

# virus

## BULLETIN

Covering the global threat landscape

### VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2022

*Ionuț Răileanu & Adrian Luca*

In this, the Q1 2022 VBSpam Test, which forms part of *Virus Bulletin's* continuously running security product test suite, six full email security solutions, one custom configured solution<sup>1</sup>, one open-source solution and two blocklists were assembled on the test bench to measure their

<sup>1</sup> *Spamhaus Data Query Service (DQS) + SpamAssassin* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

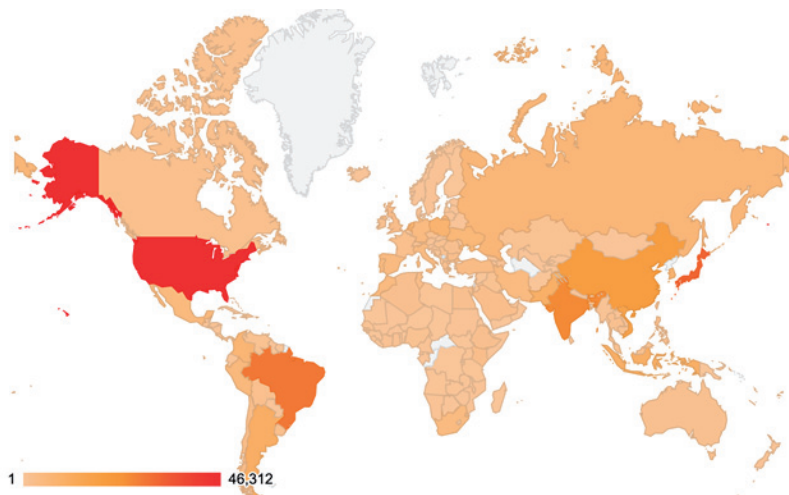
performance against various streams of wanted, unwanted and malicious emails.

This report highlights some of the latest email-related threats and how security solutions respond to them. Emotet reappeared shortly after the end of the Q4 2021 VBSpam test cycle, and in the Q1 2022 test it accounted for a large portion of the Malware corpus. During the test period, there was always at least one security solution that managed to block each of the threats we encountered.

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 during the test period.*)

#	Sender's IP country	Percentage of spam
1	United States	12.70%
2	Japan	8.76%
3	Brazil	7.77%
4	India	6.80%
5	China	5.02%
6	Vietnam	4.14%
7	Argentina	2.74%
8	Indonesia	2.64%
9	Pakistan	2.53%
10	Republic of Korea	2.08%

*Top 10 countries from which spam was sent.*



*Geographical distribution of spam based on sender IP address.*

## MALWARE AND PHISHING

In this section we highlight the malware and phishing campaigns that managed to evade the filters of most of the tested solutions. This is not intended to be an exhaustive analysis of these samples, rather we aim for this information to be of value for those interested in protecting and defending against some of the latest threats in the email landscape.

### Emotet

Having made a return to the threat landscape, the majority of the malicious samples<sup>2</sup> spotted in this test were linked to Emotet malspam campaigns. One campaign in particular managed to evade the filters of most of the tested solutions. The emails contained just a few lines of text and a password-protected archive.

The following are some of the characteristics of the malicious attachments:

#### Names:

Documento.zip  
latest-inquiry.tar.lz

<sup>2</sup> <https://bazaar.abuse.ch/sample/0bb184f9c3e9cda4571bd806b90dbda484c331d9dce7af784405fd211f6c71c4/>

### SHA256:

```
0bb184f9c3e9cda4571bd806b90dbda484c331d9dce
7af784405fd211f6c71c4
018eab1eef8c06c556addcc986a71b4c5beb6478945
706cbb6c929feeda71d65
15c365c0de7aa4340bfe6c7aa3fc2e6c6e55cc9b5b6
ee1c32d775ee5a5b4da97
```

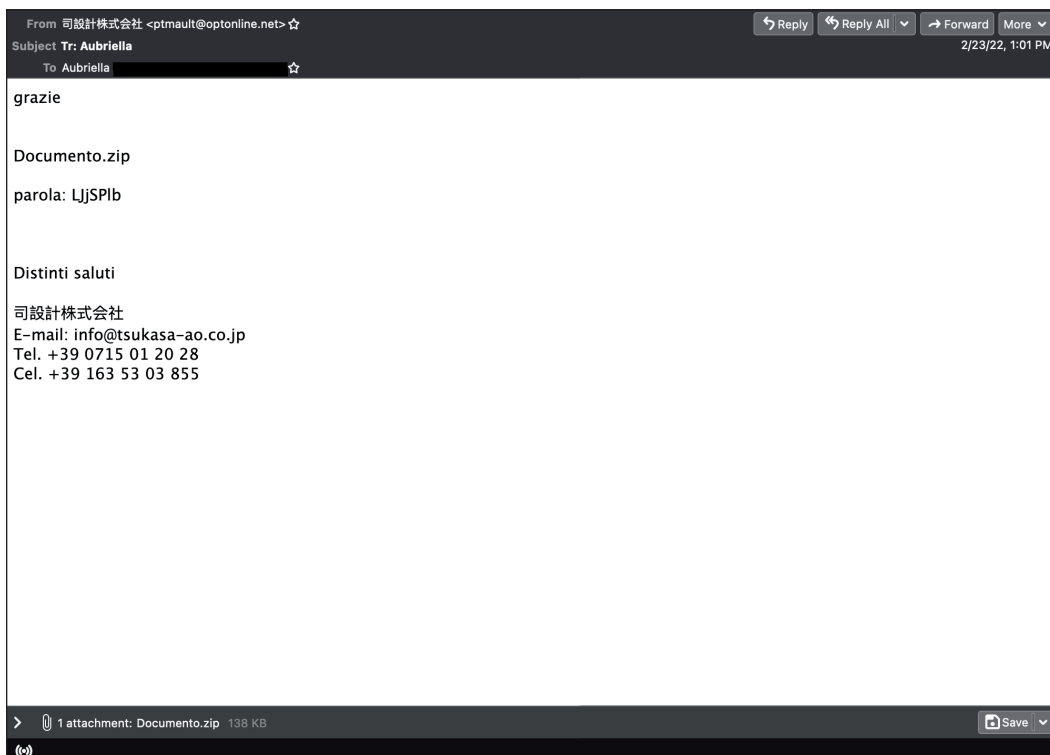
### GuLoader

GuLoader<sup>3</sup> is the name of a family of trojans that download and install additional malware. One malspam campaign caught our attention because it wasn't blocked by many of the tested solutions. We saw it active on 11 February for about an hour, from 09:30 to 10:30 UTC. The emails were sent from the same IP address, 161.35.194.187, and with the same email address in the 'From' header, g.randolph@otokar-tr.com.

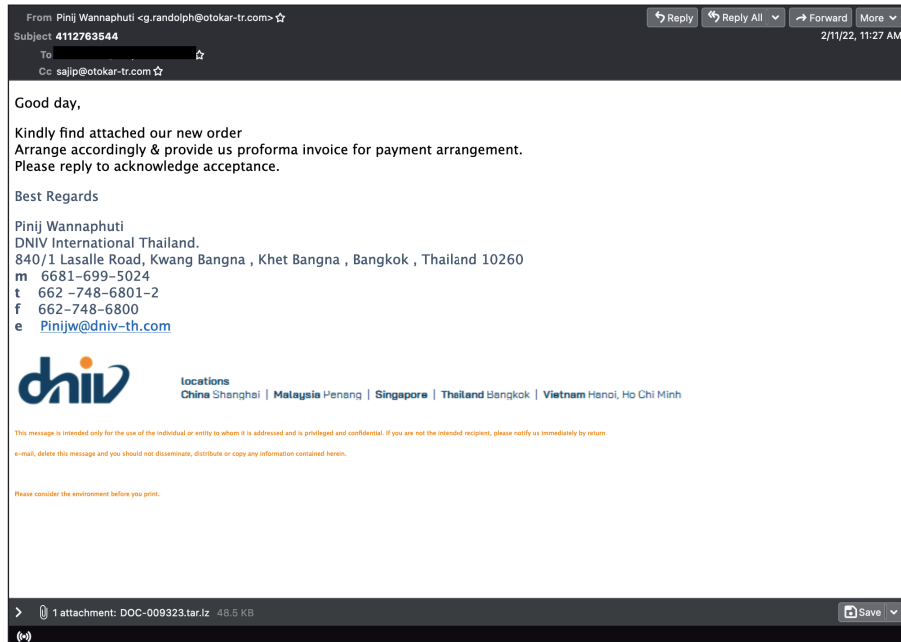
The attached archive<sup>4</sup> (78d5cacc818324c953c604fc93e8d2eddc212aa1e59afbf599efa9077d0bec0b), named DOC-009323.tar.lz, downloaded a vbs file which further loaded the GuLoader.

<sup>3</sup> <https://blog.malwarebytes.com/detections/trojan-guloader/>

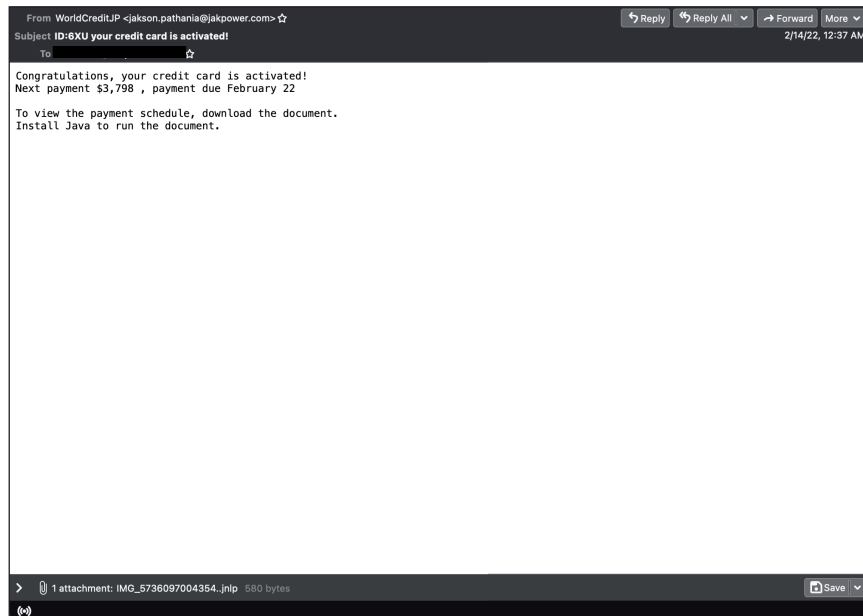
<sup>4</sup> [https://bazaar.abuse.ch/sample/b3b697f1100c8c075aaf74d735416c94ff4e6a4940dccb111c7183ea8a098739#file\\_info](https://bazaar.abuse.ch/sample/b3b697f1100c8c075aaf74d735416c94ff4e6a4940dccb111c7183ea8a098739#file_info)



Email from Emotet campaign.



*Email from GuLoader campaign.*



*Email with attachment that appears to download spyware associated with Vidar stealer.*

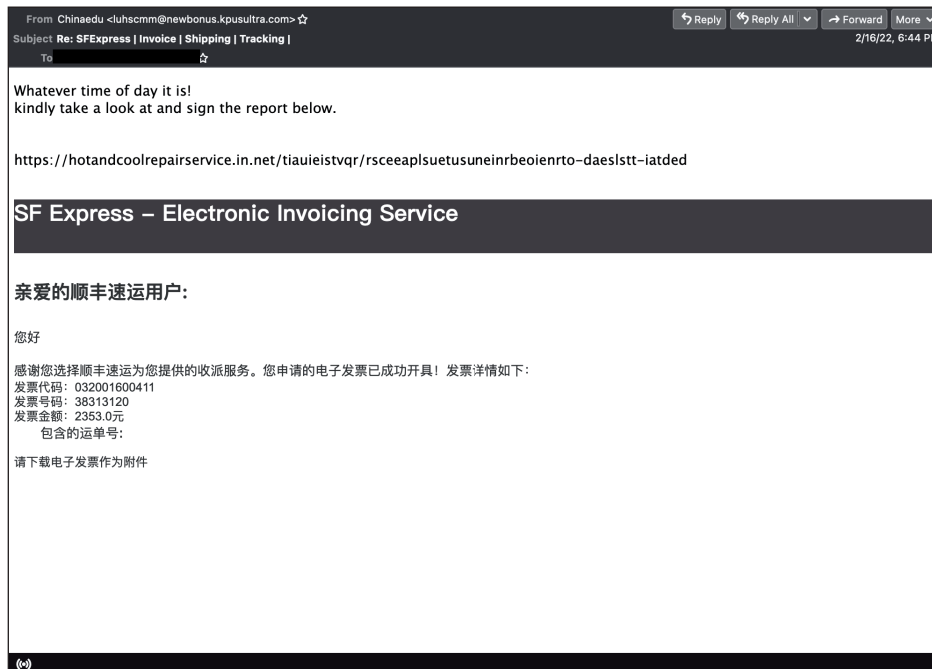
**Vidar stealer**

This is another brief campaign that we saw active for a short period on 13 February, from 22:40 to 22:51 UTC. It contained a jnlp attachment which, from our analysis, seems to download a piece of spyware associated with Vidar stealer.

The following are some features of the malicious attachments:

**Names:**

- IMG\_88162302..jnlp
- IMG\_573435033497856..jnlp
- IMG\_5736097004354..jnlp



Email from a Qakbot campaign.

**SHA256:**

102922875f9fd767c6dd985c2f54baaba13e0420afb  
 c0a42d45d5e80e3aca2b8  
 72d54d8d584434842dba9fefafa33608db0faaf25a2b0  
 02c390905ff32aae146b7  
 9963662ff89d728aa858d5d6fa2c1600c34532f94ea3  
 51d953d5b9174170e9b3

**Qakbot/Qbot<sup>5</sup>**

The majority of the missed phishing emails in the test were part of a Qakbot/Qbot spam campaign. The malicious URLs were injected into other conversations/emails. The URL itself wasn't clickable and in some cases it was reported to have no payload. In most cases on copying the URL and directly accessing it, a zip file was downloaded containing a malicious Office document.

**RESULTS**

The majority of the tested solutions managed to achieve high spam catch rates with values higher than 99%. A better comparison of performance can be made by analysing the products' malware and phishing catch rates (both of which are subsets of the Spam corpus). Of particular note was the

<sup>5</sup> <https://app.any.run/tasks/1bfd424-ed90-4b33-9611-d8d04f433630/>

performance of *Libraesva* with a 100% phishing catch rate and only two missed malware samples. Also noteworthy was *N-able Mail Assure*, which scored a 99.96% malware catch rate (just seven missed samples).

Of the participating full solutions, two – *Libraesva* and *Zoho Mail* – achieved a VBSpam award, whilst the other four – *Bitdefender*, *Cleanmail*, *Fortinet*, *N-able Mail Assure* – as well as the custom configured solution *Spamhaus Data Query Service (DQS)* + *SpamAssassin* all earned VBSpam+ certification.

**Bitdefender Security for Mail Servers 3.1.7**

- SC rate: 99.93%
- FP rate: 0.00%
- Final score: 99.93
- Malware catch rate: 98.84%
- Phishing catch rate: 99.73%
- Project Honey Pot SC rate: 100.00%
- Abusix SC rate: 99.93%
- MXMailData SC rate: 99.61%
- Newsletters FP rate: 0.0%
- Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



*Bitdefender* starts the year with a VBSpam+ award for the Q1 VBSpam Test. The product's results continue to be steady and reliable. It impresses with a 100% catch rate of the *Project Honey Pot* samples and with no false positives.

### Cleanmail Domain Gateway

**SC rate:** 99.91%

**FP rate:** 0.00%

**Final score:** 99.87

**Malware catch rate:** 99.40%

**Phishing catch rate:** 99.35%

**Project Honey Pot SC rate:** 99.93%

**Abusix SC rate:** 99.91%

**MXMailData SC rate:** 99.84%

**Newsletters FP rate:** 1.8%

**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

The developers of the *Cleanmail* product have good reason to be proud of their solution. The lack of false positives combined with a high spam catch rate earns them a VBSpam+ award for the current test. Also worthy of note are the higher than 99% malware and phishing catch rates.



### Fortinet FortiMail

**SC rate:** 99.77%

**FP rate:** 0.00%

**Final score:** 99.74

**Malware catch rate:** 97.28%

**Phishing catch rate:** 99.08%

**Project Honey Pot SC rate:** 99.84%

**Abusix SC rate:** 99.80%

**MXMailData SC rate:** 98.40%

**Newsletters FP rate:** 0.9%

**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

As in previous tests, *Fortinet* continues to show a balanced performance. The product's final score was a little influenced by a single false positive in the newsletter corpus, but remains high thanks to a 99.77% spam catch rate. In this test the product earns its fourth VBSpam+ certification in a row.



### Libraesva ESG v.4.7

**SC rate:** 99.97%

**FP rate:** 0.10%

**Final score:** 99.44

**Malware catch rate:** 99.99%

**Phishing catch rate:** 100.00%



**Project Honey Pot SC rate:** 99.95%

**Abusix SC rate:** 99.97%

**MXMailData SC rate:** 99.99%

**Newsletters FP rate:** 1.8%

**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

*Libraesva* continues to achieve the highest malware and phishing catch rates of all the products in the test. The product's spam catch rate is also impressive, with 99.97% of the samples being blocked, and it easily achieves a VBSpam award.

### N-able Mail Assure

**SC rate:** 99.94%

**FP rate:** 0.00%

**Final score:** 99.94

**Malware catch rate:** 99.96%

**Phishing catch rate:** 99.49%

**Project Honey Pot SC rate:** 99.90%

**Abusix SC rate:** 99.94%

**MXMailData SC rate:** 99.97%

**Newsletters FP rate:** 0.0%

**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

On only its third time participating in the VBSpam Test *N-able Mail Assure* takes first place in the final score rankings. The lack of false positives and spam catch rates higher than 99.90% earns it a VBSpam+ certification as well.



### Rspamd

**SC rate:** 99.10%

**FP rate:** 0.41%

**Final score:** 96.99

**Malware catch rate:** 90.93%

**Phishing catch rate:** 95.77%

**Project Honey Pot SC rate:** 98.47%

**Abusix SC rate:** 99.35%

**MXMailData SC rate:** 94.21%

**Newsletters FP rate:** 1.8%

**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

This is the fifth test in a row for open-source solution *Rspamd* and its results continue to get better each time. On this occasion it came very close to the final score threshold required for a VBSpam certification, missing it by only a shade over one percentage point, and achieving an impressive 99.10% spam catch rate.

## Spamhaus Data Query Service (DQS) + SpamAssassin

**SC rate:** 99.54%  
**FP rate:** 0.00%  
**Final score:** 99.54  
**Malware catch rate:** 97.40%  
**Phishing catch rate:** 97.65%  
**Project Honey Pot SC rate:** 99.20%  
**Abusix SC rate:** 99.59%  
**MXMailData SC rate:** 99.46%  
**Newsletters FP rate:** 0.0%  
**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

*Spamhaus Data Query Service + SpamAssassin* is a custom configured product that integrates the *Spamhaus DQS DNSBL* service and the free open-source *SpamAssassin* solution. In this test, the product showed a balanced performance with no false positives and a spam catch rate higher than 99.50%, a performance worthy of a VBSpam+ certification.



## Zoho Mail

**SC rate:** 99.69%  
**FP rate:** 0.02%  
**Final score:** 99.57  
**Malware catch rate:** 99.35%  
**Phishing catch rate:** 99.14%  
**Project Honey Pot SC rate:** 99.03%  
**Abusix SC rate:** 99.80%  
**MXMailData SC rate:** 99.40%  
**Newsletters FP rate:** 0.0%  
**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●

On its second participation in the VBSpam Test, *Zoho Mail* put in a very good performance. With malware and phishing catch rates higher than 99% and a final score of 99.57, *Zoho* easily achieves a VBSpam award.



## Abusix Mail Intelligence

**SC rate:** 99.42%  
**FP rate:** 0.00%  
**Final score:** 99.37  
**Malware catch rate:** 92.76%  
**Phishing catch rate:** 98.76%  
**Project Honey Pot SC rate:** 98.61%  
**Abusix SC rate:** 99.71%

**MXMailData SC rate:** 94.08%

**Newsletters FP rate:** 1.8%

*Abusix Mail Intelligence* is a set of blocklists that is tested as a partial solution because it has access only to parts of the emails (IP addresses, domains, URLs), which are queried as to their DNS zones. With this setup, the very high 99.42% spam catch rate and the lack of ham false positives is very impressive.

## Spamhaus Public Mirrors

**SC rate:** 73.43%  
**FP rate:** 0.24%  
**Final score:** 72.22  
**Malware catch rate:** 59.74%  
**Phishing catch rate:** 43.00%  
**Project Honey Pot SC rate:** 78.71%  
**Abusix SC rate:** 73.15%  
**MXMailData SC rate:** 57.69%  
**Newsletters FP rate:** 0.0%

*Spamhaus Public Mirrors* is a new entry in this test. It is tested as a partial solution because it has access only to parts of the emails (IP addresses, domains, URLs), which are queried as to their DNS zones.

## 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 19 days, from 12am on 5 February to 12am on 24 February 2022 (GMT) – the test period was three days longer than usual as a result of some technical issues experienced 8 to 9 February.

The test corpus consisted of 394,101 emails. 389,888 of these were spam, 48,953 of which were provided by *Project Honey Pot*, 330,478 were provided by Abusix with the remaining 10,457 spam emails provided by *MXMailData*. There were 4,103 legitimate emails ('ham') and 110 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

85 emails in the spam corpus were considered 'unwanted' (see the June 2018 report<sup>6</sup>) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 17,562 emails from the spam corpus were found to contain a malicious attachment while 3,709 contained a

<sup>6</sup> <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>

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<sup>7</sup>.

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:

$$\text{WFP rate} = (\# \text{false positives} + 0.2 * \min(\# \text{newsletter false positives}, 0.2 * \# \text{newsletters})) / (\# \text{ham} + 0.2 * \# \text{newsletters})$$

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:

$$\text{Final score} = \text{SC} - (5 * \text{WFP})$$

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.

<sup>7</sup>[http://www.postfix.org/XCLIENT\\_README.html](http://www.postfix.org/XCLIENT_README.html)

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:** Adrian Luca, Csaba Mészáros, Ionuț Răileanu  
**Operations Manager:** Bálint Tanos  
**Sales Executive:** Allison Sketchley  
**Editorial Assistant:** Helen Martin

© 2022 Virus Bulletin Ltd, Manor House - Office 6, Howbery Business Park, Wallingford OX10 8BA, UK  
 Tel: +44 20 3920 6348 Email: [editorial@virusbulletin.com](mailto:editorial@virusbulletin.com)  
 Web: <https://www.virusbulletin.com/>

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender	4103	0	0.00%	284	389536	99.93%	99.93	
Cleanmail Domain Gateway	4103	0	0.00%	334.2	389485.8	99.91%	99.87	
FortiMail	4103	0	0.00%	901.8	388918.2	99.77%	99.74	
Libraesva	4099	4	0.10%	115	389705	99.97%	99.44	
N-able Mail Assure	4103	0	0.00%	249.2	389570.8	99.94%	99.94	
Rspamd	4086	17	0.41%	3493.8	386326.2	99.10%	96.99	
Spamhaus Data Query Service (DQS) + SpamAssassin <sup>‡</sup>	4103	0	0.00%	1806.4	388013.6	99.54%	99.54	
Zoho Mail	4102	1	0.02%	1207	388613	99.69%	99.57	
Abusix Mail Intelligence*	4103	0	0.00%	2266.2	387553.8	99.42%	99.37	
Spamhaus Public Mirrors*	4093	10	0.24%	103575.2	286244.8	73.43%	72.22	

<sup>‡</sup>Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

\*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		MXMailData		STDev <sup>†</sup>
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender	0	0.0%	204	98.84%	10	99.73%	0	100.00%	243	99.93%	41	99.61%	0.32
Cleanmail Domain Gateway	2	1.8%	106	99.40%	24	99.35%	32.2	99.93%	285	99.91%	605	94.21%	0.25
FortiMail	1	0.9%	478	97.28%	34	99.08%	76.6	99.84%	658.2	99.80%	1	99.99%	0.49
Libraesva	2	1.8%	2	99.99%	0	100.00%	23.8	99.95%	90.2	99.97%	167	98.40%	0.12
N-able Mail Assure	0	0.0%	7	99.96%	19	99.49%	51.2	99.90%	195	99.94%	56	99.46%	0.18
Rspamd	2	1.8%	1593	90.93%	157	95.77%	749.6	98.47%	2139.2	99.35%	17	99.84%	1.39
Spamhaus Data Query Service (DQS) + SpamAssassin <sup>‡</sup>	0	0.0%	457	97.40%	87	97.65%	390.2	99.20%	1360.2	99.59%	63	99.40%	0.7
Zoho Mail	0	0.0%	114	99.35%	32	99.14%	474.8	99.03%	669.2	99.80%	3	99.97%	0.43
Abusix Mail Intelligence*	2	1.8%	1272	92.76%	46	98.76%	680.2	98.61%	967	99.71%	619	94.08%	1.02
Spamhaus Public Mirrors*	0	0.0%	7071	59.74%	2114	43.00%	10409	78.71%	88742.2	73.15%	4424	57.69%	20.45

<sup>†</sup> The standard deviation of a product is calculated using the set of its hourly spam catch rates.

<sup>‡</sup>Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

\*These products are partial solutions and their performance should not be compared with that of other products. None of the queries to the IP blocklist included any information on the attachments; hence their performance on the malware corpus is added purely for information. (Please refer to the text for full product names and details.)

	Speed			
	10%	50%	95%	98%
Bitdefender	●	●	●	●
Cleanmail Domain Gateway	●	●	●	●
FortiMail	●	●	●	●
Libraesva	●	●	●	●
N-able Mail Assure	●	●	●	●
Rspamd	●	●	●	●
Spamhaus Data Query Service (DQS) + SpamAssassin <sup>‡</sup>	●	●	●	●
Zoho Mail	●	●	●	●

● 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.)

<sup>‡</sup>Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

Products ranked by final score	
N-able Mail Assure	99.94
Bitdefender	99.93
Cleanmail Domain Gateway	99.87
FortiMail	99.74
Zoho Mail	99.57
Spamhaus Data Query Service (DQS) + SpamAssassin <sup>‡</sup>	99.54
Libraesva	99.44
Abusix Mail Intelligence*	99.37
Rspamd	96.99
Spamhaus Public Mirrors*	72.22

<sup>‡</sup>Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

\*These products are partial solutions and their performance should not be compared with that of other products.

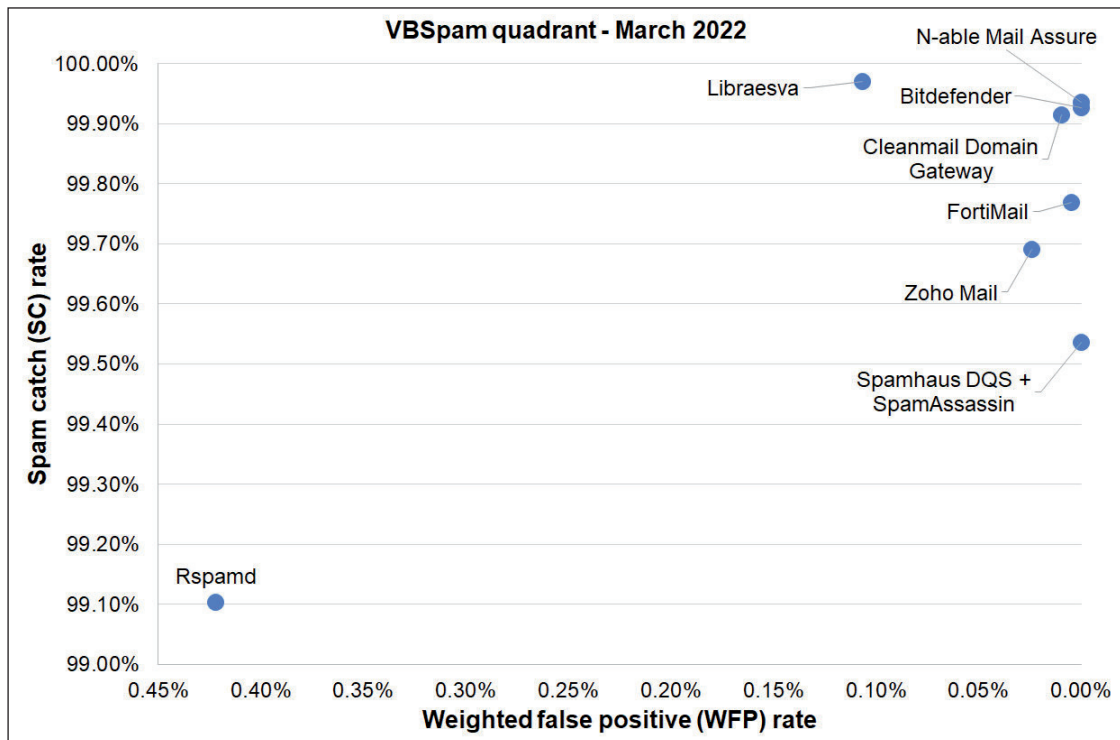
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
Zoho Mail	Zoho		√	√	√	√	√

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Bitdefender	Bitdefender	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
Libraesva	ClamAV; others optional		√	√		√		√	
Rspamd	None					√			
Spamhaus Data Query Service (DQS) + SpamAssassin <sup>‡</sup>	Optional	√	√	√					√

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

<sup>‡</sup>Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.



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