and as such it adds its 25th VBSpam award to its collection.

IBM Lotus Protector for Mail Security

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Project Honey Pot SC rate: 99.70%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.0%

IBM's anti-spam solution achieved VBSpam+ awards in the two last tests, but it has never before done so with a full 'clean sweep'. This time, however, the product didn't miss any legitimate emails in the ham corpus or any in the newsletters corpus either, and there was only a small decrease in the product's spam catch rate.

This is thus a really good result for the industry giant, which not only wins its third VBSpam+ award for the *Lotus Protector for Mail Security* product, but does so with the second highest final score.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.86%
FP rate: 0.00%
Final score: 99.86
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.78%
Newsletters FP rate: 0.0%

There were only two products with a 'clean sheet' – a lack of false positives in both the ham and newsletters corpora – and of those, *Kaspersky* had the highest spam catch rate. This means that had this test had a single winner, it would have been the company's *Linux Mail Server* product.

	Newsletters		Project Honey Pot		Abusix		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	
Axway	20	6.0%	355	99.45%	44	99.93%	0.43
Bitdefender	0	0.0%	19	99.97%	65	99.90%	0.2
Egedian	4	1.2%	106	99.84%	1111	98.27%	1.04
ESET	2	0.6%	230	99.65%	177	99.72%	0.48
FortiMail	4	1.2%	62	99.90%	16	99.98%	0.16
GFI	7	2.1%	815	98.75%	363	99.44%	0.83
IBM	0	0.0%	198	99.70%	39	99.94%	0.27
Kaspersky LMS	0	0.0%	37	99.94%	144	99.78%	0.38
Libra Esva	1	0.3%	21	99.97%	2	100.00%	0.08
McAfee SaaS	5	1.5%	609	99.06%	788	98.78%	0.85
Netmail Secure	8	2.4%	543	99.16%	235	99.63%	0.58
OnlyMyEmail	2	0.6%	2	99.997%	0	100.00%	0.02
Scrollout	78	23.2%	97	99.85%	1307	97.97%	1.14
Sophos	1	0.3%	241	99.63%	32	99.95%	0.29
SpamTitan	2	0.6%	93	99.86%	466	99.28%	0.65
ZEROSPAM	3	0.9%	137	99.79%	15	99.98%	0.23
Spamhaus DBL*	0	0.0%	49902	23.24%	62130	3.44%	4.12
Spamhaus ZEN*	0	0.0%	5660	91.29%	1544	97.60%	3.16
Spamhaus ZEN+DBL*	0	0.0%	3598	94.47%	1444	97.76%	2.68

** The Spamhaus products are partial solutions and their performance should not be compared with that of other products.*

† 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.)

Of course, this also means that the product achieved this month's highest final score and a VBSpam+ award (its fourth in a row) to boot.

Libra Esva 3.4.1.0

SC rate: 99.98%
FP rate: 0.05%
Final score: 99.74
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%

After years of testing the company's 32-bit solution, the end-of-life of that version prompted *Libra Esva*'s developers to ask us to install the 64-bit version of the product, which we happily did. Installation of the virtual machine was as easy as it had been for the 32-bit version years ago, and the 64-bit version blocked an impressive 99.98% of spam – something we have come to expect from the Italian product.

However, unlike in most of the previous tests, there were five false positives, meaning we were not able to award *Libra Esva* a VBSpam+ award this time. With a final score of 99.75, a standard VBSpam award is still well deserved though.

McAfee SaaS Email Protection

SC rate: 98.92%
FP rate: 0.00%
Final score: 98.87
Project Honey Pot SC rate: 99.06%
Abusix SC rate: 98.78%
Newsletters FP rate: 1.5%

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

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

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

Local solutions						Interface			
	Anti-malware	IPv6	DKIM	SPF	DMARC	CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender; ClamAV	√				√		√	√
ESET	ESET Threatsense					√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Netmail Secure	Proprietary	√	√	√		√		√	
Scrollout	ClamAV			√		√		√	
Sophos	Sophos		√	√				√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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

The drop in the spam catch rate for *McAfee*'s *SaaS* email solution was a little more than one percentage point and greater than that of any other solution. However, in this case it may have been a feature rather than a bug as the product also saw its false positive rate drop to zero.

While we provide the final score to give readers some guidance, we always make it clear that different organizations have different priorities when it comes to false positives and false negatives, and for many an organization, *McAfee*'s choices may well be the right ones, despite the drop in its final score.

Such organizations will be pleased to note that once again the cloud-based solution earns a VBSpam stamp of approval.

Netmail Secure

SC rate: 99.40%
FP rate: 0.00%
Final score: 99.33
Project Honey Pot SC rate: 99.16%
Abusix SC rate: 99.63%
Newsletters FP rate: 2.4%

Yet again this month, I noticed a lot of spam emails in East-Asian languages among those missed by *Netmail*'s virtual appliance – though as always, this is an observation rather than a judgement.

What we do judge products on is the catch rate, which in *Netmail*'s case was 0.3 percentage points lower than it was

Products ranked by final score	
Kaspersky LMS	99.86
IBM	99.82
FortiMail	99.81
OnlyMyEmail	99.80
Bitdefender	99.76
Libra Esva	99.74
Sophos	99.74
ZEROSPAM	99.72
ESET	99.67
SpamTitan	99.55
Netmail Secure	99.33
Egedian	99.02
GFI	98.89
McAfee SaaS	98.87
Axway	98.47
Scrollout	97.12

in March, on this occasion falling below 99.5%. This was a shame, as the lack of false positives and the low newsletter FP rate meant that it would otherwise have achieved a VBSpam+ award. Nevertheless, the product's developers should be pleased with a standard VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.998%
FP rate: 0.04%
Final score: 99.799
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.6%

Some things one never gets used to. *OnlyMyEmail*'s spam catch rate yet again falls within a rounding error of 100%: the product missed just two spam emails, both promising the same 'good news' – an email address was provided to learn what that good news actually was.

The product was a little unfortunate when it comes to the ham feed: a small configuration change caused four false positives from the same sender in short succession. This did prevent the Michigan-based cloud provider from earning another VBSpam+ award, but with the fourth highest final score a standard VBSpam award is very well deserved.

Scrollout F1

SC rate: 98.91%
FP rate: 0.24%
Final score: 97.12
Project Honey Pot SC rate: 99.85%
Abusix SC rate: 97.97%
Newsletters FP rate: 23.2%

Scrollout F1 failed to achieve a VBSpam award in three out of the last four tests and unfortunately, this test was the same. Both the spam catch rate and the false positive rate were worse than that of any other product and the final score failed to reach the threshold of 98.

However, there may be some light at the end of the tunnel. Not only did the final score increase a fair bit, but I have spoken to the developers of the open source solution and discovered that the product might have issues reading the correct source of emails in our lab environment. Fingers crossed that this will turn out to have been the issue and there will be a brighter future ahead for *Scrollout*.

Sophos Email Appliance

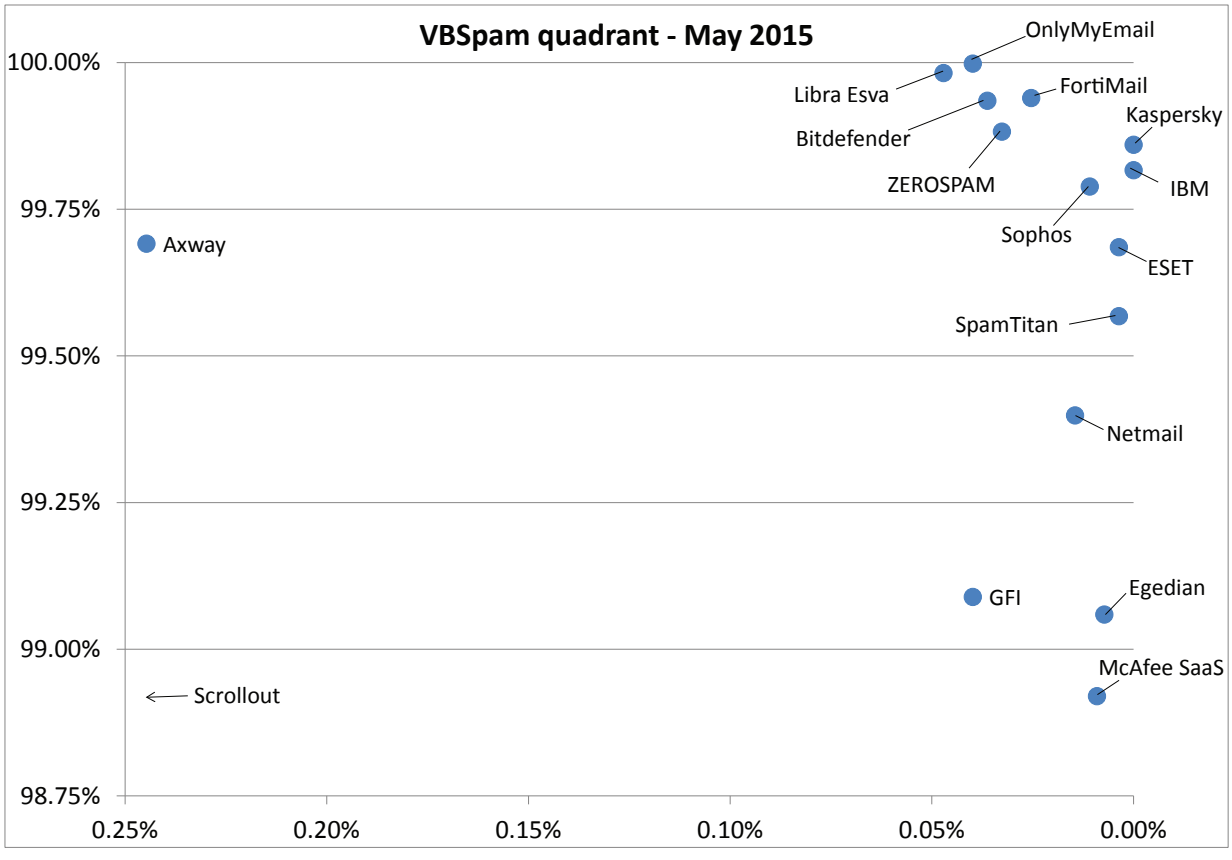
SC rate: 99.79%
FP rate: 0.01%
Final score: 99.74
Project Honey Pot SC rate: 99.63%
Abusix SC rate: 99.95%
Newsletters FP rate: 0.3%

Sophos turns 30 this year, making it one of the stalwarts of the security industry. Combined under the slogan 'security made simple', the vendor offers many solutions, of which one is the *Email Appliance*.

Making sure as few spam emails end up in the inbox as possible helps to keep things simple and with 30 VBSpam awards in as many participations thus far, *Sophos* certainly does a good job there. In this test, while a single misclassified legitimate email prevented the product from achieving a VBSpam+ award, it performed better than average on all counts, easily earning its 31st VBSpam award.

SpamTitan 6.00

SC rate: 99.57%
FP rate: 0.00%
Final score: 99.55
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.28%
Newsletters FP rate: 0.6%



The drop in *SpamTitan*'s catch rate was greater than that of the average product in this test – it mostly missed dating and pharma-spam – but I wouldn't want to call that a disappointment: the product also saw its false positive rate drop to zero, with just two missed newsletters.

As the spam catch rate remained above 99.5%, we are pleased to be able to give *SpamTitan* its sixth VBSpam+ award.

ZEROSPAM

SC rate: 99.88%
FP rate: 0.03%
Final score: 99.72
Project Honey Pot SC rate: 99.79%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.9%

I have referred to the volatility of spam several times in this review. It is one of the reasons why we run a comparative test as, in a way, the relative performance of a product compared to other products matters more than absolute performance – even if, of course, it's the latter that's experienced by the users.

ZEROSPAM did better than average in all areas, which means that this test was a win for the product despite the fact that three false positives meant we couldn't give it that VBSpam+ award all participants are aiming for. However, the product's 20th VBSpam award is well deserved.

Spamhaus DBL

SC rate: 13.39%
FP rate: 0.00%
Final score: 13.39
Project Honey Pot SC rate: 23.24%
Abusix SC rate: 3.44%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 94.43%
FP rate: 0.00%
Final score: 94.43
Project Honey Pot SC rate: 91.29%
Abusix SC rate: 97.60%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 96.10%
FP rate: 0.00%
Final score: 96.10
Project Honey Pot SC rate: 94.47%
Abusix SC rate: 97.76%
Newsletters FP rate: 0.0%

In the last couple of tests, *Spamhaus* saw a number of 'false positives' in its DBL domain-blocklist. I put quotes around 'false positives' here as they were actually caused by domains belonging to URL-shorteners, which do give a positive response when queried against the list, but *Spamhaus* has since told us that this particular return code should be used for scoring rather than for outright blocking.

Set up accordingly, none of the products had any false positives and a combination of the blacklists blocked more than 96 per cent of emails – once again showing how valuable a service like *Spamhaus* could be for doing the dirty work in your spam filter.

CONCLUSION

As I said in the introduction, I would be wary of drawing too many conclusions based on the low catch rates in this test: much of this may be caused by the natural volatility of spam. Still, it isn't good news either, and we hope that the next test will see catch rates bounce back.

The next VBSpam test will run in June 2015 (and is about to start at the time of writing this report), with the results scheduled for publication in July. Developers interested in submitting products should email martijn.grooten@virusbtn.com.