MARCH 2019

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2019

Martijn Grooten & Ionuţ Răileanu

In this test – which forms part of *Virus Bulletin*'s continuously running security product test suite – 11 full email security solutions and seven 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 VBSpam test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, particularly against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with all 11 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

This test sees the debut of the 'phishing' subcategory of emails. Phishing in this context covers emails containing links that either lead to a site with a fake login page (traditional phishing) or that download malware. The reason for grouping these two types together reflects the fact that, for an email security product, the distinction often isn't clear.

Both emails that contain malware and phishing emails are sent in much smaller batches than traditional spam emails. While this means they won't contribute much to the overall spam catch rate, it also means that the campaigns are far more likely to stay under the radar. This is even more the case with phishing than it is with malware, because the 'maliciousness' in phishing emails isn't part of the email itself and thus often can't be considered during the filtering process.[1]

On our blog[2], we have documented various recent examples of malware and phishing emails that were missed by some of the products in our lab. Looking at the phishing emails most commonly missed in this test, we see various traditional phishing scams targeting customers of banks, email and service providers, but also emails that link to malware such as Emotet.

Emotet was also one of the malware families regularly missed by a number of products when it was sent as an attachment to emails. The most widely missed email, however, was one that used the known method of attaching a *Word* document that is protected with a basic password – which prevents it from being scanned properly by anti-virus engines. Though the detection of malicious emails is about more than scanning the attachment, such non-detection does help the email to stay under the radar.

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, and four vendors – *Bitdefender*, *ESET*, *Fortinet* and *IBM* – performed well enough to achieve a VBSpam+ award.

Fortinet, *IBM* and *Libra Esva* were the only products that didn't miss a single email with a malicious attachment; *ESET* was the only product not to miss a single phishing email.

[1] While it is, in principle, possible for an email security product to open all links, doing so has a number of unwanted implications for the recipient; hence products tend to be reluctant to do so.
[2] https://www.virusbulletin.com/blog/.

ISSN 1749-7027

New to the test bench on this occasion is *Spamhaus Data Query Service*, which is a quick and easy configuration of *Apache SpamAssassin*, the popular open-source spam filter, for subscribers to the *Spamhaus Data Query Service*. Indeed, the results of this test demonstrate that this simple set-up does a good job of blocking well over 99% of spam with few false positives.

The *Abusix Mail Intelligence* combined IP- and domain-based blacklist is a continuation of *Zetascan*.

Axway MailGate 5.5.1

SC rate: 99.81%
FP rate: 0.10%
Final score: 99.31
Malware catch rate: 96.51%
Phishing catch rate: 94.46%
Project Honey Pot SC rate: 99.57%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.92
Malware catch rate: 99.13%
Phishing catch rate: 97.08%
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.97%
Newsletters FP rate: 1.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.95
Malware catch rate: 98.69%
Phishing catch rate: 100.00%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Malware catch rate: 100.00%
Phishing catch rate: 95.63%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Malware catch rate: 100.00%
Phishing catch rate: 96.50%
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky for Exchange

SC rate: 99.98%
FP rate: 0.02%
Final score: 99.89
Malware catch rate: 99.56%
Phishing catch rate: 99.42%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Linux Mail Security 8.0

SC rate: 99.98%
FP rate: 0.02%
Final score: 99.89
Malware catch rate: 99.56%
Phishing catch rate: 99.42%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libra Esva 4.4.0.0

SC rate: 99.99%
FP rate: 0.04%
Final score: 99.76
Malware catch rate: 100.00%
Phishing catch rate: 98.83%
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 99.43%
FP rate: 0.02%
Final score: 99.34
Malware catch rate: 84.72%
Phishing catch rate: 60.06%
Project Honey Pot SC rate: 98.72%
Abusix SC rate: 99.63%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spin Safemail

SC rate: 99.93%
FP rate: 0.02%
Final score: 99.84
Malware catch rate: 99.56%
Phishing catch rate: 93.59%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.92%
FP rate: 0.11%
Final score: 99.18
Malware catch rate: 99.13%
Phishing catch rate: 95.63%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.90%
Newsletters FP rate: 4.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 97.12%
FP rate: 0.13%
Final score: 96.45
Malware catch rate: 89.08%
Phishing catch rate: 76.97%
Project Honey Pot SC rate: 87.15%
Abusix SC rate[3]**:** 99.82%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 98.03%
FP rate: 0.02%
Final score: 97.93
Malware catch rate: 71.62%
Phishing catch rate: 80.17%
Project Honey Pot SC rate: 96.83%
Abusix SC rate: 98.35%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 96.92%
FP rate: 0.02%
Final score: 96.82
Malware catch rate: 70.31%
Phishing catch rate: 69.39%
Project Honey Pot SC rate: 93.69%
Abusix SC rate: 97.79%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 67.57%
FP rate: 0.00%
Final score: 67.57
Malware catch rate: 3.49%
Phishing catch rate: 48.69%
Project Honey Pot SC rate: 87.89%
Abusix SC rate: 62.06%
Newsletters FP rate: 0.0%

[3] *Abusix* is also the provider of this feed. The feed is sent in real time and *Abusix* does not have advance knowledge of what emails are part of it.

Spamhaus DBL

SC rate: 47.75%
FP rate: 0.04%
Final score: 47.56
Malware catch rate: 1.31%
Phishing catch rate: 11.08%
Project Honey Pot SC rate: 36.09%
Abusix SC rate: 50.91%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 97.53%
FP rate: 0.00%
Final score: 97.53
Malware catch rate: 58.08%
Phishing catch rate: 27.99%
Project Honey Pot SC rate: 92.86%
Abusix SC rate: 98.80%
Newsletters FP rate: 0.0%

Spamhaus ZEN+DBL

SC rate: 97.92%
FP rate: 0.04%
Final score: 97.73
Malware catch rate: 58.95%
Phishing catch rate: 31.20%
Project Honey Pot SC rate: 94.06%
Abusix SC rate: 98.96%
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 12am on 9 February to 12am on 25 February 2019.

The test corpus consisted of 192,735 emails. 187,308 of these were spam, 39,931 of which were provided by *Project Honey Pot*, with the remaining 147,377 spam emails provided by *Abusix*. There were 5,226 legitimate emails ('ham') and 201 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

181 emails in the spam corpus were considered 'unwanted' (see the June 2018 report: https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 229 emails from the spam corpus were found to contain a malicious attachment while 343 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 command[4]. Consequently, products were able to filter email in an environment that was very close to one in which they would be deployed in the real world.

For those products running in our lab, we 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 positives 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 = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #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,

[4] http://www.postfix.org/XCLIENT_README.html.

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, Ionuţ 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/

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Axway	5221	5	0.10%	364	186799.2	99.81%	99.31	SPAM Verified
Bitdefender	5226	0	0.00%	44.2	187119	99.98%	99.92	SPAM + Verified
ESET	5226	0	0.00%	23.6	187139.6	99.99%	99.95	SPAM + Verified
FortiMail	5226	0	0.00%	89.2	187074	99.95%	99.95	SPAM + Verified
IBM	5226	0	0.00%	124.2	187039	99.93%	99.93	SPAM + Verified
Kaspersky for Exchange	5225	1	0.02%	36.6	187126.6	99.98%	99.89	SPAM Verified
Kaspersky LMS	5225	1	0.02%	33.6	187129.6	99.98%	99.89	SPAM Verified
Libra Esva	5224	2	0.04%	27.6	187135.6	99.99%	99.76	SPAM Verified
Spamhaus DQS	5225	1	0.02%	1060.6	186102.6	99.43%	99.34	SPAM Verified
Spin	5225	1	0.02%	126	187037.2	99.93%	99.84	SPAM Verified
ZEROSPAM	5220	6	0.11%	154.6	187008.6	99.92%	99.18	SPAM Verified
Abusix Mail Intelligence*	5219	7	0.13%	5396.6	181766.6	97.12%	96.45	N/A
IBM X-Force Combined*	5225	1	0.02%	3696.2	183467	98.03%	97.93	N/A
IBM X-Force IP*	5225	1	0.02%	5771.4	181391.8	96.92%	96.82	N/A
IBM X-Force URL*	5226	0	0.00%	60706	126457.2	67.57%	67.57	N/A
Spamhaus DBL*	5224	2	0.04%	97791.8	89371.4	47.75%	47.56	N/A
Spamhaus ZEN*	5226	0	0.00%	4619.4	182543.8	97.53%	97.53	N/A
Spamhaus ZEN+DBL*	5224	2	0.04%	3895.6	183267.6	97.92%	97.73	N/A

**The Abusix, IBM X-Force and Spamhaus ZEN/DBL 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	1	0.5%	8	96.51%	19	94.46%	173	99.57%	190.2	99.87%	0.30
Bitdefender	3	1.5%	2	99.13%	10	97.08%	0	100.00%	42.6	99.97%	0.11
ESET	2	1.0%	3	98.69%	0	100.00%	4	99.99%	18	99.99%	0.09
FortiMail	0	0.0%	0	100.00%	15	95.63%	2	99.99%	85.6	99.94%	0.17
IBM	0	0.0%	0	100.00%	12	96.50%	14.2	99.96%	108.4	99.93%	0.25
Kaspersky for Exchange	0	0.0%	1	99.56%	2	99.42%	4.6	99.99%	30.4	99.98%	0.13
Kaspersky LMS	0	0.0%	1	99.56%	2	99.42%	4.6	99.99%	27.4	99.98%	0.13
Libra Esva	2	1.0%	0	100.00%	4	98.83%	1.2	99.997%	24.8	99.98%	0.12
Spamhaus DQS	0	0.0%	35	84.72%	137	60.06%	510.2	98.72%	548.8	99.63%	0.71
Spin	0	0.0%	1	99.56%	22	93.59%	23	99.94%	101.4	99.93%	0.22
ZEROSPAM	9	4.5%	2	99.13%	15	95.63%	11	99.97%	142	99.90%	0.25
Abusix Mail Intelligence*	0	0.0%	25	89.08%	79	76.97%	5127.4	87.15%	267.6	99.82%	1.71
IBM X-Force Combined*	0	0.0%	65	71.62%	68	80.17%	1265	96.83%	2429.6	98.35%	2.15
IBM X-Force IP*	0	0.0%	68	70.31%	105	69.39%	2515.8	93.69%	3254	97.79%	14.42
IBM X-Force URL*	0	0.0%	221	3.49%	176	48.69%	4832.2	87.89%	55872.2	62.06%	13.2
Spamhaus DBL*	0	0.0%	226	1.31%	305	11.08%	25493.6	36.09%	72296.6	50.91%	1.83
Spamhaus ZEN*	0	0.0%	96	58.08%	247	27.99%	2850.2	92.86%	1767.6	98.80%	1.71
Spamhaus ZEN+DBL*	0	0.0%	94	58.95%	236	31.20%	2367.6	94.06%	1526.4	98.96%	17.25

**The Abusix, IBM X-Force and Spamhaus ZEN/DBL 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	●	●	●	●
Spamhaus DQS	●	●	●	●
Spin	●	●	●	●
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	
FortiMail	99.95
ESET	99.95
IBM	99.93
Bitdefender	99.92
Kaspersky LMS	99.89
Kaspersky for Exchange	99.89
Spin	99.84
Libra Esva	99.76
Spamhaus DQS	99.34
Axway	99.31
ZEROSPAM	99.18

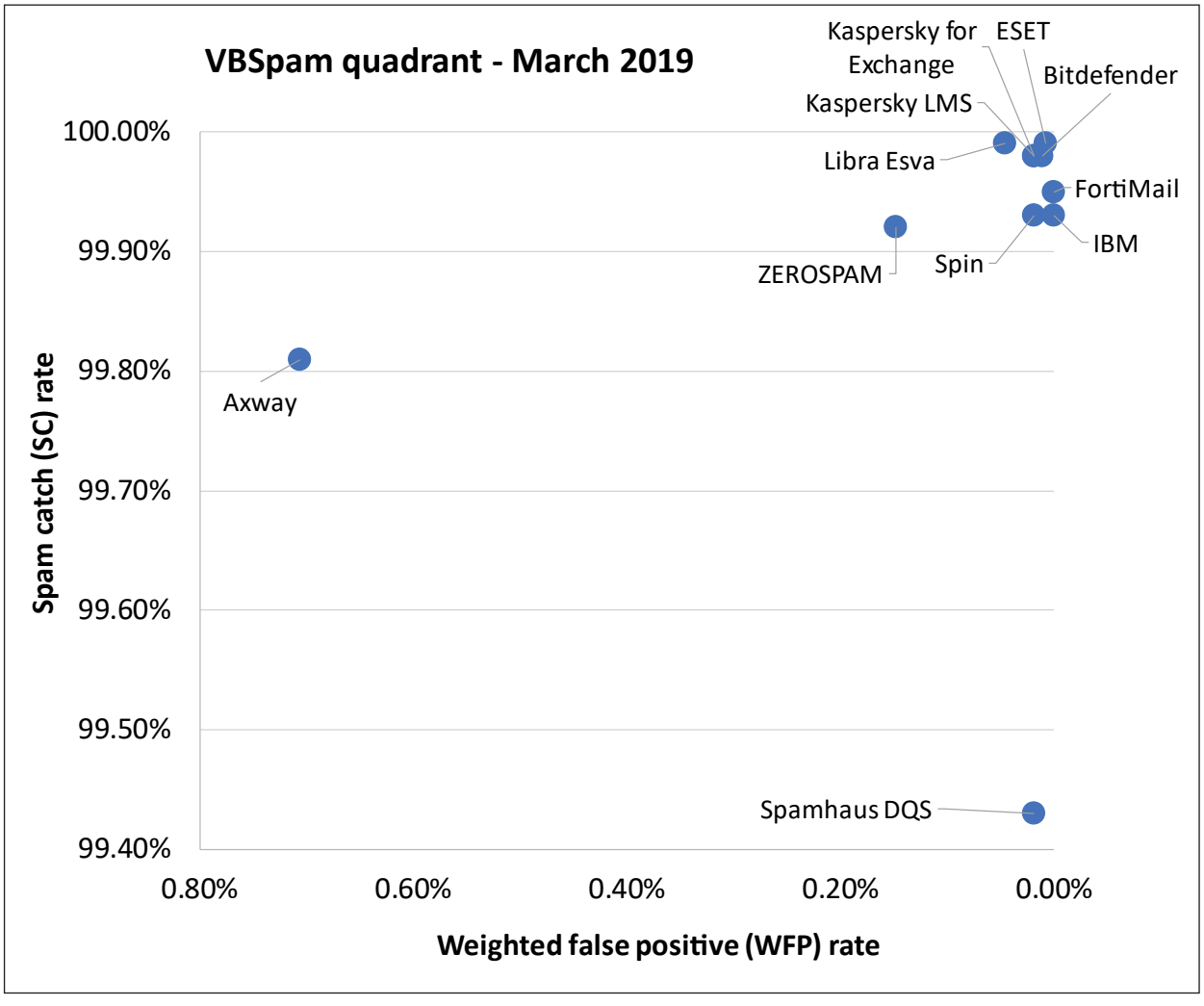
(Please refer to the text for full product names and details.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Spin	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	√	√	√					√

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



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