MARCH 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MARCH 2015

INTRODUCTION

This month we complete six years of comparative anti-spam testing. Actually, it is six years and a month – a number of issues have caused this report to be delayed by several weeks, so I will keep the introduction short.

In these six years we have seen the spam landscape change in a number of ways. Firstly, while most spam continues to be sent from compromised machines, these days, those machines are often compromised *Linux* servers rather than hijacked *Windows* PCs. It's no longer your grandparents' *XP* machine that is responsible for the sending of spam, but your geeky cousin's web server.

Secondly, spammers are using more and more hijacked resources, from webmail accounts – an example of which we saw in this test – to domains. This makes it a lot harder for a spam filter to be absolutely certain that an email is spam.

I have said on a number of occasions in these reports that spam as a problem is actually very well mitigated: the threat of spam making email unusable doesn't seem particularly realistic at the moment. Still, being mitigated successfully isn't the same as being solved; hence we continue to need spam filters as much as before.

With our VBSpam setup, we continue to provide customers with information on which products perform particularly well. At the same time, we help developers of those products to make their products better.

Sixteen full solutions and a number of DNS-based blacklists were submitted for this test. All but one of the full solutions achieved a VBSpam award, and seven 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, no products chose to make use of this option on this occasion.

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 14 February at 12am and

ISSN 1749-7027

finished 16 days later, on Monday 3 March at 12am. This time there were no serious issues affecting the test.

The test corpus consisted of 136,904 emails. 126,046 of these emails were spam, 61,519 of which were provided by *Project Honey Pot*, with the remaining 64,527 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 10,549 legitimate emails ('ham') and 309 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.

One immediately notices that there were a few periods during the test where the average performance was rather poor. In fact, this was the result of a single spam campaign (see Figure 2), which caused problems for almost all products in the test.

The campaign targets users in Germany and isn't too hard to spot as job recruitment spam. In fact, the promise of receiving a fair amount of money in return for very little work suggests that the spammers are looking for money mules.

What makes these emails difficult to filter is that they were sent from *Outlook.com* accounts that were likely generated for the purpose (rather than taken over from actual users).

Figure 2: A single spam campaign targeting German users caused problems for almost all products in the test.

Although we estimate that at least tens of thousands of email addresses were used in this campaign, this might be a small enough number to stay under the radar of both *Microsoft*'s outbound spam filters and most inbound filters like the ones in this test.

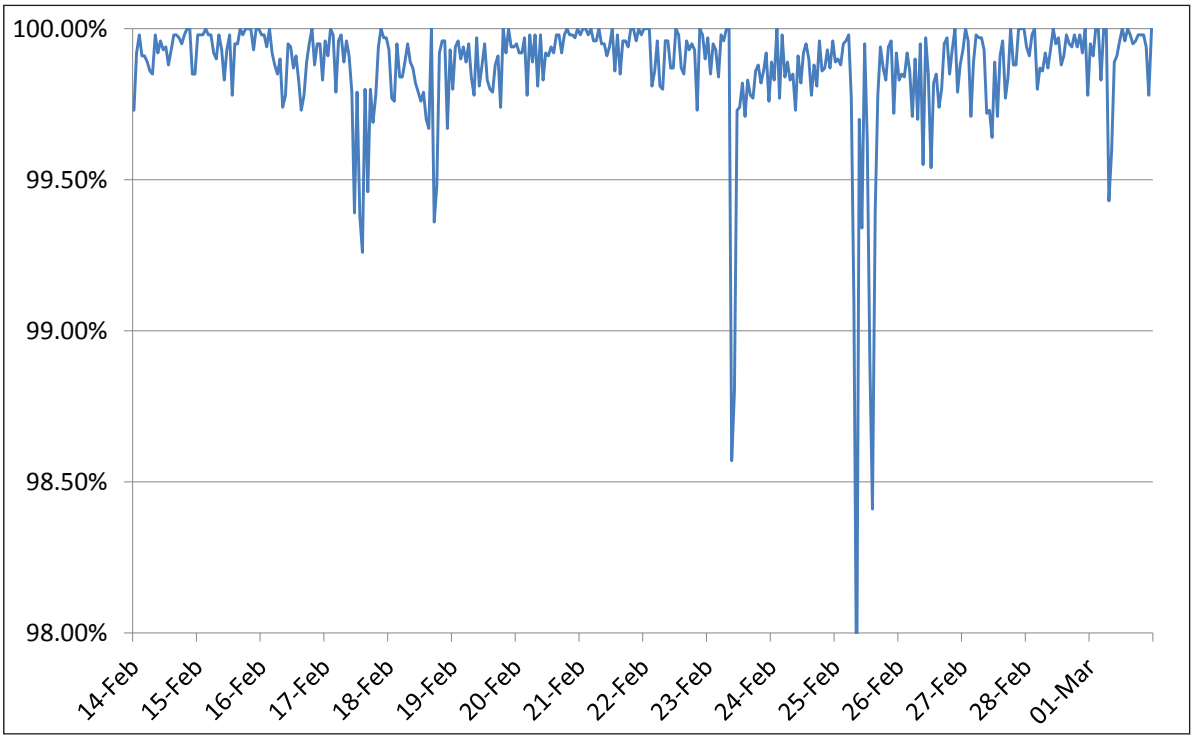


Figure 1: Spam catch rate of all full solutions throughout the test period.

RESULTS

Axway MailGate 5.3.1

SC rate: 99.67%
FP rate: 0.03%
Final score: 99.42
Project Honey Pot SC rate: 99.56%
Abusix SC rate: 99.78%
Newsletters FP rate: 3.9%

Compared to the previous test, *Axway*'s *MailGate* virtual appliance saw its spam catch rate decrease slightly. What stood out among the missed spam were a few campaigns in (Brazilian) Portuguese, as well as a campaign in which the subject lines were two random English words and the content was nothing but a link to a page on a compromised website.

At 99.67%, the product still blocked more than 299 out of every 300 spam emails. There were three false positives, so the clean sheet it achieved in the last test wasn't repeated, but the newsletter false positive rate went down. All in all, *Axway* fully deserves yet another VBSpam award, this one completing a full year of such awards.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.86%
Newsletters FP rate: 0.3%

The last test saw *Bitdefender* missing out on a VBSpam+ award for the first time in more than two years. That appears only to have been a temporary glitch though, as on this occasion the Romanian product yet again avoided false positives, while missing only one email in the newsletter category: a notification from *Twitter*.

The spam catch rate did drop a little – most interesting among the 117 missed spam emails were several where the payload seemed to be missing – but at 99.91% remained very high. Not only does *Bitdefender* complete six full years of testing without missing a single VBSpam award, the company also achieves its 13th VBSpam+ award.

Egedian Mail Security

SC rate: 99.84%
FP rate: 0.08%
Final score: 99.42
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.84%
Newsletters FP rate: 1.6%

Egedian has had a bit of an unlucky run recently, missing out on a VBSpam award twice in a row, first due to a high false positive rate and then because the product's spam catch rate dropped significantly. It's third time lucky for the French product though; or rather, the developers worked hard to get things right this time.

There were only 200 missed spam emails – most of which were emails that were missed by the majority of solutions – while neither the false positive rate nor the number of newsletters were too high. Hence *Egedian* is well deserving of a VBSpam award this time.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.92%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.96%
Newsletters FP rate: 1.0%

ESET's commendable performance in the last review was not a one-off occurrence, as this test shows. Yet again, the *Exchange*-based product didn't miss any legitimate emails, while only three newsletters were erroneously blocked.

At the same time, there were only 107 emails among the eclectic mix of missed spam – a small improvement compared to the previous test. Thus another VBSpam+ award – already the product's eighth – goes to *ESET*.

Fortinet FortiMail

SC rate: 99.86%
FP rate: 0.03%
Final score: 99.70
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.88%
Newsletters FP rate: 0.7%

The VBSpam history for *Fortinet*'s *FortiMail* appliance goes all the way back to the second test we ever ran, in June 2009, and we have run the very same appliance in all 35 tests. In none of these tests has *FortiMail* missed out on a VBSpam award, and since the introduction

Product name	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	10546	3	0.03%	416	125630	99.67%	99.42
Bitdefender	10549	0	0.00%	117	125929	99.91%	99.90
Egedian	10541	8	0.08%	200	125846	99.84%	99.42
ESET	10549	0	0.00%	107	125939	99.92%	99.89
FortiMail	10546	3	0.03%	177	125869	99.86%	99.70
GFI	10549	0	0.00%	233	125813	99.82%	99.82
IBM	10549	0	0.00%	191	125855	99.85%	99.84
Kaspersky LMS	10549	0	0.00%	33	126013	99.97%	99.97
Libra Esva	10549	0	0.00%	68	125978	99.95%	99.93
McAfee SaaS	10537	12	0.11%	41	126005	99.97%	99.38
Netmail Secure	10549	0	0.00%	380	125666	99.70%	99.63
OnlyMyEmail	10547	2	0.02%	4	126042	100.00%	99.91
Scrollout	10488	61	0.58%	1026	125020	99.19%	95.73
Sophos	10545	4	0.04%	260	125786	99.79%	99.60
SpamTitan	10541	8	0.08%	133	125913	99.89%	99.45
ZEROSPAM	10548	1	0.01%	170	125876	99.87%	99.80
Spamhaus DBL*	10483	66	0.63%	53358	72688	57.67%	54.54
Spamhaus ZEN*	10549	0	0.00%	11612	114434	90.79%	90.79
Spamhaus ZEN+DBL*	10483	66	0.63%	5072	120974	95.98%	92.85

**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.)*

of the VBSpam+ awards a few years ago, the product has snatched up a few of those too.

In the last test, it was a relatively high number of false positives among the newsletters that prevented the product from winning another VBSpam+ award. That wasn't a problem this time – there were only two misclassifications – but three false positives in the ham corpus meant that yet again, we had to deny the product a VBSpam+ award. However, with a spam catch rate of more than 99.85%, *FortiMail* had no problem achieving its 15th VBSpam award.

GFI MailEssentials

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Project Honey Pot SC rate: 99.72%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.0%

This month, *GFI MailEssentials* completes two dozen participations in the VBSpam test. The product has never failed to achieve a VBSpam award, and recently has found itself among the better performers.

In this test, *MailEssentials* missed 233 spam emails – resulting in a decent spam catch rate of 99.82% – and that's all that went wrong: it was one of only two products that had no false positives in either the ham corpus or the newsletter corpus. Another VBSpam+ award for *GFI*'s Maltese developers – their sixth already – is thus very well deserved.

IBM Lotus Protector for Mail Security

SC rate: 99.85%
FP rate: 0.00%
Final score: 99.84
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%

	Newsletters		Project Honey Pot		Abusix		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	
Axway	12	3.9%	273	99.56%	143	99.78%	1.62
Bitdefender	1	0.3%	26	99.96%	91	99.86%	0.35
Egedian	5	1.6%	99	99.84%	101	99.84%	0.35
ESET	3	1.0%	82	99.87%	25	99.96%	0.2
FortiMail	2	0.7%	97	99.84%	80	99.88%	0.34
GFI	0	0.0%	170	99.72%	63	99.90%	0.35
IBM	1	0.3%	177	99.71%	14	99.98%	0.34
Kaspersky LMS	0	0.0%	25	99.96%	8	99.99%	0.13
Libra Esva	2	0.7%	22	99.96%	46	99.93%	0.28
McAfee SaaS	3	1.0%	38	99.94%	3	100.00%	0.13
Netmail Secure	7	2.3%	298	99.52%	82	99.87%	0.47
OnlyMyEmail	0	0.0%	4	99.99%	0	100.00%	0.04
Scrollout	75	24.3%	430	99.30%	596	99.08%	0.85
Sophos	0	0.0%	169	99.73%	91	99.86%	0.39
SpamTitan	7	2.3%	60	99.90%	73	99.89%	0.22
ZEROSPAM	2	0.7%	92	99.85%	78	99.88%	0.38
Spamhaus DBL*	2	0.7%	17683	71.26%	35675	44.71%	9.88
Spamhaus ZEN*	0	0.0%	9961	83.81%	1651	97.44%	2.99
Spamhaus ZEN+DBL*	2	0.7%	3909	93.65%	1163	98.20%	1.76

**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.)

IBM's *Lotus Protector* product missed fewer than 200 spam emails in this test, and it was interesting to see a fair amount of duplicates among those emails. We don't give discounts for duplicates – after all, part of the problem of spam is its volume – but even with those duplicates, a 99.85% spam catch rate is very good.

What's more, *IBM* didn't miss a single legitimate email, and only missed one newsletter. Not only does that mean the industry giant achieves its second VBSpam+ award, but it does so with its best final score to date.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.97%

FP rate: 0.00%

Final score: 99.97

Project Honey Pot SC rate: 99.96%

Abusix SC rate: 99.99%

Newsletters FP rate: 0.0%

The last test was a good one for *Kaspersky*'s *Linux Mail Server* product, as it combined a total lack of false positives with a spam catch rate of over 99.9%, but in this test it outdid itself. Yet again, the solution didn't miss a single email from either the ham or the newsletter corpus, and it combined this with missing only 33 spam emails (about half of which were written in Japanese).

Clearly, this means that yet another VBSpam+ award is earned by *Kaspersky*, and the fact that it finished this test with the highest final score adds a little extra glitter to that award.

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	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						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.)

Libra Esva 3.4.1.0

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.7%

Libra Esva missed 68 spam emails in this test. That's more than the virtual appliance has missed in a while, but almost all of these were also missed by most other products. Moreover, the virtual appliance didn't block a single legitimate email (yet again).

Add to that only two blocked newsletters – one from the US and one from Belgium – and with a second highest final score, *Libra Esva* completes its first full dozen VBSpam+ awards.

McAfee SaaS Email Protection

SC rate: 99.97%
FP rate: 0.11%
Final score: 99.38
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 100.00%
Newsletters FP rate: 1.0%

Missing just 40 spam emails – fewer than all but two other solutions – the spam catch rate of *McAfee*'s *SaaS* solution was even higher than it was in the last test and certainly impressive.

Against this stood 12 false positives from six senders, which is on the high side, especially given how well most products have been dealing with the ham feed in recent tests. Nevertheless, the product still achieves a VBSpam award without any difficulty.

Netmail Secure

SC rate: 99.70%
FP rate: 0.00%
Final score: 99.63
Project Honey Pot SC rate: 99.52%
Abusix SC rate: 99.87%
Newsletters FP rate: 2.3%

There was a small decrease in the spam catch rate for *Netmail Secure* this month, but nothing really to worry about. Yet again I noticed spam in East Asian languages being prevalent among those spam emails that made it past the spam filter.

More importantly, *Netmail* didn't block any emails from the ham corpus, while the newsletter false positive rate decreased a little (interestingly, all but one of the missed newsletters were sent through *MailChimp*), which meant that *Netmail Secure* earned a VBSpam+ award this time.

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.02%
Final score: 99.91
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%

It has been a while (November 2013, to be precise) since *OnlyMyEmail* last blocked an email from the ham corpus. This month, it blocked two, albeit both from the same sender.

That is neither worrying nor shocking, especially as the product didn't block any newsletters and only missed four out of more than 125,000 emails from the spam feed – and these were in fact four instances of the same email. There may be no VBSpam+ award for the Michigan-based hosted solution this time, but with the third highest final score in the test, the product's developers have plenty to be pleased about.

Scrollout F1

SC rate: 99.19%
FP rate: 0.58%
Final score: 95.73
Project Honey Pot SC rate: 99.30%
Abusix SC rate: 99.08%
Newsletters FP rate: 24.3%

Scrollout F1 is a free and open source anti-spam solution, one that we have been testing for a little over four years. It has picked up several VBSpam awards along the way, but showed some issues in the last test, in particular a high false positive rate.

This time, things actually got a little worse. More than one in every 200 legitimate emails was blocked by the product, while the spam catch rate fell too. 99.19% might not be too bad for a catch rate, but it was by far the lowest among participating solutions. We hope that some changes made to the product's settings will be able to turn the tide for the next test; this time, we couldn't give *Scrollout* a VBSpam award.

Sophos Email Appliance

SC rate: 99.79%
FP rate: 0.04%
Final score: 99.60
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.86%
Newsletters FP rate: 0.0%

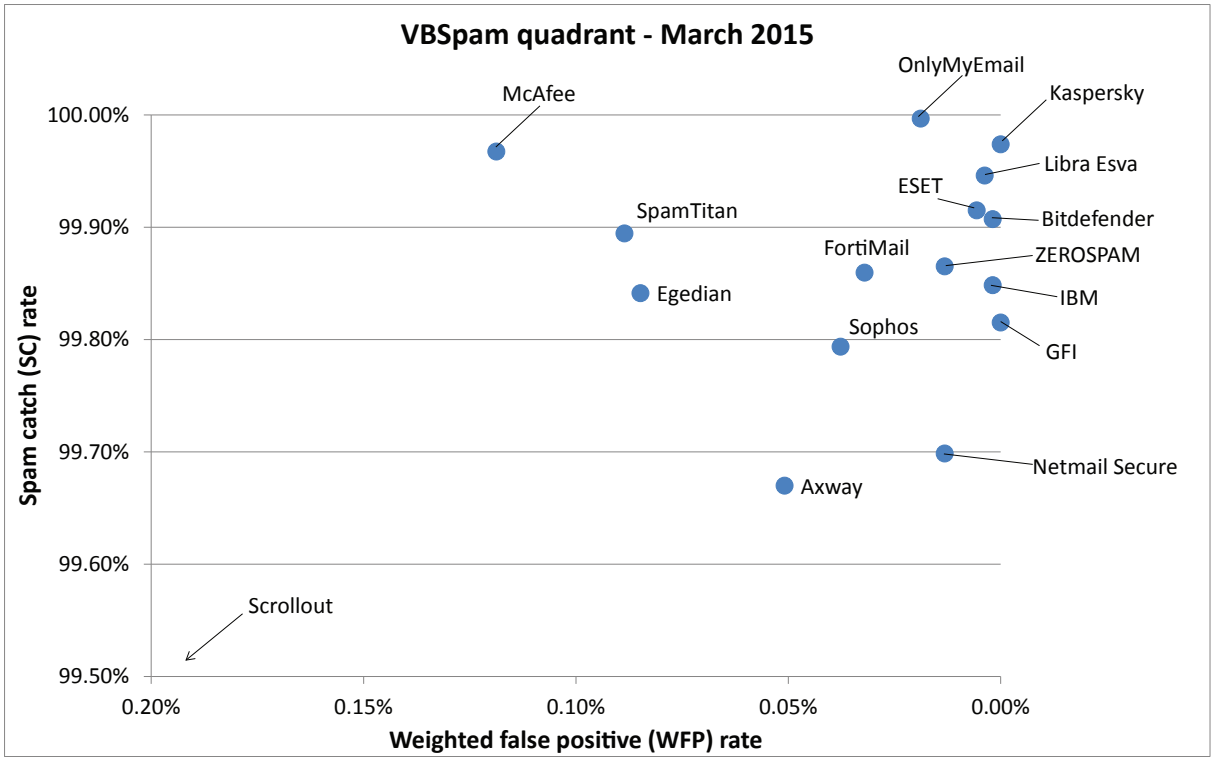
Sophos's *Email Appliance* has traditionally been strong when it comes to avoiding false positives among newsletters; in fact, in this test it avoided them altogether, while erroneously blocking four legitimate emails.

The latter means we couldn't give *Sophos* a VBSpam+ award, but with an overall decent performance, the appliance continues its unbroken run of more than 30 VBSpam awards.

SpamTitan 6.00

SC rate: 99.89%
FP rate: 0.08%
Final score: 99.45
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.89%
Newsletters FP rate: 2.3%

A low catch rate meant that, earlier this year, *SpamTitan* missed its first VBSpam award in more than five years of VBSpam participation. In this test, the Irish virtual solution proved that this was really a one-off thing: the product missed just 133 spam emails – a catch rate of almost 99.9% – among which several fake tax refund emails stood out the most.



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

There were also eight false positives – all in English – which means that there was no VBSpam+ award this time, but the product's 32nd VBSpam award is as well deserved as ever.

ZEROSPAM

SC rate: 99.87%
FP rate: 0.01%
Final score: 99.80
Project Honey Pot SC rate: 99.85%
Abusix SC rate: 99.88%
Newsletters FP rate: 0.7%

In the VBSpam test, we take a liberal view of emails: if a real person meant to send an email – and if the recipient opted in to receiving it – we think it acceptable for the email to be included in the test, even if it didn't follow best practices. This was certainly the case for the single false positive for *ZEROSPAM* in this test: an email from Costa Rica which was sent from an IP address without a valid PTR record.

ZEROSPAM doesn't earn another VBSpam+ award, but with just 170 missed spam emails, the hosted solution that operates from Canada easily wins its 19th VBSpam award in as many tests.

Spamhaus DBL

SC rate: 57.67%
FP rate: 0.63%
Final score: 54.54
Project Honey Pot SC rate: 71.26%
Abusix SC rate: 44.71%
Newsletters FP rate: 0.7%

Spamhaus ZEN

SC rate: 90.79%
FP rate: 0.00%
Final score: 90.79
Project Honey Pot SC rate: 83.81%
Abusix SC rate: 97.44%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 95.98%
FP rate: 0.63%

Products ranked by final score	
Kaspersky Security 8 for Linux Mail Server	99.97
Libra Esva 3.4.1.0	99.93
OnlyMyEmail's Corporate MX-Defender	99.91
Bitdefender Security for Mail Servers 3.1.2	99.90
ESET Mail Security for Microsoft Exchange Server	99.89
IBM Lotus Protector for Mail Security	99.84
GFI MailEssentials	99.82
ZEROSPAM	99.80
Fortinet FortiMail	99.70
Netmail Secure	99.63
Sophos Email Appliance	99.60
SpamTitan 6.00	99.45
Egedian Mail Security	99.42
Axway MailGate 5.3.1	99.42
McAfee SaaS Email Protection	99.38
Scrollout F1	95.73

Final score: 92.85

Project Honey Pot SC rate: 93.65%

Abusix SC rate: 98.20%

Newsletters FP rate: 0.7%

It has been mentioned in these reports before that URL shorteners are a huge pain for spam filters in general and domain-based blocklists in particular: they are commonly used in spam to hide the real destination of a link, but are also occasionally used by legitimate senders to make the links in their emails look prettier.

The high false positive rate for the *Spamhaus DBL* – and thus also for the combined *ZEN+DBL* list – was largely due to such shorteners. Thankfully, the blacklist sends a special response for such URLs, so administrators who include the *DBL* in their anti-spam solution could easily prevent such URLs from being blocked. This might of course come at the cost of some extra false negatives.

Of course, some may opt only to use the IP-based blacklists combined in *ZEN*. It is worth noting that those lists didn't have any false positives, yet still blocked more than nine out of ten spam emails based on the sending IP address alone.

CONCLUSION

With one exception, this test once again demonstrated how well anti-spam solutions block spam. However, the dozens of emails sent from specially created *Outlook.com* accounts show that there remain options for spammers to bypass most spam filters, even if these options might not scale too well.

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

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/