

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW DECEMBER 2019

Martijn Grooten & Ionuț Răileanu

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – 11 full email security solutions and five blacklists of various kinds were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

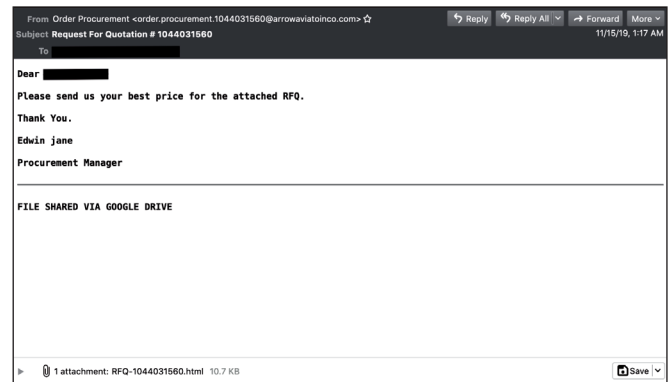
The news in these test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, especially against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with all 11 full solutions obtaining a VBSpam award and eight 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.

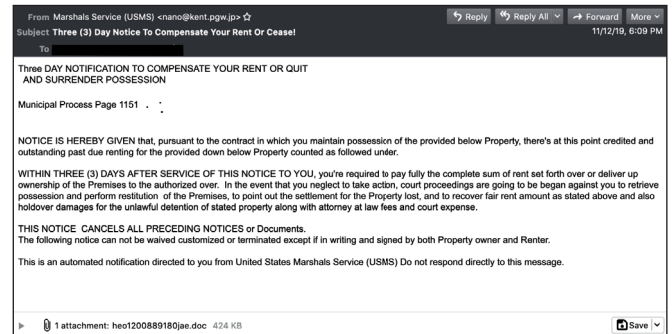
MALWARE AND PHISHING

In this test we continue to highlight the email security solutions' performance against malware and phishing emails. In these two categories we consider emails with a malicious attachment or containing links that either lead to a site with a fake login page (traditional phishing) or that download malware. Also considered as phishing are those emails with an HTML or PDF attachment that doesn't display malicious behaviour itself, but which contains links leading to a phishing site.

During the test we also spotted emails – missed by some of the products – with an 'application/HTML' MIME part, an invalid type (as mentioned in a blog post by *Libraesva*¹), but used to bypass the filters of the email security solutions. Other difficult to block phishing emails included phishes for *Netflix*, *Amazon* and *PayPal* accounts.



Emails containing Emotet-infected malicious attachments continued to be the most difficult to block. Even though not sent in bulk, an email containing the banking trojan IcedID was among the most commonly missed malware samples.



¹ <https://www.libraesva.com/email-trojan-horse-application-html-entity/>

Also worth mentioning is a sextortion campaign, sent from outlook accounts, in which the emails contained password-protected PDFs. In this case the emails went undetected by more than half of the products in test.

RESULTS

Spam catch rates continued to be high, with many products blocking 99.9% or more of the spam, but the catch rates on malware and phishing were significantly lower. All participating full solutions achieved a VBSpam award, and eight vendors – *Axway*, *Bitdefender*, *ESET*, *Fortinet*, *IBM*, *Libraesva*, *Safemail* and *ZEROSPAM* – performed well enough to achieve a VBSpam+ award.

ESET and *Libraesva* were the only products that didn't miss a single email with a malicious attachment, while only *ESET* scored a perfect score in the phishing category, closely followed by *Libraesva*, which missed only one email.

New to the test bench this month is *Abusix Mail Intelligence rspamd*, an open-source spam filtering system written in C, extensible via Lua API and easily integrated with many open-source SMTP servers via the Milter API. *AMI (rspamd)* is designed to showcase the type of results you can achieve by using all *AMI* lists. The problem with IP and domain name blocking is that these cannot be used in certain scenarios, and these scenarios are becoming more common as spam comes up with new ways to avoid them. Additionally, the *rspamd* configuration doesn't just look up the *AMI* IP lists on the connecting IP, it also checks each Received header hop, which provides coverage for hosts that relay spam from compromised accounts.

Abusix Mail Intelligence rspamd

SC rate: 99.56%
FP rate: 0.70%
Final score: 96.04
Malware catch rate: 85.25%
Phishing catch rate: 93.91%
Project Honey Pot SC rate: 98.81%
Abusix SC rate: 99.71%
Newsletters FP rate: 1.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Axway MailGate 5.6

SC rate: 99.77%
FP rate: 0.00%
Final score: 99.75
Malware catch rate: 96.72%
Phishing catch rate: 97.03%
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.78%
Newsletters FP rate: 0.5%
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: 95.81%
Phishing catch rate: 98.87%
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ESET Mail Security for Microsoft Exchange Server

SC rate: 100.00%
FP rate: 0.00%
Final score: 100.00
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: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet FortiMail

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.94
Malware catch rate: 98.91%
Phishing catch rate: 97.73%



Fortinet FortiMail contd.

Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.85%
FP rate: 0.00%
Final score: 99.85
Malware catch rate: 92.08%
Phishing catch rate: 97.45%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.83%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Libraesva ESG v.4.7

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.92
Malware catch rate: 100.00%
Phishing catch rate: 99.86%
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.95%
Newsletters FP rate: 1.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Safemail

SC rate: 99.89%
FP rate: 0.00%
Final score: 99.89
Malware catch rate: 99.69%
Phishing catch rate: 96.88%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus Data Query Service

SC rate: 99.45%
FP rate: 0.02%
Final score: 99.35
Malware catch rate: 97.29%
Phishing catch rate: 76.91%
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.39%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus rsync

SC rate: 99.12%
FP rate: 0.00%
Final score: 99.12
Malware catch rate: 96.97%
Phishing catch rate: 72.52%
Project Honey Pot SC rate: 99.32%
Abusix SC rate: 99.08%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ZEROSPAM

SC rate: 99.85%
FP rate: 0.00%
Final score: 99.71
Malware catch rate: 99.84%
Phishing catch rate: 99.29%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.82%
Newsletters FP rate: 3.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Abusix Mail Intelligence

SC rate: 99.52%
FP rate: 0.08%
Final score: 99.13
Malware catch rate: 75.78%
Phishing catch rate: 85.27%
Project Honey Pot SC rate: 98.47%
Abusix SC rate: 99.74%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 97.40%
FP rate: 0.02%
Final score: 97.30
Malware catch rate: 65.99%
Phishing catch rate: 81.44%
Project Honey Pot SC rate: 99.10%
Abusix SC rate: 97.04%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 96.33%
FP rate: 0.02%
Final score: 96.23
Malware catch rate: 63.04%
Phishing catch rate: 74.79%
Project Honey Pot SC rate: 97.77%
Abusix SC rate: 96.03%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 56.56%
FP rate: 0.00%
Final score: 56.56
Malware catch rate: 7.76%
Phishing catch rate: 30.17%
Project Honey Pot SC rate: 93.23%
Abusix SC rate: 48.93%
Newsletters FP rate: 0.0%

Kaspersky DNSBL

SC rate: 88.39%
FP rate: 0.00%
Final score: 88.39
Malware catch rate: 38.98%
Phishing catch rate: 54.67%
Project Honey Pot SC rate: 93.81%
Abusix SC rate: 87.26%
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 November to 12am on 25 November 2019.

The test corpus consisted of 265,568 emails. 260,380 of these were spam, 44,844 of which were provided by *Project Honey Pot*, with the remaining 215,536 spam emails provided by *Abusix*. There were 5,003 legitimate emails ('ham') and 185 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) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 644 emails from the spam corpus were found to contain a malicious attachment while 706 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 command².

For those products running in our lab, we ran them all 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

²http://www.postfix.org/XCLIENT_README.html

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/>

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
AMI rspamd	4968	35	0.70%	1154.8	259080.4	99.56%	96.04	
Axway	5003	0	0.00%	592	259635.2	99.77%	99.75	
Bitdefender	5003	0	0.00%	82.8	260152.4	99.97%	99.97	
ESET	5003	0	0.00%	9	260226.2	99.996%	99.996	
FortiMail	5003	0	0.00%	158.6	260076.6	99.94%	99.94	
IBM	5003	0	0.00%	400	259835.2	99.85%	99.85	
Libraesva	5003	0	0.00%	105.8	260090.4	99.96%	99.92	
Safemail	5003	0	0.00%	286.4	259948.8	99.89%	99.89	
Spamhaus DQS	5002	1	0.02%	1437.6	258778.6	99.45%	99.35	
Spamhaus rsync	5003	0	0.00%	2286.8	257929.4	99.12%	99.12	
ZEROSPAM	5003	0	0.00%	396.8	259157	99.85%	99.71	
AMI*	4999	4	0.08%	1238.2	258997	99.52%	99.13	N/A
IBM X-Force Combined*	5002	1	0.02%	6772.8	253462.4	97.40%	97.30	N/A
IBM X-Force IP*	5002	1	0.02%	9554.4	250680.8	96.33%	96.23	N/A
IBM X-Force URL*	5003	0	0.00%	113055.6	147179.6	56.56%	56.56	N/A
Kaspersky DNSBL*	5003	0	0.00%	30213.2	230022	88.39%	88.39	N/A

*These 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	
AMI rspamd	2	1.08%	95	85.25%	43	93.91%	532.4	98.81%	622.4	99.71%	0.59
Axway	1	0.54%	21	96.72%	21	97.03%	111.8	99.75%	480.2	99.78%	0.63
Bitdefender	0	0.00%	27	95.81%	8	98.87%	0	100.00%	82.8	99.96%	0.14
ESET	0	0.00%	0	100.00%	0	100.00%	0.2	99.999%	8.8	99.995%	0.11
FortiMail	0	0.00%	7	98.91%	16	97.73%	5	99.99%	153.6	99.93%	0.26
IBM	0	0.00%	51	92.08%	18	97.45%	25	99.94%	375	99.83%	0.5
Libraesva	2	1.08%	0	100.00%	1	99.86%	2.2	99.995%	103.6	99.95%	0.19
Safemail	0	0.00%	2	99.69%	22	96.88%	12.6	99.97%	273.8	99.87%	0.29
Spamhaus DQS	0	0.00%	17	97.29%	163	76.91%	123.2	99.73%	1314.4	99.39%	0.85
Spamhaus rsync	0	0.00%	19	96.97%	194	72.52%	303	99.32%	1983.8	99.08%	1.21
ZEROSPAM	7	3.78%	1	99.84%	5	99.29%	12	99.97%	384.8	99.82%	0.4
AMI*	0	0.00%	156	75.78%	104	85.27%	686.6	98.47%	551.6	99.74%	0.7
IBM X-Force Combined*	0	0.00%	219	65.99%	131	81.44%	401.4	99.10%	6371.4	97.04%	2.75
IBM X-Force IP*	0	0.00%	238	63.04%	178	74.79%	1000.4	97.77%	8554	96.03%	3.46
IBM X-Force URL*	0	0.00%	594	7.76%	493	30.17%	3032.2	93.23%	110023.4	48.93%	20.4
Kaspersky DNSBL*	0	0.00%	393	38.98%	320	54.67%	2771.8	93.81%	27441.4	87.26%	6.9

*These 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%
AMI rspamd	●	●	●	●
Axway	●	●	●	●
Bitdefender	●	●	●	●
ESET	●	●	●	●
FortiMail	●	●	●	●
IBM	●	●	●	●
Libraesva	●	●	●	●
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	99.996
Bitdefender	99.97
FortiMail	99.94
Libraesva	99.92
Safemail	99.89
IBM	99.85
Axway	99.75
ZEROSPAM	99.71
Spamhaus DQS	99.35
Spamhaus rsync	99.12
AMI rspamd	96.04

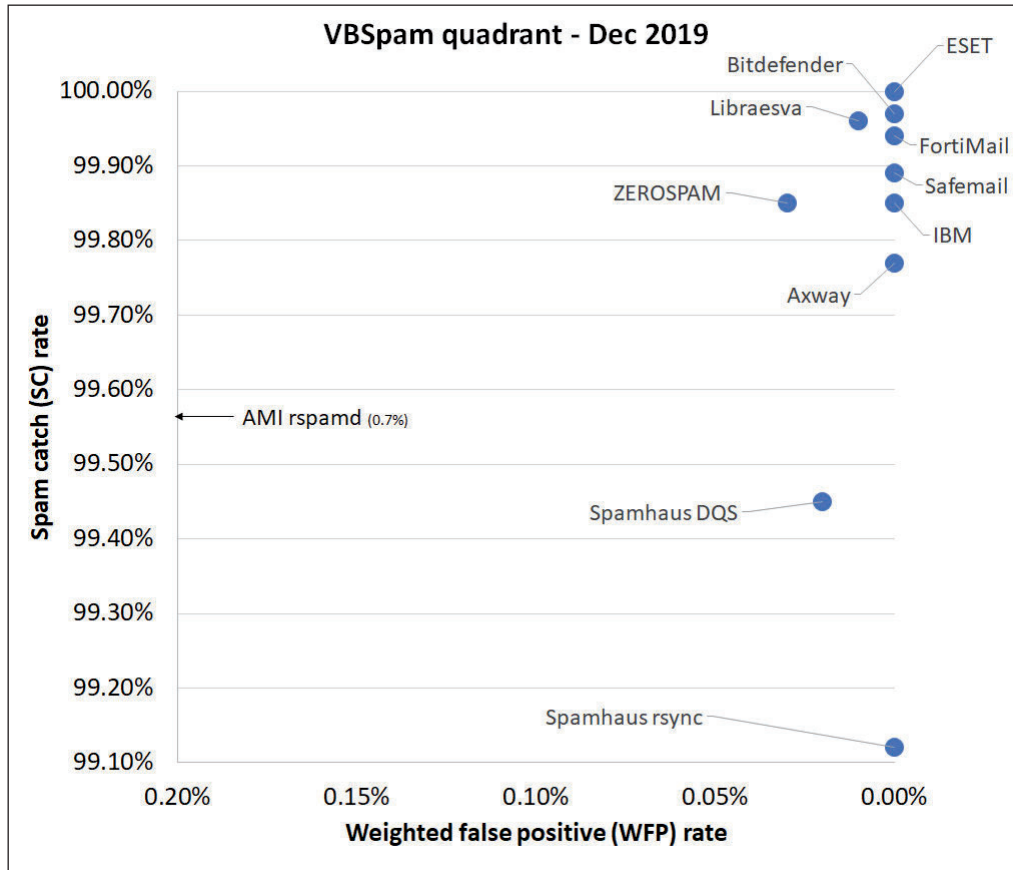
(Please refer to the text for full product names and details.)

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			√		√		√	
Libraesva	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.)