JUNE 2022

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2022

Ionuţ Răileanu & Adrian Luca

In this, the Q2 2022 VBSpam Test,which forms part of *Virus Bulletin*'s continuously running security product test suite, seven full email security solutions, one custom configured solution[1], one open-source solution and two blocklists were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

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

In this report we see a balanced performance from the tested solutions. There were very few false positives in the ham and newsletter test sets, although phishing emails proved to be a bit of a challenge, particularly those that were not in English.

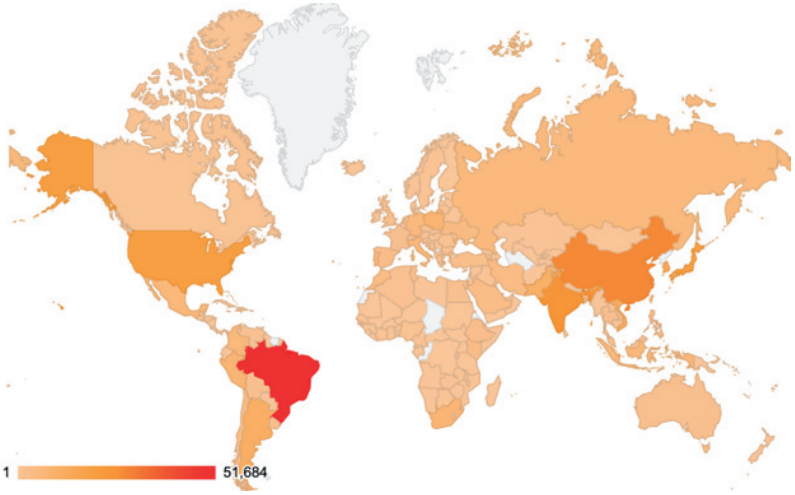
During the test period one in five emails containing malware were part of an Emotet campaign. There were also Agent Tesla and Qakbot-related samples that managed to evade detection.

Overall, however, the news is good: most of the email security solutions blocked more than 99% of all the spam emails.

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	Brazil	13.06%
2	China	7.13%
3	India	6.51%
4	United States	5.01%
5	Japan	4.79%
6	Republic of Korea	3.46%
7	Vietnam	3.07%
8	Argentina	2.88%
9	Pakistan	2.60%
10	Poland	2.07%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

MALWARE AND PHISHING

As in previous VBSpam reports, 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.

Agent Tesla

This sample evaded the filters of most of the tested solutions. It is reported to be linked to Agent Tesla[2].

The attachment has a '.tar.lz' archive (4c6b715a1e83fbfa42e25f01676e1da5588b1ffeeaba9bb6f8c6972a16c477f5), not password protected, that contains an '.scr' executable file.

The email was sent from 209.85.208.51, a *Google* IP address, and the content seems crafted to avoid text-based detection.

The sample wasn't part of a larger campaign and it very much looks like a targeted spam.

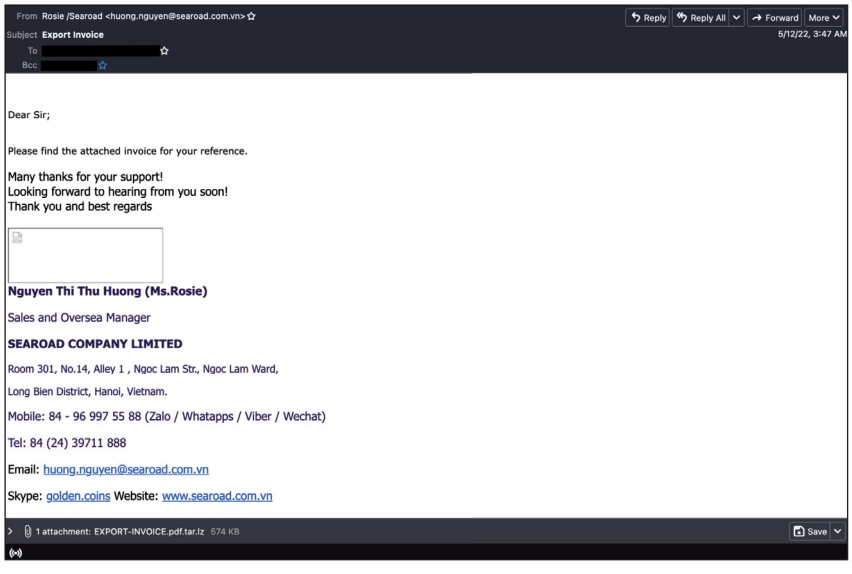
Emotet

Around 20% of the malware samples from this test were linked to Emotet[3]. There was no pause in this campaign, which was active during the 16 days the test ran, with a spike on 12 May.

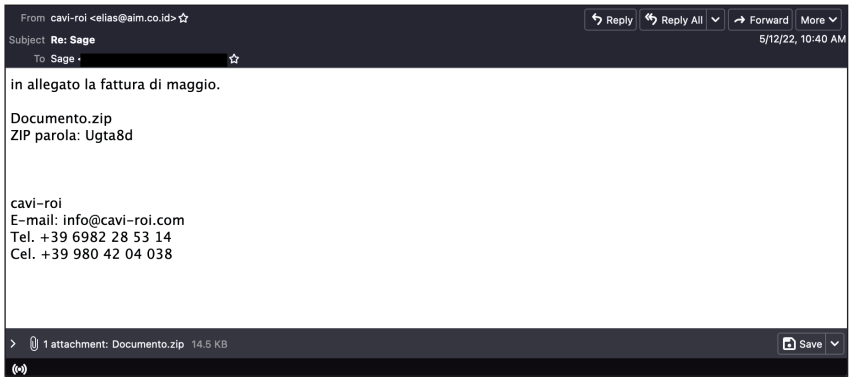
The samples contain little text and a password-protected zip archive, with the password shared in the text of the email. Most of the missed samples were in languages other than English.

[2] https://bazaar.abuse.ch/sample/2b21885c68cf8bcee3be7e08574372130a42c74a047b1f962cc5e270bb7b543e/#intel.

[3] https://bazaar.abuse.ch/sample/bcb53af88c2eb7a3e04c8874854a6c4fc0a2b9890ed39cc4bc9c1f7ef6380563/.



Agent Tesla sample.

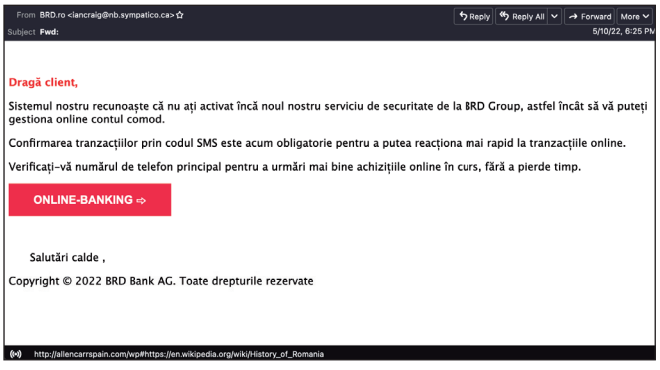


Emotet sample.

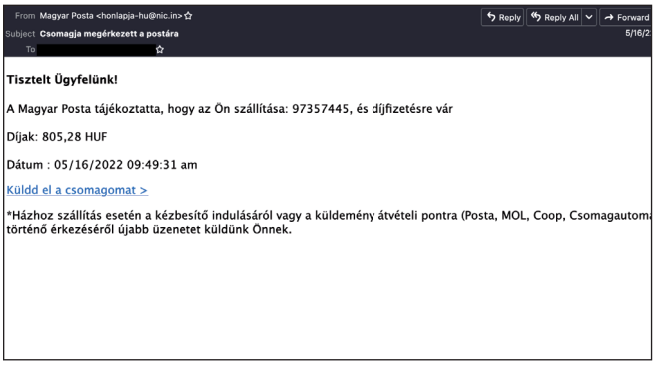
Non-English phishing

In this test we continued to observe that the majority of the phishing emails that passed through the email filters were in languages other than English.

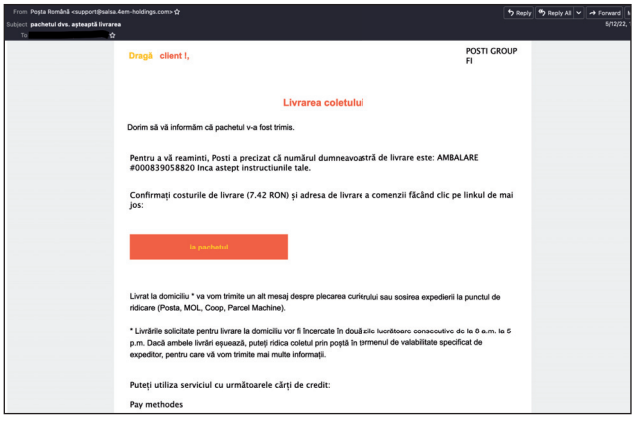
The examples shown below are not related to each other or part of a large campaign but they highlight the diversity of the phishing samples we saw in the wild. What all these samples have in common, beside the one Romanian banking email, is that in all the cases the attackers try to leverage the local postal services to convince the recipients to click on the malicious links.



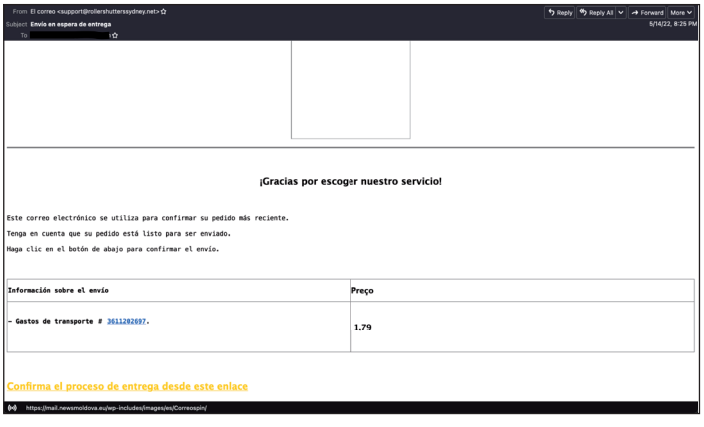
The phishing sample missed by most of the tested solutions.



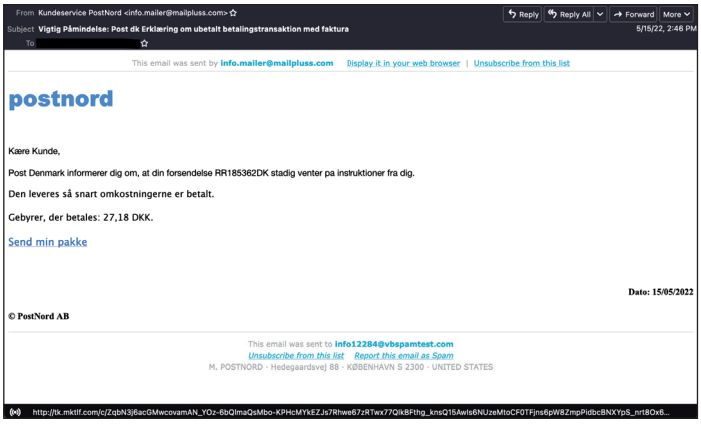
Example of a Hungarian phishing email.



Another example of a phishing email in Romanian.



Example of a Spanish phishing email.



Example of a Danish phishing email.

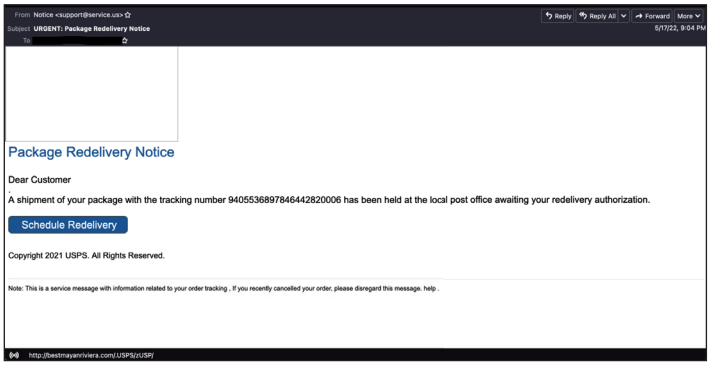
English phishing

Even though the majority of English phishing emails were blocked by the email filters, there were some that broke through. Below are two examples of this kind (masquerading as messages from UPS and Netflix). For both of them, the attackers used cloud hosting services (*AWS*, *Beget*) to send the emails. The IP addresses from which the emails were sent were `54.240.8.13` and `87.236.19.240`.

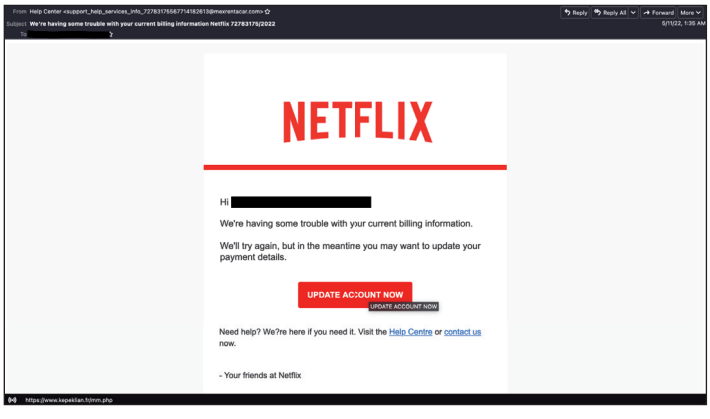
Qakbot

Compared to the previous quarterly tests, there weren't many Qakbot-related samples in this test, but we mention this sample because was missed by several of the security solutions.

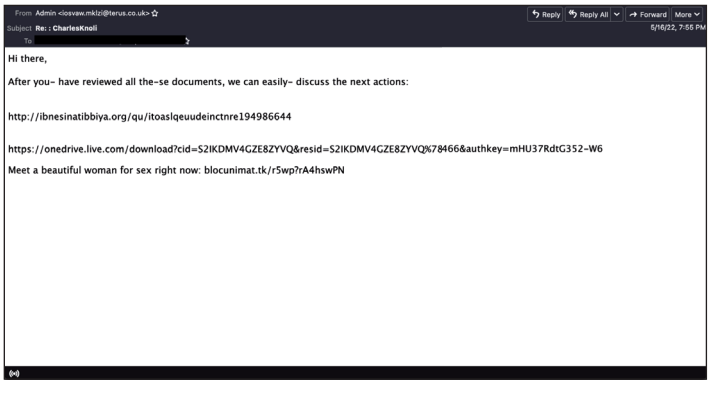
The template is similar to what we have seen in the past, file-hosting service URLs temporarily used to access malicious files. The emails were sent as replies to others.



UPS phishing email.



Netflix phishing email.



Qakbot example.

RESULTS

The majority of the tested solutions managed to achieve very good spam catch rates, with values exceeding 99%. A better comparison between the solutions can be made by looking at the malware and phishing catch rates, subsets of the spam corpus. Here, we highlight the performance of *Cleanmail*, *Libraesva* and *SEPPmail*, all with 100% malware catch rate. No solution achieved a 100% catch rate in the phishing corpus but *SEPPmail* deserves a mention for having missed only two samples of this kind.

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

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Malware catch rate: 98.81%
Phishing catch rate: 99.76%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.94%
MXMailData SC rate: 98.58%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The Q2 test of 2022 sees *Bitdefender* earning another VBSpam+ award, continuing the product's impressive record. With a 99.93% spam catch rate and no ham or newsletter false positives, the Romania-based company has every reason to be proud of its steady and reliable solution.

Cleanmail Domain Gateway

SC rate: 99.96%
FP rate: 0.03%
Final score: 99.74
Malware catch rate: 100.00%
Phishing catch rate: 99.59%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.96%
MXMailData SC rate: 100%
Newsletters FP rate: 1.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Not a single malware sample got past *Cleanmail*'s filters. With a 99.96% spam catch rate and all ham emails returned in less than 30 seconds, it was just one false positive in the ham corpus that stood between *Cleanmail* and a VBSpam+ award. Nevertheless, it earns VBSpam certification with ease.

Fortinet FortiMail

SC rate: 99.92%
FP rate: 0.00%
Final score: 99.92
Malware catch rate: 99.81%
Phishing catch rate: 99.32%
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.93%
MXMailData SC rate: 99.60%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

FortiMail continues a run of VBSpam+ awards, this time making it five in a row. With malware and phishing catch rates higher than 99%, no false positives of any kind and green labels at all the speed percentiles, we can only congratulate and highlight one of the most balanced email security solutions in the test.

Libraesva ESG v.4.7

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.94
Malware catch rate: 100.00%
Phishing catch rate: 99.73%
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.97%
MXMailData SC rate: 100%
Newsletters FP rate: 0.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

No malicious email managed to get past *Libraesva*'s filters. Despite one false positive in the newsletter corpus, *Libraesva* ranks top in the final score rankings with an impressive 99.94. Needless to say, the product earns another VBSpam+ certification to add to its collection.

N-able Mail Assure

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.88

N-able Mail Assure contd

Malware catch rate: 99.99%
Phishing catch rate: 99.41%
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.91%
MXMailData SC rate: 100%
Newsletters FP rate: 0.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

N-able Mail Assure continues the run of good performance, blocking more than 99.90% of spam emails as well as more than 99% of the malware and phishing samples. With no false positives in the ham corpus, all the criteria for a VBSpam+ certification are met.

Rspamd

SC rate: 97.73%
FP rate: 0.44%
Final score: 95.37
Malware catch rate: 59.82%
Phishing catch rate: 95.32%
Project Honey Pot SC rate: 96.70%
Abusix SC rate: 98.22%
MXMailData SC rate: 57.23%
Newsletters FP rate: 5.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test the open-source solution struggled a little in dealing with the malware samples. However, the numbers are encouraging on the entire spam corpus, with a 97.73% catch rate. Unfortunately the solution didn't quite meet the criteria to earn VBSpam certification.

SEPPmail.cloud Filter

SC rate: 99.995%
FP rate: 0.00%
Final score: 99.84
Malware catch rate: 100.00%
Phishing catch rate: 99.94%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.996%
MXMailData SC rate: 100%
Newsletters FP rate: 4.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

On its first participation in the VBSpam tests *SEPPMail* is impressive, with no false negatives in the malware set, only two phishing samples missed, and almost a 100% spam catch rate with just 18 spam samples missed. Due to five newsletter false positives it narrowly misses out on a VBSpam+ award this time, but it earns VBSpam certification with ease.

Spamhaus Data Query Service (DQS) + SpamAssassin

SC rate: 99.74%
FP rate: 0.00%
Final score: 99.74
Malware catch rate: 99.60%
Phishing catch rate: 98.19%
Project Honey Pot SC rate: 99.25%
Abusix SC rate: 99.76%
MXMailData SC rate: 99.30%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service + SpamAssassin is a custom configured solution that integrates the *Spamhaus DQS* DNSBL service and the free open-source solution *SpamAssassin*. In this test the solution shows a balanced performance with no false positives and a spam catch rate higher than 99.70%, thus earning VBSpam+ certification.

Zoho Mail

SC rate: 99.15%
FP rate: 0.00%
Final score: 99.15
Malware catch rate: 83.77%
Phishing catch rate: 99.44%
Project Honey Pot SC rate: 97.86%
Abusix SC rate: 99.35%
MXMailData SC rate: 84.61%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With a 99.15% spam catch rate and no false positives in the ham or newsletter test sets, *Zoho Mail* is awarded VBSpam certification. It is worth highlighting the product's impressive phishing catch rate, which exceeds 99%.

Abusix Mail Intelligence

SC rate: 98.43%
FP rate: 0.00%

Final score: 98.40
Malware catch rate: 45.27%
Phishing catch rate: 99.14%
Project Honey Pot SC rate: 97.92%
Abusix SC rate: 99.01%
MXMailData SC rate: 48.41%
Newsletters FP rate: 0.9%

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, it's impressive that the product manages to achieve a spam catch rate of 98.43% and zero ham false positives.

Spamhaus Public Mirrors

SC rate: 53.85%
FP rate: 0.09%
Final score: 53.38
Malware catch rate: 8.04%
Phishing catch rate: 48.83%
Project Honey Pot SC rate: 54.86%
Abusix SC rate: 54.29%
MXMailData SC rate: 11.75%
Newsletters FP rate: 0.0%

This is the second time *Spamhaus Public Mirrors* has participated in the VBSpam test. The product 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 16 days, from 12am on 7 May to 12am on 23 May 2022 (GMT).

The test corpus consisted of 398,959 emails. Of these, 395,646 were spam, 13,030 of which were provided by *Project Honey Pot*, 378,328 were provided by *Abusix*, and the remaining 4,288 spam emails were provided by *MXMailData*. There were 3,204 legitimate emails (or 'ham') and 109 newsletters – a category that includes various kinds of commercial and non-commercial opt-in mailings.

97 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[4]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 9,248 emails from the spam corpus were found to contain a malicious attachment while 3,375 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[5].

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:

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

● (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: Adrian Luca, Csaba Mészáros, Ionuț Răileanu
Operations Manager: Bálint Tanos
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
Bitdefender	3204	0	0.00%	290.4	395278	99.93%	99.93	SPAM + Verified
Cleanmail Domain Gateway	3203	1	0.03%	152	395416.4	99.96%	99.74	SPAM Verified
FortiMail	3204	0	0.00%	321.4	395247	99.92%	99.92	SPAM + Verified
Libraesva	3204	0	0.00%	107.6	395460.8	99.97%	99.94	SPAM + Verified
N-able Mail Assure	3204	0	0.00%	367.8	395200.6	99.91%	99.88	SPAM + Verified
Rspamd	3186	18	0.56%	8977.8	386590.6	97.73%	95.37	
SEPPmail.cloud Filter	3204	0	0.00%	18	395550.4	99.995%	99.84	SPAM Verified
Spamhaus Data Query Service (DQS) + SpamAssassin‡	3204	0	0.00%	1032	394536.4	99.74%	99.74	SPAM + Verified
Zoho Mail	3204	0	0.00%	3378	392190.4	99.15%	99.15	SPAM Verified
Abusix Mail Intelligence*	3204	0	0.00%	6209.4	389359	98.43%	98.40	N/A
Spamhaus Public Mirrors*	3201	3	0.09%	182560.6	213007.8	53.85%	53.38	N/A

‡*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 SpamAssasssin. 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†
	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%	110	98.81%	8	99.76%	1	99.99%	228.4	99.94%	61	98.58%	0.49
Cleanmail Domain Gateway	2	1.8%	0	100.00%	14	99.59%	8	99.94%	144	99.96%	0	100.00%	0.18
FortiMail	0	0.0%	18	99.81%	23	99.32%	21	99.84%	283.4	99.93%	17	99.60%	0.51
Libraesva	1	0.9%	0	100.00%	9	99.73%	10.8	99.92%	96.8	99.97%	0	100.00%	0.17
N-able Mail Assure	1	0.9%	1	99.99%	20	99.41%	28.4	99.78%	339.4	99.91%	0	100.00%	0.38
Rspamd	6	5.5%	3716	59.82%	158	95.32%	429	96.70%	6714.8	98.22%	1834	57.23%	5.93
SEPPmail. cloud Filter	5	4.6%	0	100.00%	2	99.94%	4	99.97%	14	99.996%	0	100.00%	0.07
Spamhaus Data Query Service (DQS) + SpamAssassin‡	0	0.0%	37	99.60%	61	98.19%	97.8	99.25%	904.2	99.76%	30	99.30%	0.72
Zoho Mail	0	0.0%	1501	83.77%	19	99.44%	277.8	97.86%	2440.2	99.35%	660	84.61%	2.47
Abusix Mail Intelligence*	1	0.9%	5061	45.27%	29	99.14%	270.4	97.92%	3727	99.01%	2212	48.41%	5.27
Spamhaus Public Mirrors*	0	0.0%	8504	8.04%	1727	48.83%	5863.4	54.86%	172913.2	54.29%	3784	11.75%	11.99

† *The standard deviation of a product is calculated using the set of its hourly spam catch rates.*

‡ *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 SpamAssasssin. 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	🟢	🟢	🟢	🟢
SEPPmail.cloud Filter	🟢	🟢	🟢	🟡
Spamhaus Data Query Service (DQS) + SpamAssassin‡	🟢	🟢	🟢	🟢
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.)

‡*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 SpamAssasssin. 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	
Libraesva	99.94
Bitdefender	99.93
FortiMail	99.92
N-able Mail Assure	99.88
SEPPmail.cloud Filter	99.84
Cleanmail Domain Gateway	99.74
Spamhaus Data Query Service (DQS) + SpamAssassin‡	99.74
Zoho Mail	99.15
Abusix Mail Intelligence*	98.40
Rspamd	95.37
Spamhaus Public Mirrors*	53.38

‡*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 SpamAssasssin. 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.*

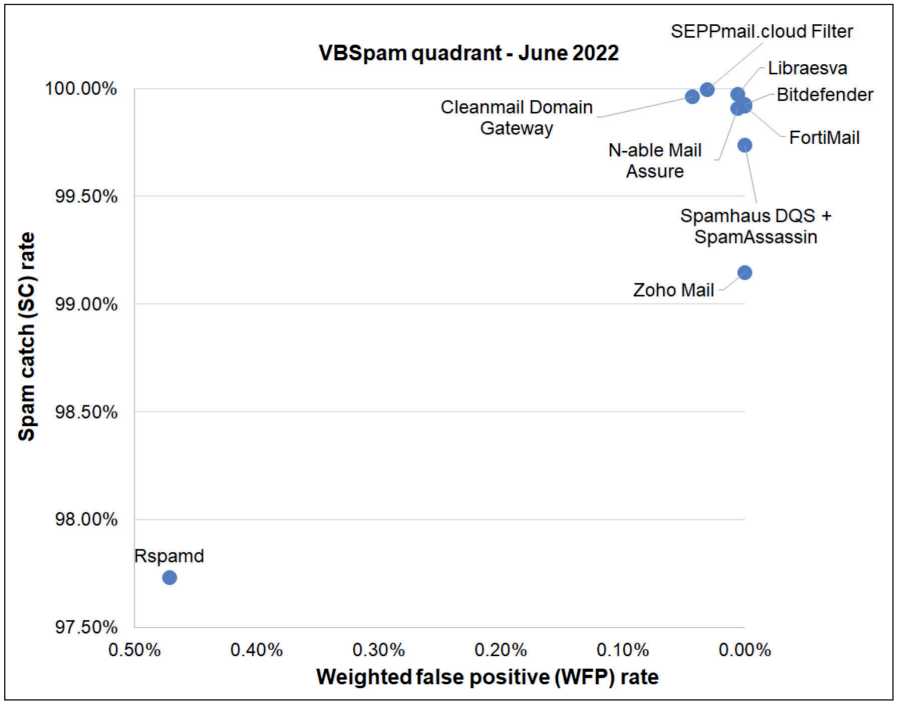
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

(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‡	Optional	√	√	√					√

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

‡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 SpamAssasssin. 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.)