MARCH 2021

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2021

Ionuţ Răileanu

In this test, which forms part of *Virus Bulletin*'s continuously running security product test suite, 28 email security products were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails. The results for the 10 products that elected to be tested publicly – seven full email security solutions, one custom configured solution[1], one open-source solution and one blocklist – are included in this report.

[1] *Spamhaus DQS* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

#	Sender's IP country	Percentage of spam
1	China	13.71%
2	Japan	12.41%
3	Vietnam	5.96%
4	United States	5.64%
5	Brazil	5.14%
6	India	4.55%
7	Argentina	2.47%
8	Korea, Republic of	2.33%
9	Russian Federation	2.28%
10	France	2.23%

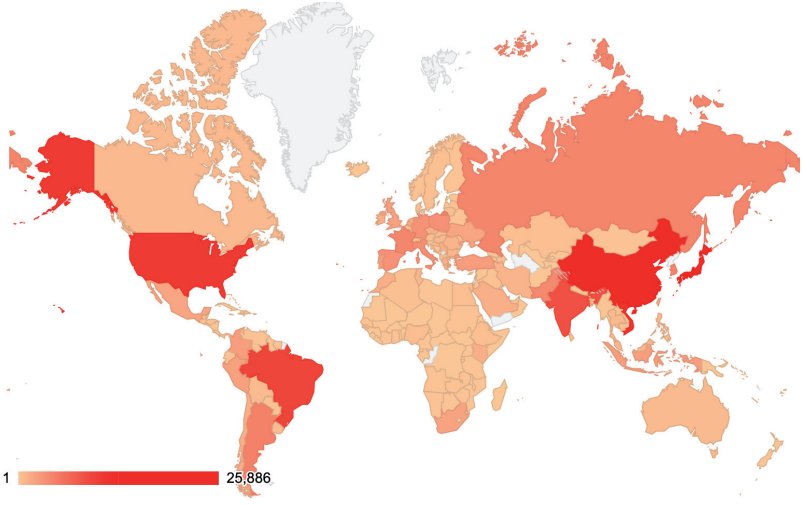
Top 10 countries from which spam was sent.

In this round of testing we welcome three new participants to the public VBSpam test: *Cleanmail Domain Gateway*, *Cyren eXpurgate* and *Rspamd*.

The results are good – the security solutions we tested demonstrated that they are well equipped to defend in the first line against malware and phishing attacks.

With the threat landscape shifting due to the takedown of the Emotet botnet we noted an overall decrease in the number of spam emails seen, not only of those with malicious attachments or URLs. In this report we briefly describe the emails that proved the most challenging for the tested solutions to deal with correctly.

For some additional background to this report, the table and map below show the geographical distribution (based on sender IP address) of the spam emails seen in the test. *(Note: these statistics are relevant only to the spam samples we received in real time.)*



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

MALWARE AND PHISHING

QBot malware

This malware campaign was the most challenging for the solutions participating in our test. The attached zip archive contained an xls file with a macro. On opening the file, a connection was initiated to a domain associated with QBot (casadodestino[.]com). The given example had an attachment with the SHA 256 value of `1da459e6c1bb2779ec85ecab38dc22bcbba40376af754f4ff9ac93bb5b532a22`.

Three solutions managed to block every email of this campaign: *Cleanmail Domain Gateway*, *Libraesva* and *ZEROSPAM*.

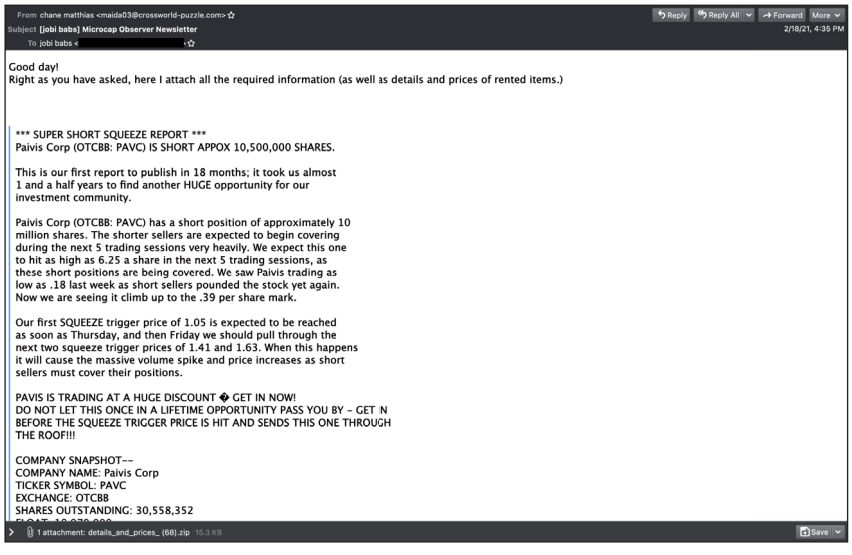
Legitimate services in phishing emails

Despite a decrease in overall numbers, the phishing emails that are the most successful in evading email security solution filtering continue to be those that contain legitimate service URLs, an example of which is shown below. At the time of the analysis the URL in this sample was blocked by *Google* for violating its Terms of Use so we don't have any more details on its behaviour.

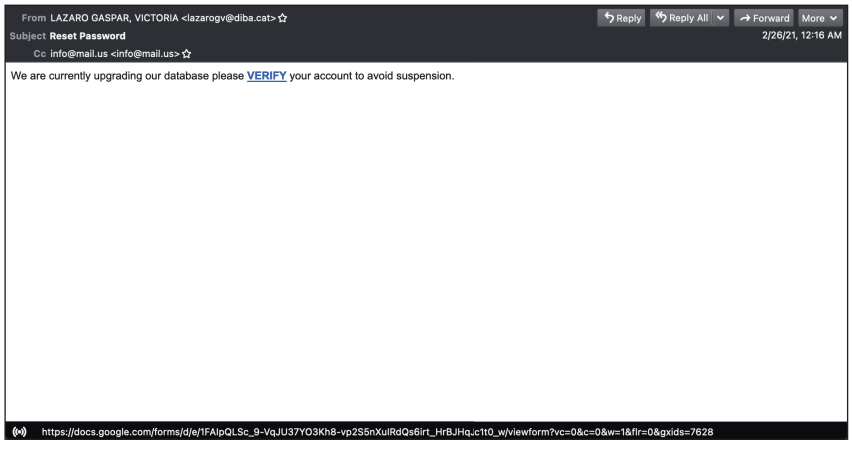
The solutions that correctly blocked this challenging sample were *Bitdefender*, *Cleanmail Domain Gateway* and *ZEROSPAM*.

RESULTS

The majority of the tested security solutions managed to block more than 99% of the spam emails, with three



Example of a QBot malware email.



Example of an email containing a legitimate service URL.

products, *Cleanmail*, *Libraesva* and *ZEROSPAM*, blocking all the malware samples. In the phishing category, the catch rates were lower but we still see many values of more than 98%.

Of the participating full solutions, four achieved a VBSpam award: *Axway, Cleanmail, Fortinet* and *ZEROSPAM*, while a further four performed well enough to achieve a VBSpam+ award: *Bitdefender, Cyren eXpurgate, Libraesva* and *Spamhaus DQS*.

Axway MailGate 5.6

SC rate: 99.86%
FP rate: 0.03%
Final score: 99.73
Malware catch rate: 96.41%
Phishing catch rate: 98.58%
Project Honey Pot SC rate: 99.72%
Abusix SC rate: 99.88%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Malware catch rate: 97.26%
Phishing catch rate: 99.07%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Cleanmail Domain Gateway

SC rate: 99.98%
FP rate: 0.03%
Final score: 99.75
Malware catch rate: 100.00%
Phishing catch rate: 99.95%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.98%
Newsletters FP rate: 3.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Cyren eXpurgate

SC rate: 99.65%
FP rate: 0.00%
Final score: 99.62
Malware catch rate: 98.68%
Phishing catch rate: 94.77%
Project Honey Pot SC rate: 98.93%
Abusix SC rate: 99.78%
Newsletters FP rate: 0.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.78%
FP rate: 0.03%
Final score: 99.65
Malware catch rate: 99.06%
Phishing catch rate: 98.64%
Project Honey Pot SC rate: 99.47%
Abusix SC rate: 99.84%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libraesva ESG v.4.7

SC rate: 99.92%
FP rate: 0.00%
Final score: 99.90
Malware catch rate: 100.00%
Phishing catch rate: 99.67%
Project Honey Pot SC rate: 99.74%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Rspamd

SC rate: 90.17%
FP rate: 0.38%
Final score: 88.08
Malware catch rate: 65.63%
Phishing catch rate: 75.15%
Project Honey Pot SC rate: 84.51%
Abusix SC rate: 91.24%
Newsletters FP rate: 5.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 99.71%
FP rate: 0.00%
Final score: 99.64
Malware catch rate: 93.48%
Phishing catch rate: 98.53%
Project Honey Pot SC rate: 99.17%
Abusix SC rate: 99.82%
Newsletters FP rate: 2.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 98.75%
FP rate: 0.00%
Final score: 98.73
Malware catch rate: 100.00%
Phishing catch rate: 98.86%
Project Honey Pot SC rate: 98.62%
Abusix SC rate: 98.78%
Newsletters FP rate: 0.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence[2]

SC rate: 98.99%
FP rate: 0.03%
Final score: 98.84
Malware catch rate: 98.02%
Phishing catch rate: 98.20%
Project Honey Pot SC rate: 97.42%
Abusix SC rate: 99.29%
Newsletters FP rate: 0.8%

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 13 February to 12am on 1 March 2021 (GMT).

The test corpus consisted of 199,023 emails. 194,992 of these were spam, 31,303 of which were provided by *Project Honey Pot*, with the remaining 163,689 spam emails provided by *Abusix*. There were 3,909 legitimate emails ('ham') and 122 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

302 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[3]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 1,059 emails from the spam corpus were found to contain a malicious attachment while 1,835 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].

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)

2 This product is a partial solution. Such a solution has access only to part of the emails and does not receive the emails through SMTP.

[3] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review
[4] http://www.postfix.org/XCLIENT_README.html

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

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

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Axway	3908	1	0.03%	281	194469.4	99.86%	99.73	SPAM Verified
Bitdefender	3909	0	0.00%	127.8	194622.6	99.93%	99.93	SPAM + Verified
Cleanmail Domain Gateway	3908	1	0.03%	43.8	194706.6	99.98%	99.75	SPAM Verified
Cyren eXpurgate	3909	0	0.00%	689.4	194061	99.65%	99.62	SPAM + Verified
FortiMail	3908	1	0.03%	433.2	194317.2	99.78%	99.65	SPAM Verified
Libraesva	3909	0	0.00%	149.4	194601	99.92%	99.90	SPAM + Verified
Rspamd	3894	15	0.38%	19151.8	175598.6	90.17%	88.08	
Spamhaus DQS	3909	0	0.00%	558	194192.4	99.71%	99.64	SPAM + Verified
ZEROSPAM	3909	0	0.00%	2429.8	192303.6	98.75%	98.73	SPAM Verified
Abusix Mail Intelligence*	3908	1	0.03%	1958.8	192791.6	98.99%	98.84	N/A

**This product is a partial solution and its 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	0	0.00%	38	96.41%	26	98.58%	88.6	99.72%	192.4	99.88%	0.35
Bitdefender	0	0.00%	29	97.26%	17	99.07%	2	99.99%	125.8	99.92%	0.23
Cleanmail Domain Gateway	4	3.28%	0	100.00%	1	99.95%	8.4	99.97%	35.4	99.98%	0.14
Cyren eXpurgate	1	0.82%	14	98.68%	96	94.77%	335	98.93%	354.4	99.78%	0.59
FortiMail	0	0.00%	10	99.06%	25	98.64%	166	99.47%	267.2	99.84%	0.42
Libraesva	1	0.82%	0	100.00%	6	99.67%	80.2	99.74%	69.2	99.96%	0.23
Rspamd	7	5.74%	364	65.63%	456	75.15%	4826.4	84.51%	14325.4	91.24%	9.26
Spamhaus DQS	3	2.46%	69	93.48%	27	98.53%	259.8	99.17%	298.2	99.82%	0.59
ZEROSPAM	1	0.82%	0	100.00%	21	98.86%	431.4	98.62%	1998.4	98.78%	4.23
Abusix Mail Intelligence*	1	0.82%	21	98.02%	33	98.20%	803.8	97.42%	1155	99.29%	1.03

**This product is a partial solution and its performance should not be compared with that of other products. None of the queries to the IP blocklists included any information on the attachments; hence its 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	●	●	●	●
Cleanmail Domain Gateway	●	●	●	●
Cyren eXpurgate	●	●	●	●
FortiMail	●	●	●	●
Libraesva	●	●	●	●
Rspamd	●	●	●	●
Spamhaus DQS	●	●	●	●
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	
Bitdefender	99.93
Libraesva	99.90
Cleanmail Domain Gateway	99.75
Axway	99.73
FortiMail	99.65
Spamhaus DQS	99.64
Cyren eXpurgate	99.62
ZEROSPAM	98.73
Rspamd	88.08

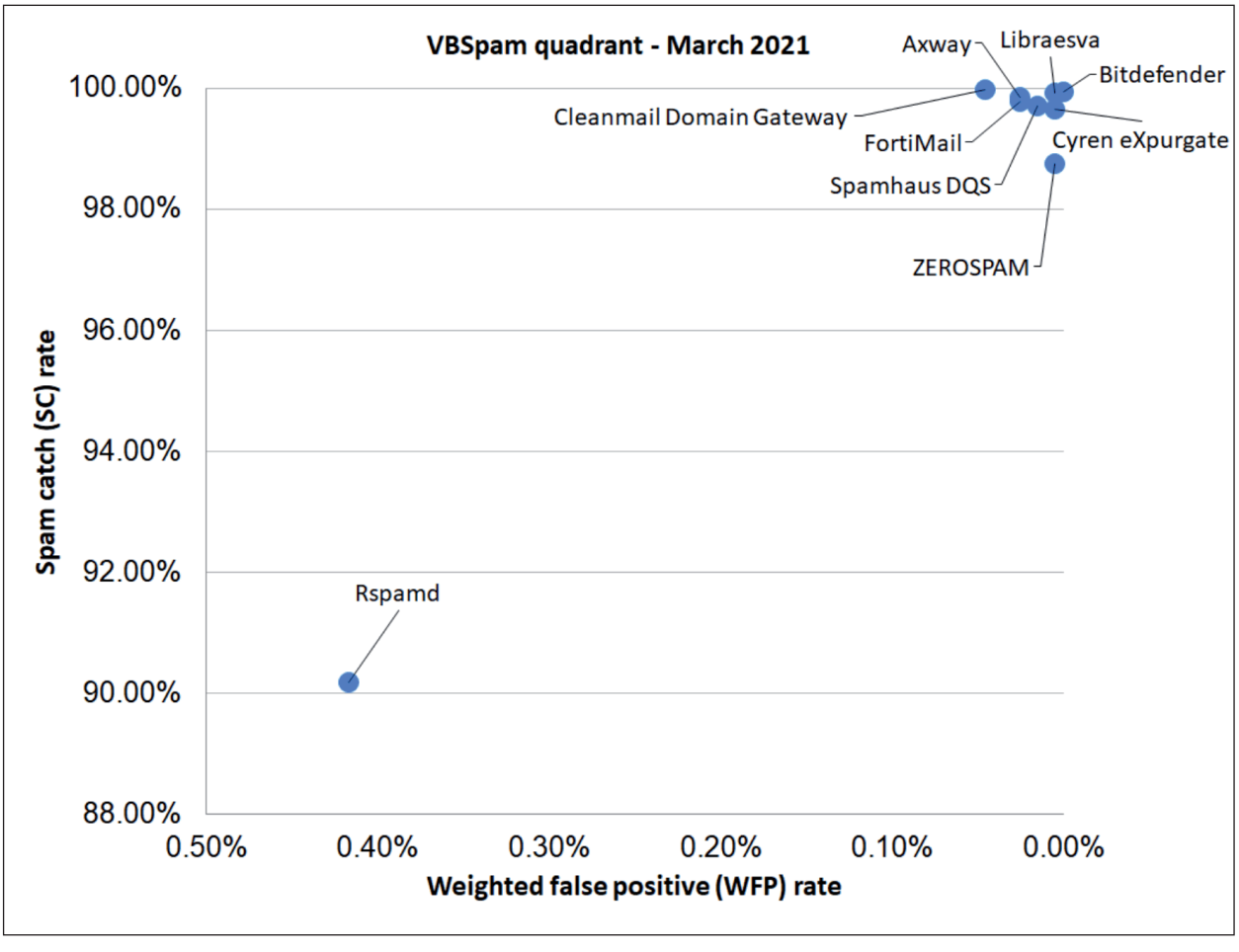
(Please refer to the text for full product names.)

Hosted solutions	**Anti-malware**	**IPv6**	**DKIM**	**SPF**	**DMARC**	**Multiple MX-records**	**Multiple locations**
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
Cyren eXpurgate	Avira SAVAPI	√	√	√	√	√	
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	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
Libraesva	ClamAV; others optional		√	√		√		√	
Rspamd	None					√			
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.)