

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW DECEMBER 2022

Ionuț Răileanu & Adrian Luca

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – we measured the performance of a number of email security solutions against various streams of wanted, unwanted and malicious emails. One third of the solutions we tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished). The solutions tested publicly were eight full email security solutions, one custom configured solution¹, one open-source solution and one blocklist.

This Q4 2022 report marks the 70th VBSpam test since VBSpam certification began in 2009 – we thank all those

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	Brazil	10.16%
2	China	6.93%
3	Japan	6.28%
4	India	5.45%
5	United States	5.20%
6	Argentina	4.11%
7	France	3.16%
8	Republic of Korea	3.08%
9	Vietnam	2.71%
10	Peru	2.19%

Top 10 countries from which spam was sent.

who have participated, and on this occasion we also welcome *Mimecast*, which makes its VBSpam debut in this test.

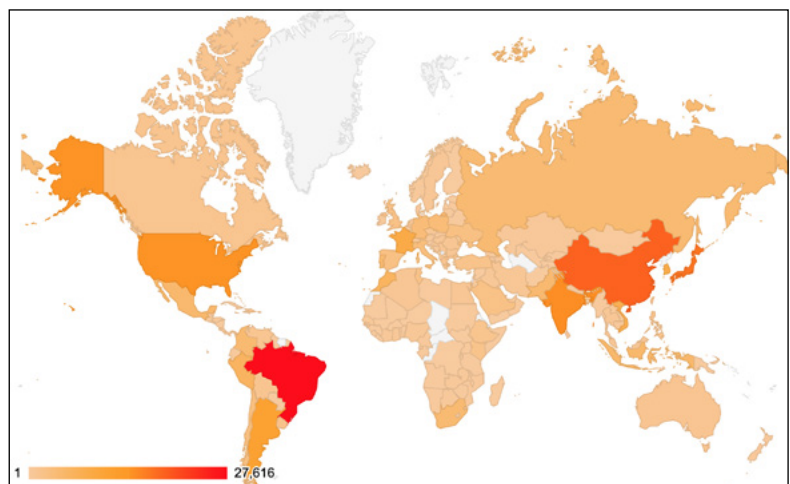
During the 16 days in which the test ran we saw a fair number of malware and phishing attacks, but the security solutions proved to be a good line of defence, blocking the majority of spam samples in the test.

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.*)

MALWARE AND PHISHING

Agent Tesla

This malware sample was one of those that managed to escape detection by most of the solutions in the test. It



Geographical distribution of spam based on sender IP address.

was reported to have been linked with Agent Tesla². We saw only two samples of this kind, each with the same gz archive attached. The Agent Tesla remote access trojan (RAT) was hidden in the archive with an inflated executable. The following are some features:

- **Subject:** po
- **Mail From:** kittinan@tomasaccesorios[.]com[.]ar
- **Attachment name:** G88AH33-339.gz
- **Attachment SHA256:** 6d9efa19352da2c7a37b43b5c854f660c562b93ef07711f1186cce78cebfafd0
- **First seen:** 10 November at 02:38 UTC and 08:09 UTC

² <https://bazaar.abuse.ch/sample/720b7352f254c6ad7bd16506d5a1d51ce7813da9d0bfe5b9657e5b959ad14ec5/>

Emotet

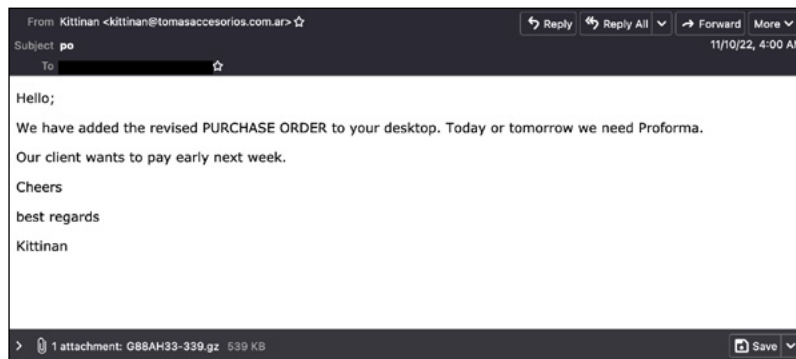
The Emotet malspam campaign continues to evolve, representing a recurring challenge for security solutions. The emails contain a few lines of text and a password to open the password-protected attachment.

A new feature³ of this particular Emotet campaign is the attacker's attempt to get the user to manually copy the malicious xls file to a location that is bypassed by default by *Microsoft Office* scanners.

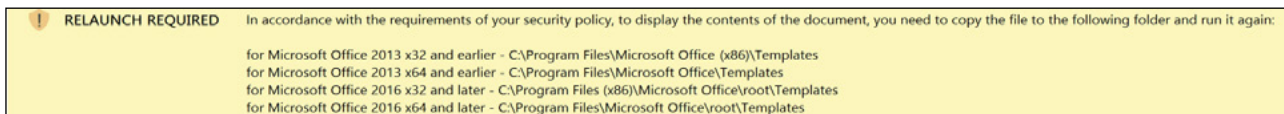
Banking phishing

We continue to see a diversity of languages in the most commonly missed phishing emails. In this test, these happened to be banking phishing emails, abusing social media shortening URLs (t[.]co, lnkd[.]in).

³ <https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return>



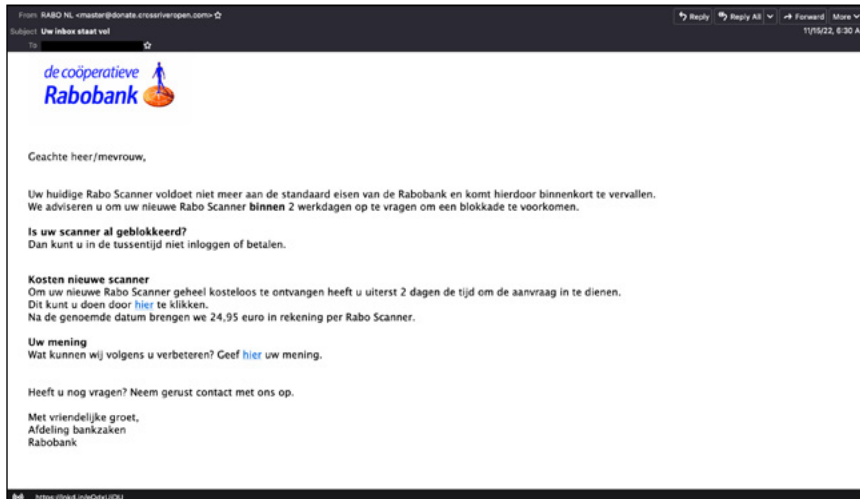
Malspam sample with an Agent Tesla infected attachment.



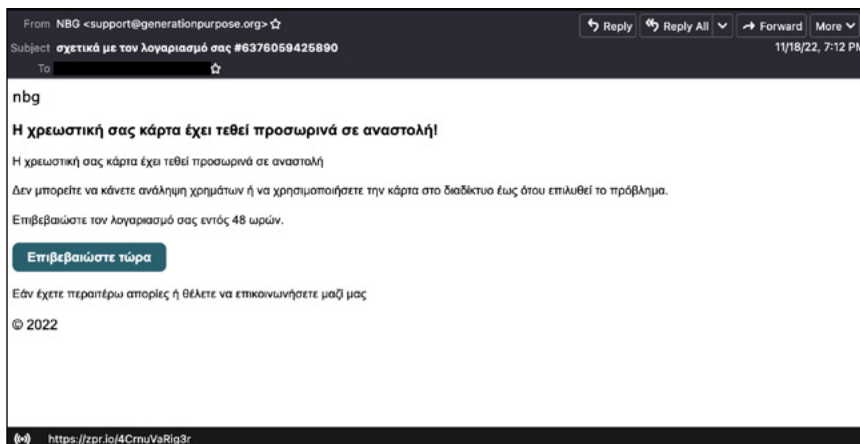
Content of the Emotet xls infected files.



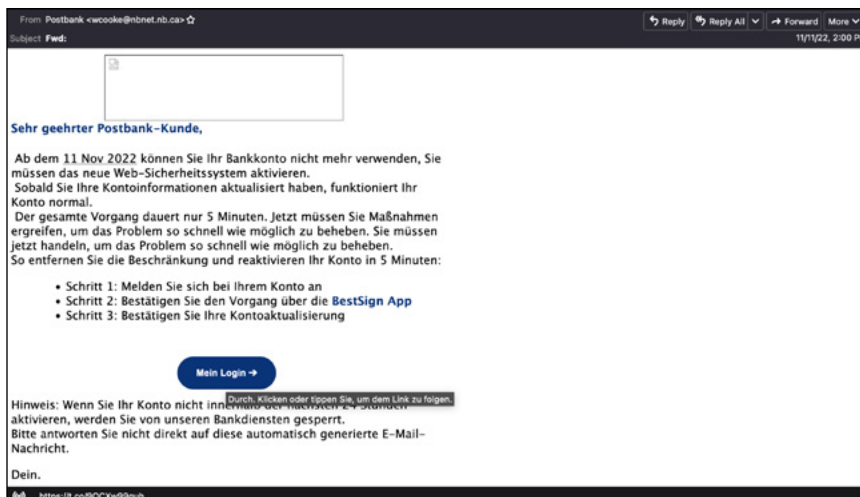
Malspam sample with an Emotet infected attachment.



German banking phishing sample using a [lnkd.fj.in](https://lnkd.fj.in/90Cw99guh) shortening URL.



Greek banking phishing sample.



German phishing sample using a [t.f.co](https://t.co/90Cw99guh) shortening URL.

RESULTS

The majority of the tested solutions achieved spam catch rates of more than 99%. A better comparison can be made by analysing the products' performance against the malware and phishing sets, both of which are subsets of the spam corpus. Here we highlight the performance of *Cleanmail* and *Mimecast*, which both achieved a 100% malware catch rate, as well as that of *Bitdefender*, which only missed one phishing sample.

Of the participating full solutions, one (*Zoho Mail*) achieved a VBSpam award, while seven were awarded a VBSpam+ certification: *Bitdefender*, *Cleanmail*, *Fortinet*, *Mimecast*, *N-able Mail Assure*, *N-able SpamExperts* and *SEPPmail*.

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.98%
 FP rate: 0.00%
 Final score: 99.98
 Malware catch rate: 99.82%
 Phishing catch rate: 99.98%
 Project Honey Pot SC rate: 99.99%
 Abusix SC rate: 99.98%
 MXMailData SC rate: 99.87%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Bitdefender's performance in the Q4 2022 VBSpam test is impressive. The product's VBSpam+ certification streak continues, this time with a final score of 99.98, the highest phishing catch rate in this test, and no ham or newsletter false positives.

Cleanmail Domain Gateway

SC rate: 99.94%
 FP rate: 0.00%
 Final score: 99.94
 Malware catch rate: 100.00%
 Phishing catch rate: 99.55%
 Project Honey Pot SC rate: 99.91%
 Abusix SC rate: 99.95%
 MXMailData SC rate: 100.00%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



No malware sample managed to evade *Cleanmail's* filters, and the product correctly classified all ham and newsletter samples. With a spam catch rate of 99.94%, *Cleanmail* easily achieves VBSpam+ certification.

Fortinet FortiMail

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.97
 Malware catch rate: 99.84%
 Phishing catch rate: 99.90%
 Project Honey Pot SC rate: 99.94%
 Abusix SC rate: 99.97%
 MXMailData SC rate: 99.75%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet's performance in this test was impressive too. With catch rates exceeding 99% in the malware, phishing and spam sets, and no false positives of any kind, *Fortinet* earns a VBSpam+ award.

Mimecast

SC rate: 99.94%
 FP rate: 0.00%
 Final score: 99.90
 Malware catch rate: 100.00%
 Phishing catch rate: 99.43%
 Project Honey Pot SC rate: 99.62%
 Abusix SC rate: 99.96%
 MXMailData SC rate: 100.00%
 Newsletters FP rate: 1.1%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Mimecast makes a strong debut in the VBSpam test. Alongside a perfect performance on the malware corpus, we highlight the lack of ham false positives and a 99.94% spam catch rate. The product earns a VBSpam+ award on its first visit to the VBSpam test bench.

N-able Mail Assure

SC rate: 99.91%
 FP rate: 0.00%
 Final score: 99.91
 Malware catch rate: 99.84%
 Phishing catch rate: 99.06%
 Project Honey Pot SC rate: 99.71%
 Abusix SC rate: 99.93%
 MXMailData SC rate: 99.92%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



It was another great performance for *N-able Mail Assure* in the Q4 2022 VBSpam test. With malware, phishing and spam catch rates all exceeding 99%, and no ham or newsletter false positives, the product is awarded VBSpam+ certification.

N-able SpamExperts

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Malware catch rate: 99.84%
Phishing catch rate: 99.06%
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.93%
MXMailData SC rate: 99.92%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



N-able's second entry in this test, *SpamExperts*, put in a similarly impressive performance, also achieving malware, phishing and spam catch rates in excess of 99% and a zero false positive score. Thus *SpamExperts* is also awarded VBSpam+ certification.

Rspamd

SC rate: 97.63%
FP rate: 0.93%
Final score: 92.93
Malware catch rate: 63.58%
Phishing catch rate: 91.11%
Project Honey Pot SC rate: 96.60%
Abusix SC rate: 98.04%
MXMailData SC rate: 62.73%
Newsletters FP rate: 2.1%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test, the open-source *Rspamd* struggled a little with the samples in the malware corpus, but the numbers for the overall spam corpus are encouraging, with a decent catch rate of 97.63%.

SEPPmail.cloud Filter

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.95
Malware catch rate: 99.92%
Phishing catch rate: 99.92%



Project Honey Pot SC rate: 99.86%

Abusix SC rate: 99.99%

MXMailData SC rate: 99.87%

Newsletters FP rate: 1.1%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The developers of the Swiss-based *SEPPmail* solution have good reason to be proud of their product, which achieved the highest spam catch rate in this test, alongside a zero false positive rate. What's more, the product scored over 99.90% against the malware and phishing sets. *SEPPmail* earns a VBSpam+ award.

Spamhaus Data Query Service + SpamAssassin

SC rate: 97.79%
FP rate: 0.00%
Final score: 97.79
Malware catch rate: 99.35%
Phishing catch rate: 98.07%
Project Honey Pot SC rate: 98.49%
Abusix SC rate: 97.72%
MXMailData SC rate: 99.07%
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 combined solution correctly identified all ham and newsletter samples, and although it didn't reach the VBSpam certification threshold we highlight its impressive malware and phishing catch rates.

Zoho Mail

SC rate: 99.64%
FP rate: 0.00%
Final score: 99.52
Malware catch rate: 97.33%
Phishing catch rate: 99.02%
Project Honey Pot SC rate: 99.13%
Abusix SC rate: 99.70%
MXMailData SC rate: 97.14%
Newsletters FP rate: 3.2%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail achieved a decent overall spam catch rate exceeding 99.60%. We continued to see a good performance on the phishing samples as well, with a 99.02% catch



rate and no ham false positives. *Zoho Mail* easily earns a VBSpam award.

Abusix Mail Intelligence

SC rate: 99.02%

FP rate: 0.00%

Final score: 98.94

Malware catch rate: 65.28%

Phishing catch rate: 96.80%

Project Honey Pot SC rate: 95.16%

Abusix SC rate: 99.66%

MXMailData SC rate: 63.02%

Newsletters FP rate: 2.1%

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 to their DNS zones. With this setup, the 99.02% spam catch rate and lack of ham false positives is very impressive.

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 5 November to 12am on 21 November 2022 (GMT).

The test corpus consisted of 274,599 emails. 271,927 of these were spam, 19,409 of which were provided by *Project Honey Pot*, 250,141 were provided by *Abusix*, with the remaining 2,377 spam emails provided by *MXMailData*. There were 2,578 legitimate emails ('ham') and 94 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

112 emails in the spam corpus were considered 'unwanted' (see the June 2018 report⁴) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 3,860 emails from the spam corpus were found to contain a malicious attachment while 4,881 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.

⁴ <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>.

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 command⁵.

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.

⁵ 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

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender	2578	0	0.00%	41.8	271795.6	99.98%	99.98	
Cleanmail Domain Gateway	2578	0	0.00%	150.6	271686.8	99.94%	99.94	
FortiMail	2578	0	0.00%	86.4	271751	99.97%	99.97	
Mimecast	2578	0	0.00%	165.4	271672	99.94%	99.90	
N-able Mail Assure	2578	0	0.00%	234.4	271603	99.91%	99.91	
N-able SpamExperts	2578	0	0.00%	232.4	271605	99.91%	99.91	
Rspamd	2554	24	0.93%	6440	265397.4	97.63%	92.93	
SEPPmail.cloud Filter	2578	0	0.00%	43.4	271794	99.98%	99.95	
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	2578	0	0.00%	6011.8	265825.6	97.79%	97.79	
Zoho Mail	2578	0	0.00%	986	270851.4	99.64%	99.52	
Abusix Mail Intelligence*	2578	0	0.00%	2676.8	269160.6	99.02%	98.94	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 SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.*

**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		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%	7	99.82%	1	99.98%	1	99.99%	41	99.98%	3	99.87%	0.12
Cleanmail Domain Gateway	0	0.0%	0	100.00%	22	99.55%	17	99.91%	136	99.95%	0	100.00%	0.27
FortiMail	0	0.0%	6	99.84%	5	99.90%	12	99.94%	70	99.97%	6	99.75%	0.19
Mimecast	1	1.1%	0	100.00%	28	99.43%	73.8	99.62%	98	99.96%	0	100.00%	0.4
N-able Mail Assure	0	0.0%	6	99.84%	46	99.06%	56.8	99.71%	178	99.93%	2	99.92%	0.48
N-able SpamExperts	0	0.0%	6	99.84%	46	99.06%	55.8	99.71%	177	99.93%	2	99.92%	0.47
Rspamd	2	2.1%	1406	63.58%	434	91.11%	658.2	96.60%	4915	98.04%	886	62.73%	5.28
SEPPmail.cloud Filter	1	1.1%	3	99.92%	4	99.92%	27	99.86%	15	99.99%	3	99.87%	0.16
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	0	0.0%	25	99.35%	94	98.07%	291.8	98.49%	5706	97.72%	22	99.07%	8.7
Zoho Mail	3	3.2%	103	97.33%	48	99.02%	168.6	99.13%	763	99.69%	68	97.14%	0.93
Abusix Mail Intelligence*	2	2.1%	1340	65.28%	156	96.80%	936.4	95.16%	863	99.65%	879	63.02%	2.5

[†]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 SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

*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 blocklist included any information on the attachments; hence its 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	●	●	●	●
Mimecast	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
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 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	
Bitdefender	99.98
FortiMail	99.97
SEPPmail.cloud Filter	99.95
Cleanmail Domain Gateway	99.94
N-able SpamExperts	99.91
N-able Mail Assure	99.91
Mimecast	99.90
Zoho Mail	99.52
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	97.79
Rspamd	92.93

[‡]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.

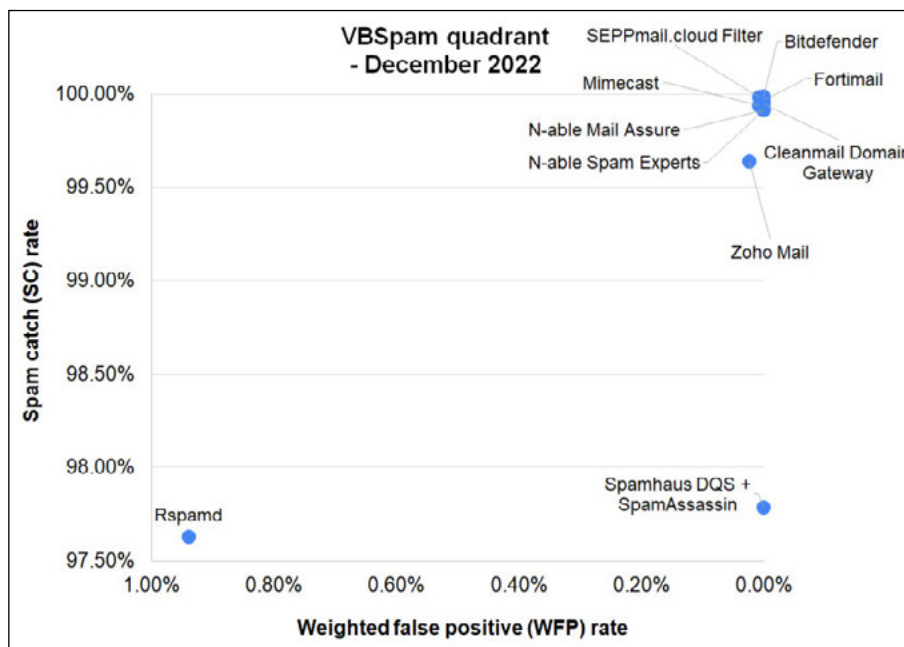
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail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