MAY 2016

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MAY 2016

Martijn Grooten & Ionuţ Răileanu

INTRODUCTION

Since we first started the VBSpam tests in the spring of 2009, we have run 44 official VBSpam tests, each covering a period of about two weeks.

Yet, in the periods between these tests our lab has been just as active, with thousands of emails continuing to flow through the products in real time. We have been using these between-test periods to provide those participating in the VBSpam tests (as well as a number of other companies that have asked us to measure the performance of their products on a consultancy basis) with feedback on what kind of emails have been misclassified by their products. For many participants, this regular feedback is just as valuable as the reports themselves, which demonstrate to the wider community how well the products have performed.

At the end of this month's test, however, we took a short break in order to move all our test machines to a brand new lab, which should allow the VBSpam tests to grow in both size and depth. This accounts for the delay in the publication of this report, as well as the fact that it is slightly shorter than previous ones.

A total of 16 full email security (or anti-spam) solutions took part in this test, all of which achieved VBSpam certification. Six of them performed well enough to earn the VBSpam+ accolade.

THE TEST SET-UP

The VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/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)

Final score = SC - (5 x WFP)

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

Extra criteria based on the speed of delivery of emails in the ham corpus were not included on this occasion, as a number of network issues meant we could not be 100 per cent confident about the accuracy of the speed measurements. However, we believe that the awards achieved would have been unchanged had speed data been included.

THE EMAIL CORPUS

The test ran for 18 days, from 12am on 23 April to 12am on

ISSN 1749-7027

11 May 2016 – slightly longer than normal to account for some interruptions as described below.

The test corpus consisted of 169,565 emails. 160,426 of these emails were spam, 78,612 of which were provided by *Project Honey Pot*, with the remaining 81,814 spam emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 8,803 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 noticeable from this graph. The first is that spam catch rates remain very high, although slightly lower than in the last test.

The second noticeable thing is a number of small gaps: these concerned hours during which testing conditions weren't optimal, leading us to exclude the corresponding emails from the test. As our goal is to measure accurately and realistically rather than to run an always-on system of mail servers, this is not an issue, though we did extend the test by two days to make up the numbers.

The performance of some filters dropped slightly albeit noticeably on the evening of 4 May, but this appeared to have been caused by a number of unrelated emails rather than by a single campaign.

Although participating products all performed very well, some spam emails were missed, among which were some with malicious content. Of course, given the prevalence of the ransomware threat, this is something users are extremely concerned about. In future tests, we will be examining the ability of products to block this type of email in particular.

RESULTS

Three products – the *OnlyMyEmail* hosted email solution, *ESET Mail Security for Microsoft Exchange*, and *Fortinet*'s *FortiMail* appliance – achieved a final score that, rounded to two decimals, would be 100. Each of these products had no false positives, not even among the newsletters, and missed just one, two and five spam emails respectively.

Clearly, these three products achieved a VBSpam+ award, as did *IBM*, *Bitdefender* and *Libra Esva*. The remaining 10 products all achieved a VBSpam award; in many cases, it was just a single false positive that stood in the way of them achieving a VBSpam+ award. For detailed descriptions of the products, we refer to previous test reports.

Regular readers of these reports will notice the appearance of *Trustwave*'s *Secure Email Gateway* product. This is a

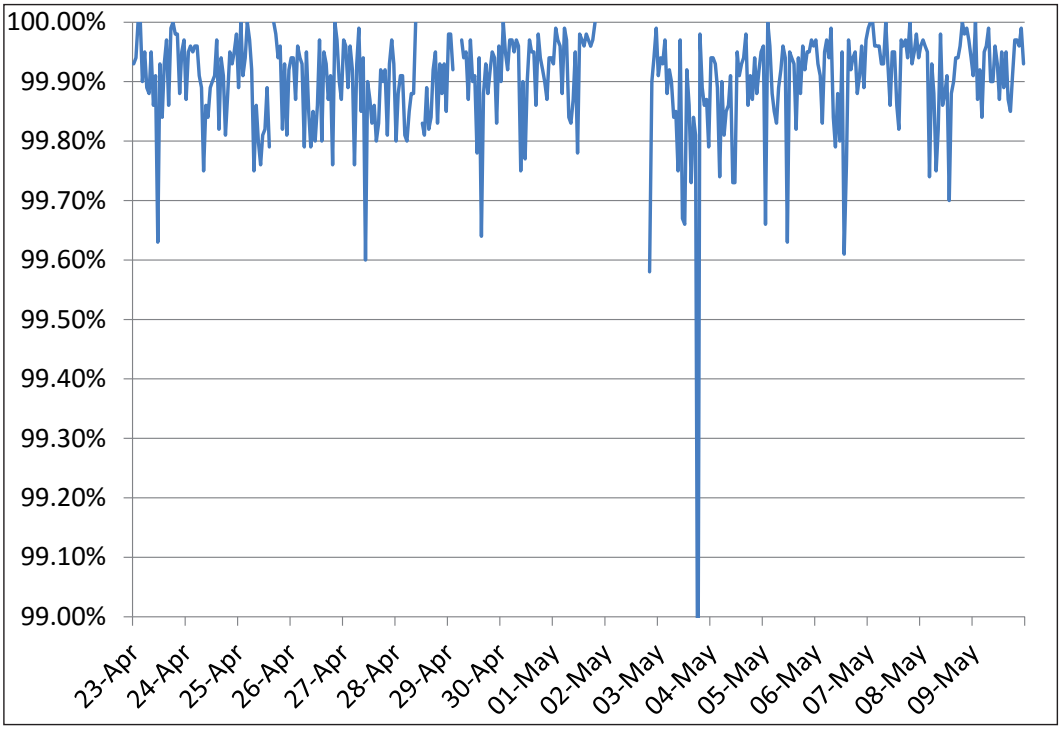


Figure 1: Spam catch rate of all full solutions throughout the test period.

new participant – although a previous incarnation of the same product impressed us with its performance in the very early VBSpam tests. The product runs on *Windows* and with a very good catch rate came within a whisker (that is, within one false positive) of a VBSpam+ award.

IBM's *X-Force API* is also new to the test. The product is an IP blacklist, which queried the sending IP address of every email and made its blocking decision based solely on that. Therefore it entered the test as a partial solution, whose performance shouldn't be compared with those of full solutions and not necessarily even with those of other partial solutions. Still, even outside of that context, blocking almost 97 per cent of emails based on the IP address is pretty impressive.

FULL SOLUTIONS

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.6%

Egedian Mail Security

SC rate: 99.95%
FP rate: 0.01%
Final score: 99.87
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.6%

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%

Fortinet FortiMail

SC rate: 99.997%
FP rate: 0.00%

Fortinet FortiMail contd.

Final score: 99.997
Project Honey Pot SC rate: 99.995%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.0%

GFI MailEssentials

SC rate: 99.55%
FP rate: 0.23%
Final score: 98.31
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.38%
Newsletters FP rate: 3.0%

IBM Lotus Protector for Mail Security

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.0%

Kaspersky Linux Mail Security 8.0

SC rate: 99.90%
FP rate: 0.01%
Final score: 99.84
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%

Kaspersky Secure Mail Gateway

SC rate: 99.88%
FP rate: 0.01%
Final score: 99.82
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%

Libra Esva 3.7.0.0

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%

Netmail Secure

SC rate: 99.97%
FP rate: 0.03%
Final score: 99.78
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.6%

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%

Sophos Email Appliance

SC rate: 99.79%
FP rate: 0.01%
Final score: 99.74
Project Honey Pot SC rate: 99.60%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%

SpamTitan 6.00

SC rate: 99.96%
FP rate: 0.01%
Final score: 99.88
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.6%

Trustwave Secure Email Gateway

SC rate: 99.85%
FP rate: 0.01%
Final score: 99.73
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.8%

Vade Retro MailCube

SC rate: 99.85%
FP rate: 0.02%
Final score: 99.73
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.3%

ZEROSPAM

SC rate: 99.94%
FP rate: 0.02%
Final score: 99.72
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.996%
Newsletters FP rate: 2.7%

PARTIAL SOLUTIONS

The products listed below are 'partial solutions', which means they only have access to part of the emails and/or SMTP transaction, and are intended to be used as part of a full spam solution. As such, their performance should neither be compared with those of the full solutions listed above, nor necessarily with each other's.

IBM XForce API

SC rate: 96.97%
FP rate: 0.00%
Final score: 96.97
Project Honey Pot SC rate: 94.40%
Abusix SC rate: 99.43%
Newsletters FP rate: 0.0%

Spamhaus DBL

SC rate: 23.82%
FP rate: 0.00%
Final score: 23.78
Project Honey Pot SC rate: 47.65%
Abusix SC rate: 0.93%
Newsletters FP rate: 1.2%

Spamhaus ZEN

SC rate: 95.17%
FP rate: 0.00%
Final score: 95.17
Project Honey Pot SC rate: 90.93%
Abusix SC rate: 99.24%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

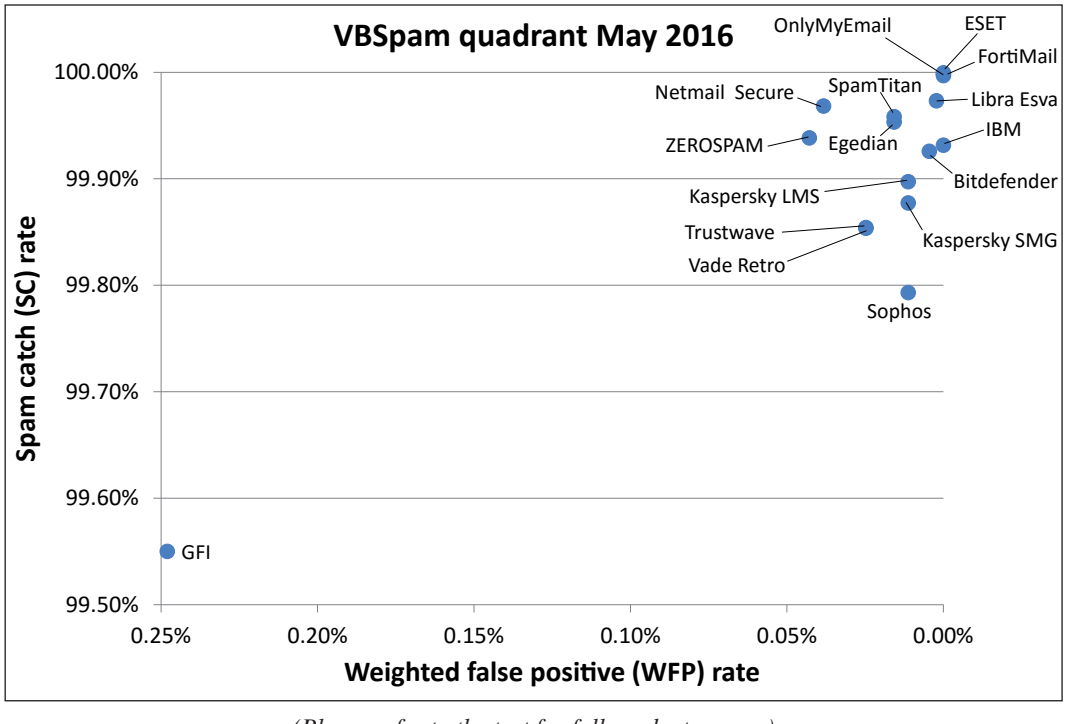
SC rate: 96.38%
FP rate: 0.00%
Final score: 96.34
Project Honey Pot SC rate: 93.41%
Abusix SC rate: 99.24%
Newsletters FP rate: 1.2%

CONCLUSION

In this, the 44th VBSpam test, spam catch rates continued to be very good. Yet emails do occasionally slip through the mazes of email security solutions, and while one may argue we are doing as well as we can, those missed spam emails often have malware attached and can thus cause real harm. For that reason, in future tests we will be looking at how well spam filters block specific campaigns.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock
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: https://www.virusbulletin.com/



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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Bitdefender	8803	0	0.00%	119	160307	99.93%	SPAM + Verified	99.90
Egedian	8802	1	0.01%	75	160351	99.95%	SPAM Verified	99.87
ESET	8803	0	0.00%	2	160424	99.999%	SPAM + Verified	99.999
FortiMail	8803	0	0.00%	5	160421	99.997%	SPAM + Verified	99.997
GFI	8783	20	0.23%	722	159704	99.55%	SPAM Verified	98.31
IBM	8803	0	0.00%	110	160316	99.93%	SPAM + Verified	99.93
Kaspersky LMS	8802	1	0.01%	165	160261	99.90%	SPAM Verified	99.84
Kaspersky SMG	8802	1	0.01%	197	160229	99.88%	SPAM Verified	99.82
Libra Esva	8803	0	0.00%	43	160383	99.97%	SPAM + Verified	99.96
Netmail Secure	8800	3	0.03%	51	160375	99.97%	SPAM Verified	99.78
OnlyMyEmail	8803	0	0.00%	1	160425	99.999%	SPAM + Verified	99.999
Sophos	8802	1	0.01%	332	160094	99.79%	SPAM Verified	99.74
SpamTitan	8802	1	0.01%	67	160359	99.96%	SPAM Verified	99.88
Trustwave	8802	1	0.01%	234	160192	99.85%	SPAM Verified	99.73
Vade Retro MailCube	8801	2	0.02%	235	160191	99.85%	SPAM Verified	99.73
ZEROSPAM	8801	2	0.02%	99	160327	99.94%	SPAM Verified	99.72
IBM X-Force*	8803	0	0.00%	4868	4868	96.97%	N/A	96.97
Spamhaus DBL*	8803	0	0.00%	122207	122207	23.82%	N/A	23.78
Spamhaus ZEN*	8803	0	0.00%	7756	7756	95.17%	N/A	95.17
Spamhaus ZEN+DBL*	8803	0	0.00%	5804	5804	96.38%	N/A	96.34

**The Spamhaus products and IBM X-Force 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.)

	Newsletters		Project Honey Pot		Abusix		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender	2	0.6%	111	99.86%	8	99.99%	0.17
Egedian	2	0.6%	74	99.91%	1	99.999%	0.14
ESET	0	0.0%	2	99.997%	0	100.00%	0.01
FortiMail	0	0.0%	4	99.995%	1	99.999%	0.03
GFI	10	3.0%	212	99.73%	510	99.38%	0.41
IBM	0	0.0%	109	99.86%	1	99.999%	0.15
Kaspersky LMS	0	0.0%	153	99.81%	12	99.99%	0.34
Kaspersky SMG	0	0.0%	181	99.77%	16	99.98%	0.48
Libra Esva	1	0.3%	35	99.96%	8	99.99%	0.1
Netmail Secure	2	0.6%	50	99.94%	1	99.999%	0.1
OnlyMyEmail	0	0.0%	1	99.999%	0	100.00%	0.01
Sophos	0	0.0%	317	99.60%	15	99.98%	0.28
SpamTitan	2	0.6%	67	99.92%	0	100.00%	0.13
Trustwave	6	1.8%	227	99.71%	7	99.99%	0.32
Vade Retro MailCube	1	0.3%	229	99.71%	6	99.99%	0.25
ZEROSPAM	9	2.7%	96	99.88%	3	99.996%	0.23
IBM X-Force*	0	0.0%	4405	94.40%	463	99.43%	1.51
Spamhaus DBL*	4	1.2%	41150	47.65%	81057	93.41%	7.44
Spamhaus ZEN*	0	0.0%	7133	90.93%	623	99.24%	1.93
Spamhaus ZEN+DBL*	4	1.2%	5184	0.9341	620	99.24%	1.68

** The Spamhaus products and IBM X-Force 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.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Retro MailCube	DrWeb; proprietary	√	√	√		√	√
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
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender, ClamAV	√				√		√	√
ESET	ESET Threatsense	√				√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky Lab	√	√	√	√	√		√	
Kaspersky SMG	Kaspersky Lab	√	√	√	√	√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Netmail Secure	Proprietary	√	√	√		√		√	
Profil	Bitdefender	√				√		√	
Sophos	Sophos		√	√				√	√
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	
Trustwave	Support for multiple third-party engines	√	√	√		√	√	√	√

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