

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2019

Martijn Grooten & Ionuț Răileanu

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – 12 full email security solutions and three blacklists of various kinds were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

The news in these test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, especially against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with all 12 full solutions obtaining a VBSpam award and four of them performing well enough to earn a VBSpam+ award.

However, it is important to look beyond the spam catch rates: block rates of malware and phishing emails, though still high, were significantly lower than the block rates of ordinary spam emails.

MALWARE AND PHISHING

As in the previous test, in this test we look at the performance of products against 'malware' and 'phishing' emails, defined as emails with a malicious attachment and those with a malicious link, respectively. It should be noted that the distinction between these categories isn't always clear, for example when an email has a PDF attachment that includes a link to a phishing website (we classify this as 'phishing', arguing that the attachment itself isn't malicious).

An example of such an email, with the attachment masquerading as an invoice that required 'email verification'

in order to view it, was among those phishing emails missed by at least half the products we tested; other 'difficult' emails included phishes for Apple IDs and email credentials, while a fake but very believable UPS email linked to a site that downloaded the Adwind RAT.

Block rates of emails with a malicious attachment were, as usual, a little better, but there were still some that were missed by many products, with emails carrying the infamous Emotet trojan found to be the most difficult to block – something we have observed consistently.

RESULTS

Spam catch rates were once again high, with many products blocking 99.9% or more of the spam, but block rates of malware and phishing were significantly lower. All participating full solutions achieved a VBSpam award, with six products – *Bitdefender*, *ESET*, *IBM*, *Safemail* and both *Kaspersky* products – performing well enough to achieve a VBSpam+ award.

ESET and *Libra Esva* were the only products that didn't miss a single email with a malicious attachment; they were also the only products not to miss a single phishing email.

New to the test bench on this occasion is *Spamhaus rsync*. Like the *Spamhaus Data Query Service* this product is a quick and easy configuration of *Apache SpamAssassin*, the popular open-source spam filter. This configuration uses the data from *Spamhaus's* public mirrors that have a one-minute delay between updates, while the DQS is updated in real time and has some extra features. We noticed the rsync-based product missing almost twice as many spam emails as the DQS.

These products replace the individual *Spamhaus* lists that have been tested by *Virus Bulletin* in the past. *Virus Bulletin* has no control over how these products have been set up.

Axway MailGate 5.6

SC rate: 99.81%
 FP rate: 0.02%
 Final score: 99.68
 Malware catch rate: 94.82%
 Phishing catch rate: 95.13%
 Project Honey Pot SC rate: 99.73%
 Abusix SC rate: 99.85%
 Newsletters FP rate: 1.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM Lotus Protector for Mail Security

SC rate: 99.92%
 FP rate: 0.00%
 Final score: 99.92
 Malware catch rate: 95.43%
 Phishing catch rate: 96.07%
 Project Honey Pot SC rate: 99.97%
 Abusix SC rate: 99.91%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.97
 Malware catch rate: 99.39%
 Phishing catch rate: 98.13%
 Project Honey Pot SC rate: 99.99%
 Abusix SC rate: 99.96%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky for Exchange

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.97
 Malware catch rate: 96.95%
 Phishing catch rate: 97.75%
 Project Honey Pot SC rate: 99.97%
 Abusix SC rate: 99.97%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ESET Mail Security for Microsoft Exchange Server

SC rate: 99.997%
 FP rate: 0.00%
 Final score: 99.98
 Malware catch rate: 100.00%
 Phishing catch rate: 100.00%
 Project Honey Pot SC rate: 100.00%
 Abusix SC rate: 100.00%
 Newsletters FP rate: 0.5%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky Linux Mail Security 8.0

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.97
 Malware catch rate: 97.26%
 Phishing catch rate: 97.38%
 Project Honey Pot SC rate: 99.97%
 Abusix SC rate: 99.97%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet FortiMail

SC rate: 99.97%
 FP rate: 0.04%
 Final score: 99.74
 Malware catch rate: 99.70%
 Phishing catch rate: 97.94%
 Project Honey Pot SC rate: 100.00%
 Abusix SC rate: 99.97%
 Newsletters FP rate: 1.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Libra Esva 4.4.0.0

SC rate: 99.98%
 FP rate: 0.02%
 Final score: 99.85
 Malware catch rate: 100.00%
 Phishing catch rate: 100.00%
 Project Honey Pot SC rate: 99.98%
 Abusix SC rate: 99.98%
 Newsletters FP rate: 1.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Safemail

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.94
Malware catch rate: 99.70%
Phishing catch rate: 96.63%
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus Data Query Service

SC rate: 99.21%
FP rate: 0.00%
Final score: 99.21
Malware catch rate: 81.71%
Phishing catch rate: 65.54%
Project Honey Pot SC rate: 99.52%
Abusix SC rate: 99.09%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus rsync

SC rate: 98.62%
FP rate: 0.00%
Final score: 98.62
Malware catch rate: 80.49%
Phishing catch rate: 62.17%
Project Honey Pot SC rate: 99.32%
Abusix SC rate: 98.37%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ZEROSPAM

SC rate: 99.90%
FP rate: 0.06%
Final score: 99.48
Malware catch rate: 99.39%
Phishing catch rate: 92.32%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.87%
Newsletters FP rate: 3.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM X-Force Combined

SC rate: 98.44%
FP rate: 0.06%
Final score: 98.15
Malware catch rate: 79.88%
Phishing catch rate: 68.54%
Project Honey Pot SC rate: 98.97%
Abusix SC rate: 98.25%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 95.96%
FP rate: 0.06%
Final score: 95.67
Malware catch rate: 78.35%
Phishing catch rate: 61.99%
Project Honey Pot SC rate: 93.05%
Abusix SC rate: 97.04%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 61.89%
FP rate: 0.00%
Final score: 61.89
Malware catch rate: 4.27%
Phishing catch rate: 28.09%
Project Honey Pot SC rate: 90.60%
Abusix SC rate: 51.33%
Newsletters FP rate: 0.0%

APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

The full VBSpam test methodology can be found at <https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/>.

The test ran for 16 days, from 4pm on 14 May to 12am on 30 May 2019.¹

The test corpus consisted of 153,680 emails. 148,301 of these were spam, 39,865 of which were provided by *Project Honey Pot*, with the remaining 108,436 spam emails provided by *Abusix*. There were 5,183 legitimate emails ('ham') and 196 newsletters, a category that includes

¹ Due to a technical glitch, the test was started a few days later than originally planned and ran for a few extra days.

various kinds of commercial and non-commercial opt-in mailings.

255 emails in the spam corpus were considered ‘unwanted’ (see the June 2018 report²) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 328 emails from the spam corpus were found to contain a malicious attachment while 534 contained a link to a phishing or malware site; though we report separate performance metrics on these corpora, it should be noted that these emails were also counted as part of the spam corpus.

Emails were sent to the products in real time and in parallel. Though products received the email from a fixed IP address, all products had been set up to read the original sender’s IP address as well as the EHLO/HELO domain sent during the SMTP transaction, either from the email headers or through an optional XCLIENT SMTP command³.

For those products running in our lab, we all ran them as virtual machines on a *VMware ESXi* cluster. 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.

Although we stress that different customers have different needs and priorities, and thus different preferences when it comes to the ideal ratio of false positive to false negatives, we created a one-dimensional ‘final score’ to compare products. This 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 = $(\# \text{false positives} + 0.2 * \min(\# \text{newsletter false positives}, 0.2 * \# \text{newsletters})) / (\# \text{ham} + 0.2 * \# \text{newsletters})$

while in the spam catch rate (SC), emails considered ‘unwanted’ (see above) are included with a weight of 0.2. The final score is then defined as:

Final score = SC - (5 x WFP)

In addition, for each product, we measure how long it takes to deliver emails from the ham corpus (excluding false positives) and, after ordering these emails by this time,

we colour-code the emails at the 10th, 50th, 95th and 98th percentiles:

- (green) = up to 30 seconds
- (yellow) = 30 seconds to two minutes
- (orange) = two to ten minutes
- (red) = more than ten minutes

Products earn VBSpam certification if the value of the final score is at least 98 and the ‘delivery speed colours’ at 10 and 50 per cent are green or yellow and that at 95 per cent is green, yellow or orange.

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives, no more than 2.5% false positives among the newsletters and ‘delivery speed colours’ of green at 10 and 50 per cent and green or yellow at 95 and 98 per cent earn a VBSpam+ award.

Editor: Martijn Grooten

Head of Testing: Peter Karsai

Security Test Engineers: Gyula Hachbold, Adrian Luca, Csaba Mészáros, Tony Oliveira, Ionuț Răileanu

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin


© 2019 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

Web: <https://www.virusbulletin.com/>

² <https://www.virusbulletin.com/virusbulletin/2018/06vbspam-comparative-review>

³ http://www.postfix.org/XCLIENT_README.html

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Axway	5182	1	0.02%	274.6	147822.4	99.81%	99.68	
Bitdefender	5183	0	0.00%	40.8	148056.2	99.97%	99.97	
ESET	5183	0	0.00%	3.8	148093.2	99.997%	99.98	
FortiMail	5181	2	0.04%	37.4	148059.6	99.97%	99.74	
IBM	5183	0	0.00%	114	147983	99.92%	99.92	
Kaspersky for Exchange	5183	0	0.00%	40.4	148056.6	99.97%	99.97	
Kaspersky LMS	5183	0	0.00%	41.4	148055.6	99.97%	99.97	
Libra Esva	5182	1	0.02%	24.8	148072.2	99.98%	99.85	
Safemail	5183	0	0.00%	93	148004	99.94%	99.94	
Spamhaus DQS	5183	0	0.00%	1174.2	146922.8	99.21%	99.21	
Spamhaus rsync	5183	0	0.00%	2039.2	146057.8	98.62%	98.62	
ZEROSPAM	5180	3	0.06%	143.2	147953.8	99.90%	99.48	
IBM X-Force Combined*	5180	3	0.06%	2306.4	145790.6	98.44%	98.15	N/A
IBM X-Force IP*	5180	3	0.06%	5977.6	142119.4	95.96%	95.67	N/A
IBM X-Force URL*	5183	0	0.00%	56438.6	91658.4	61.89%	61.89	N/A

*The IBM X-Force 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.)

	Newsletters		Malware		Phishing		Project Honey Pot		Abusix		STDev [†]
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway	2	1.0%	17	94.82%	26	95.13%	107.6	99.73%	167	99.85%	0.46
Bitdefender	0	0.0%	2	99.39%	10	98.13%	2	99.99%	38.8	99.96%	0.18
ESET	1	0.5%	0	100.00%	0	100.00%	0	100.00%	3.8	99.996%	0.09
FortiMail	2	1.0%	1	99.70%	11	97.94%	0	100.00%	37.4	99.97%	0.11
IBM	0	0.0%	15	95.43%	21	96.07%	13.2	99.97%	100.8	99.91%	0.41
Kaspersky for Exchange	0	0.0%	10	96.95%	12	97.75%	13	99.97%	27.4	99.97%	0.25
Kaspersky LMS	0	0.0%	9	97.26%	14	97.38%	13	99.97%	28.4	99.97%	0.25
Libra Esva	2	1.0%	0	100.00%	0	100.00%	6	99.985%	18.8	99.98%	0.12
Safemail	0	0.0%	1	99.70%	18	96.63%	17.2	99.96%	75.8	99.93%	0.4
Spamhaus DQS	0	0.0%	60	81.71%	184	65.54%	190	99.52%	984.2	99.09%	2.72
Spamhaus rsync	0	0.0%	64	80.49%	202	62.17%	271	99.32%	1768.2	98.37%	2.98
ZEROSPAM	7	3.6%	2	99.39%	41	92.32%	7.2	99.98%	136	99.87%	0.63
IBM X-Force Combined*	0	0.0%	66	79.88%	168	68.54%	411.4	98.97%	1895	98.25%	1.83
IBM X-Force IP*	0	0.0%	71	78.35%	203	61.99%	2768.4	93.05%	3209.2	97.04%	3.91
IBM X-Force URL*	0	0.0%	314	4.27%	384	28.09%	3742.6	90.60%	52696	51.33%	20.63

*The IBM X-Force products are partial solutions and their performance should not be compared with that of other products. None of the queries to the IP blacklists included any information on the attachments; hence their performance on the malware corpus is added purely for information.

†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 and details.)

	Speed			
	10%	50%	95%	98%
Axway	●	●	●	●
Bitdefender	●	●	●	●
ESET	●	●	●	●
FortiMail	●	●	●	●
IBM	●	●	●	●
Kaspersky for Exchange	●	●	●	●
Kaspersky LMS	●	●	●	●
Libra Esva	●	●	●	●
Safemail	●	●	●	●
Spamhaus DQS	●	●	●	●
Spamhaus rsync	●	●	●	●
ZEROSPAM	●	●	●	●

● 0–30 seconds; ● 30 seconds to two minutes; ● two minutes to 10 minutes; ● more than 10 minutes.

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

Products ranked by final score	
ESET	99.98
Kaspersky for Exchange	99.97
Bitdefender	99.97
Kaspersky LMS	99.97
Safemail	99.94
IBM	99.92
Libra Esva	99.85
FortiMail	99.74
Axway	99.68
ZEROSPAM	99.48
Spamhaus DQS	99.21
Spamhaus rsync	98.62

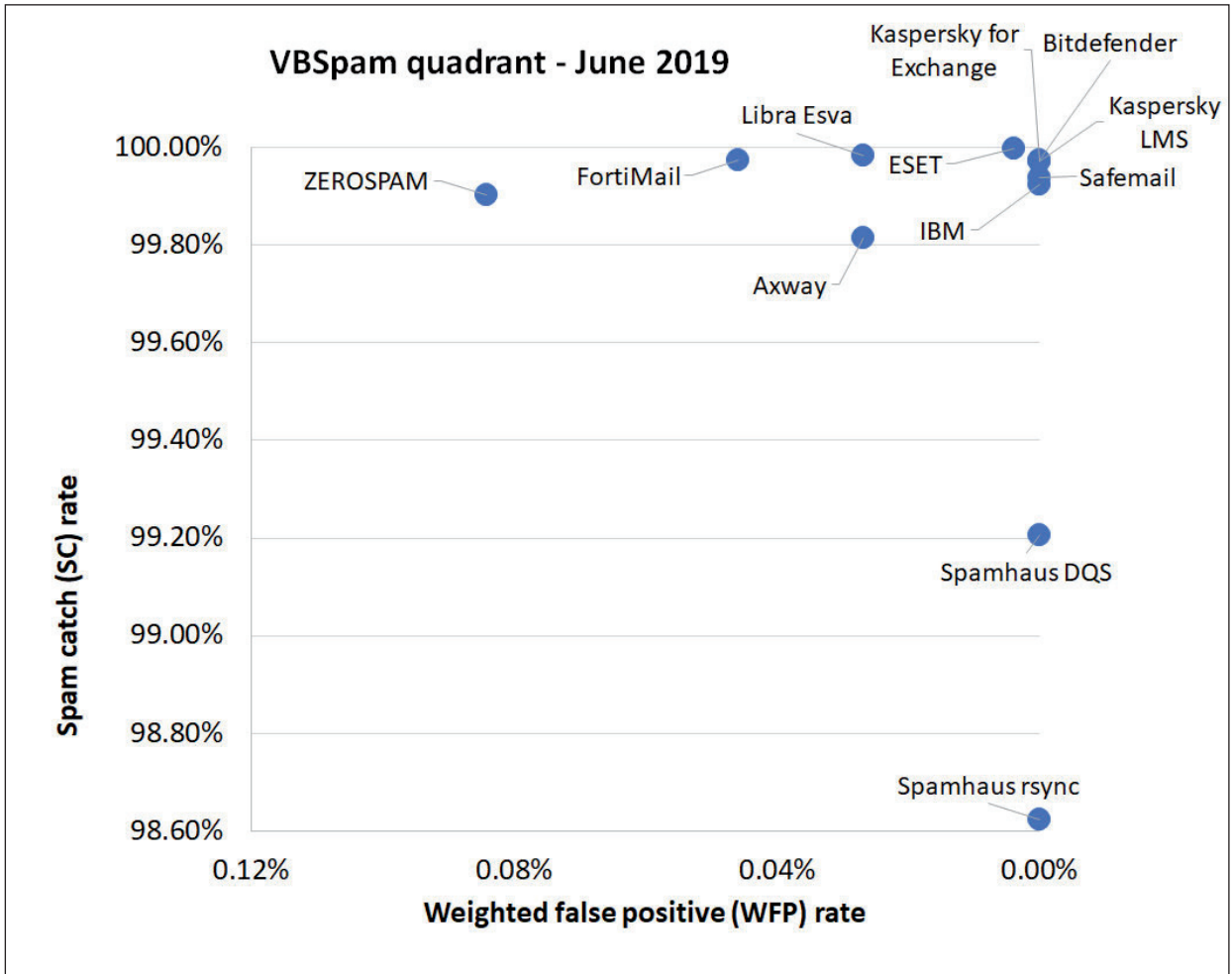
(Please refer to the text for full product names and details.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Safemail	ClamAV; proprietary	√	√	√	√	√	√
ZEROSPAM	ClamAV			√		√	√

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√	√	√		√	√
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky for Exchange	Kaspersky Lab	√		√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√	√	√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Spamhaus DQS	Optional	√	√	√					√
Spamhaus rsyc	Optional	√	√	√					√

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



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