MARCH 2020

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2020

Ionuţ Răileanu

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

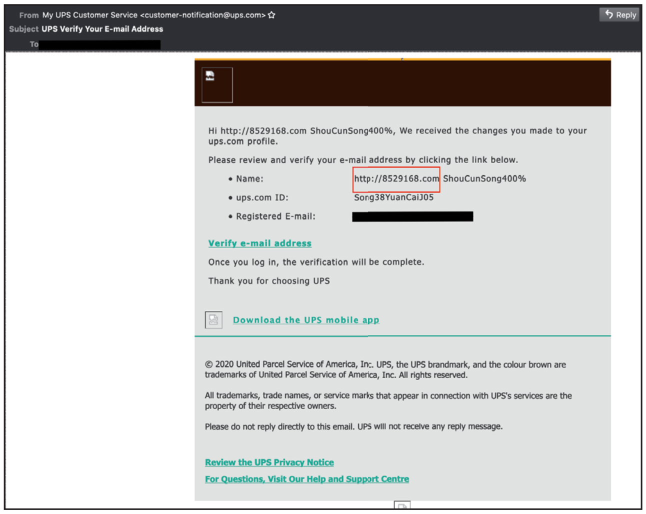
The news in these test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, especially against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with 10 full solutions obtaining a VBSpam award and seven 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 on 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 that lead to a phishing site.

We have seen an increase in spam emails sent from legitimate web pages through open forms. One such campaign caught our attention since it was missed by many of the products in the test. The emails are sent from *UPS* and contain a suspicious URL in the text of the email in place of the name of the recipient.



From My UPS Customer Service <customer-notification@ups.com>
Subject UPS Verify Your E-mail Address
To [redacted]

Hi http://8529168.com ShouCunSong400%, We received the changes you made to your ups.com profile.

Please review and verify your e-mail address by clicking the link below.

- Name: http://8529168.com ShouCunSong400%
- ups.com ID: Song38YuanCaiJ05
- Registered E-mail: [redacted]

Verify e-mail address

Once you log in, the verification will be complete.

Thank you for choosing UPS

Download the UPS mobile app

© 2020 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the colour brown are trademarks of United Parcel Service of America, Inc. All rights reserved.

All trademarks, trade names, or service marks that appear in connection with UPS's services are the property of their respective owners.

Please do not reply directly to this email. UPS will not receive any reply message.

Review the UPS Privacy Notice

For Questions, Visit Our Help and Support Centre

Spam campaign in which emails are sent from UPS and contain a suspicious URL in the text of the email in place of the name of the recipient.

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. Ten of the participating full solutions achieved a VBSpam award, with the products of seven vendors – *Axway*, *Bitdefender*, *ESET*, *Fortinet*, *IBM*, *Safemail* and *ZEROSPAM* – performing well enough to achieve a VBSpam+ award.

ISSN 1749-7027

Bitdefender, *ESET*, *FortiMail*, *Libraesva* and *Safemail* didn't miss a single email with a malicious attachment. Only *ESET* and *ZEROSPAM* achieved a perfect score in the phishing category, while *Libraesva* missed just one phishing email.

Abusix Mail Intelligence rspamd

SC rate: 99.59%
FP rate: 0.45%
Final score: 97.22
Malware catch rate: 97.33%
Phishing catch rate: 87.06%
Project Honey Pot SC rate: 99.17%
Abusix SC rate: 99.83%
Newsletters FP rate: 3.7%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Axway MailGate 5.6

SC rate: 99.72%
FP rate: 0.00%
Final score: 99.70
Malware catch rate: 94.33%
Phishing catch rate: 90.91%
Project Honey Pot SC rate: 99.80%
Abusix SC rate: 99.71%
Newsletters FP rate: 0.5%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb March 2020 VERIFIED SPAM + virusbtn.com

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Malware catch rate: 100.00%
Phishing catch rate: 98.77%
Project Honey Pot SC rate: 99.995%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb March 2020 VERIFIED SPAM + virusbtn.com

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.98%
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: 99.98%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb March 2020 VERIFIED SPAM + virusbtn.com

Fortinet FortiMail

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.97
Malware catch rate: 100.00%
Phishing catch rate: 98.15%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb March 2020 VERIFIED SPAM + virusbtn.com

IBM Lotus Protector for Mail Security

SC rate: 99.88%
FP rate: 0.00%
Final score: 99.88
Malware catch rate: 99.67%
Phishing catch rate: 98.00%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb March 2020 VERIFIED SPAM + virusbtn.com

Libraesva ESG v.4.7

SC rate: 99.95%
FP rate: 0.02%
Final score: 99.85
Malware catch rate: 100.00%
Phishing catch rate: 99.85%

vb March 2020 VERIFIED SPAM virusbtn.com

Libraesva ESG v.4.7 contd.

Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Safemail

vb March 2020 VERIFIED SPAM + virusbtn.com

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.89
Malware catch rate: 100.00%
Phishing catch rate: 99.08%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.93%
Newsletters FP rate: 1.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

vb March 2020 VERIFIED SPAM virusbtn.com

SC rate: 99.42%
FP rate: 0.00%
Final score: 99.40
Malware catch rate: 85.50%
Phishing catch rate: 86.29%
Project Honey Pot SC rate: 99.67%
Abusix SC rate: 99.35%
Newsletters FP rate: 0.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus rsync

vb March 2020 VERIFIED SPAM virusbtn.com

SC rate: 98.78%
FP rate: 0.00%
Final score: 98.78
Malware catch rate: 83.67%
Phishing catch rate: 79.51%
Project Honey Pot SC rate: 98.99%
Abusix SC rate: 98.74%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

vb March 2020 VERIFIED SPAM + virusbtn.com

SC rate: 99.85%
FP rate: 0.00%
Final score: 99.75
Malware catch rate: 99.83%
Phishing catch rate: 100.00%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.82%
Newsletters FP rate: 2.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 99.21%
FP rate: 0.00%
Final score: 99.21
Malware catch rate: 92.00%
Phishing catch rate: 83.98%
Project Honey Pot SC rate: 97.99%
Abusix SC rate: 99.80%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 95.52%
FP rate: 0.02%
Final score: 95.42
Malware catch rate: 83.50%
Phishing catch rate: 84.75%
Project Honey Pot SC rate: 99.57%
Abusix SC rate: 93.79%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 94.73%
FP rate: 0.02%
Final score: 94.63
Malware catch rate: 83.00%
Phishing catch rate: 80.28%
Project Honey Pot SC rate: 98.62%
Abusix SC rate: 93.07%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 65.58%

FP rate: 0.00%

Final score: 65.58

Malware catch rate: 8.83%

Phishing catch rate: 27.27%

Project Honey Pot SC rate: 93.88%

Abusix SC rate: 53.27%

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/vbspam-methodology-ver20.

The test ran for 16 days, from 12am on 8 February to 12am on 24 February 2020 with a few hours of downtime from 9 February 19:00 to 10 February 08:00 GMT, caused by some issues in our network.

The test corpus consisted of 158,322 emails. 153,234 of these were spam, 46,542 of which were provided by *Project Honey Pot*, with the remaining 106,692 spam emails provided by Abusix. There were 4,898 legitimate emails ('ham') and 190 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

155 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[1]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 600 emails from the spam corpus were found to contain a malicious attachment while 649 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[2].

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 = (#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, 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.

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

© 2020 Virus Bulletin Ltd, Manor House - Office 6, Howbery Business Park, Wallingford OX10 8BA, UK

Tel: +44 20 3920 6348 Email: editorial@virusbulletin.com

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

[1] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
AMI rspamd	4864	22	0.45%	569	152541	99.59%	97.22	
Axway	4898	0	0.00%	398.4	152711.6	99.72%	99.70	SPAM+ Verified
Bitdefender	4898	0	0.00%	25.4	153084.6	99.98%	99.98	SPAM+ Verified
ESET	4898	0	0.00%	19.8	153090.2	99.98%	99.98	SPAM+ Verified
FortiMail	4898	0	0.00%	42.8	153067.2	99.97%	99.97	SPAM+ Verified
IBM	4898	0	0.00%	168.6	152941.4	99.88%	99.88	SPAM+ Verified
Libraesva	4897	1	0.02%	64	153046	99.95%	99.85	SPAM Verified
Safemail	4898	0	0.00%	86.8	153023.2	99.93%	99.89	SPAM+ Verified
Spamhaus DQS	4898	0	0.00%	848.4	152261.6	99.42%	99.40	SPAM Verified
Spamhaus rsync	4898	0	0.00%	1815	151295	98.78%	98.78	SPAM Verified
ZEROSPAM	4898	0	0.00%	196.6	152903.4	99.85%	99.75	SPAM+ Verified
AMI*	4898	0	0.00%	1147.2	151962.8	99.21%	99.21	N/A
IBM X-Force Combined*	4897	1	0.02%	6823.2	146286.8	95.52%	95.42	N/A
IBM X-Force IP*	4897	1	0.02%	8028.8	145081.2	94.73%	94.63	N/A
IBM X-Force URL*	4898	0	0.00%	52678	100432	65.58%	65.58	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	7	3.68%	16	97.33%	84	87.06%	384.4	99.17%	184.6	99.83%	0.54
Axway	1	0.53%	34	94.33%	59	90.91%	93.6	99.80%	304.8	99.71%	0.5
Bitdefender	0	0.00%	0	100.00%	8	98.77%	2	99.995%	23.4	99.98%	0.16
ESET	0	0.00%	0	100.00%	0	100.00%	0	100.00%	19.8	99.98%	0.16
FortiMail	0	0.00%	0	100.00%	12	98.15%	2.4	99.99%	40.4	99.96%	0.11
IBM	0	0.00%	2	99.67%	13	98.00%	26.2	99.94%	142.4	99.87%	0.3
Libraesva	0	0.00%	0	100.00%	1	99.85%	2.6	99.99%	61.4	99.94%	0.15
Safemail	2	1.05%	0	100.00%	6	99.08%	12.2	99.97%	74.6	99.93%	0.18
Spamhaus DQS	1	0.53%	87	85.50%	89	86.29%	153.4	99.67%	695	99.35%	0.7
Spamhaus rsync	0	0.00%	98	83.67%	133	79.51%	469	98.99%	1346	98.74%	1.07
ZEROSPAM	5	2.63%	1	99.83%	0	100.00%	7.2	99.98%	189.4	99.82%	0.35
AMI*	0	0.00%	48	92.00%	104	83.98%	935.8	97.99%	211.4	99.80%	0.71
IBM X-Force Combined*	0	0.00%	99	83.50%	99	84.75%	202	99.57%	6621.2	93.79%	3.34
IBM X-Force IP*	0	0.00%	102	83.00%	128	80.28%	640.4	98.62%	7388.4	93.07%	3.47
IBM X-Force URL*	0	0.00%	547	8.83%	472	27.27%	2846	93.88%	49832	53.27%	24.36

**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	99.98
Bitdefender	99.98
FortiMail	99.97
Safemail	99.89
IBM	99.88
Libraesva	99.85
ZEROSPAM	99.75
Axway	99.70
Spamhaus DQS	99.40
Spamhaus rsync	98.78
AMI rspamd	97.22

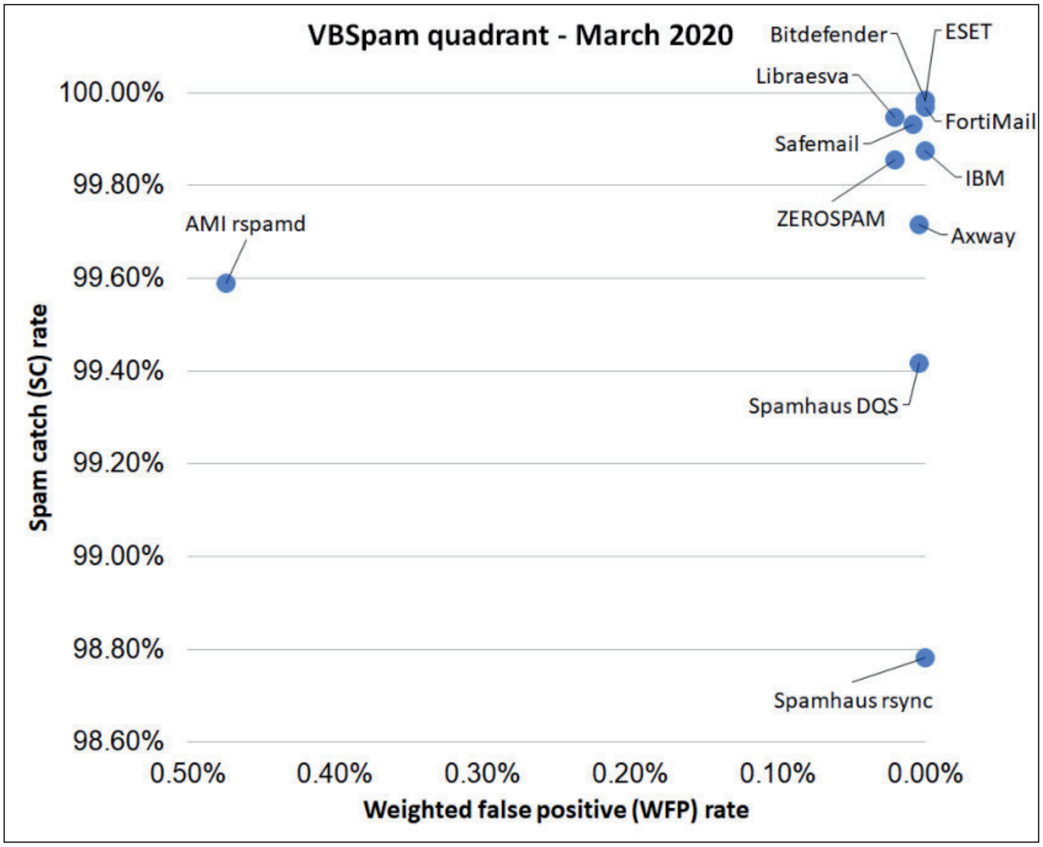
(Please refer to the text for full product names and details.)

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.)