

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW DECEMBER 2023

Ionuț Răileanu & Adrian Luca

In the Q4 2023 VBSpam 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tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished).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.

Out of the eight full email security solutions, six blocked 100% of malware samples while the other two blocked more than 99.50%. It seems that emails containing

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

malicious attachments no longer present much of a problem. *Microsoft's* decision to disable macros by default in *Office* apps for *Windows* users may have contributed to bad actors' lack of interest in this kind of threat.

However, though not on quite the same level, we also see a good performance from the security solutions against phishing emails, with detection rates for the most part higher than 99.50%.

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.*)

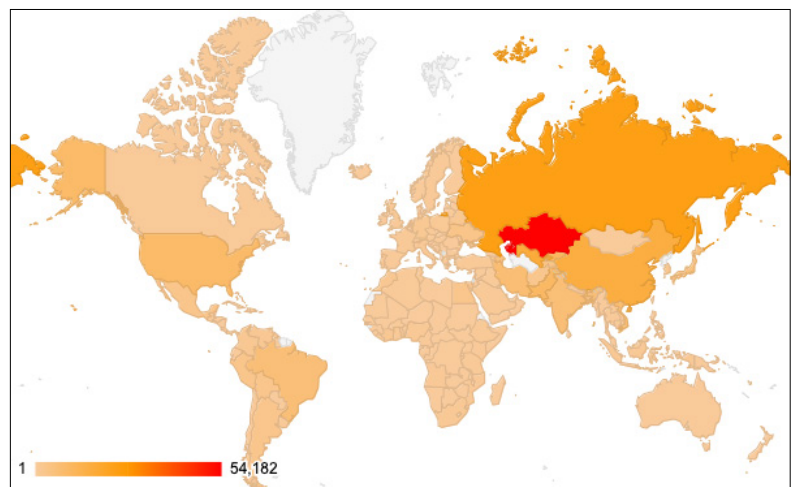
HIGHLIGHTS

Non-English phishing emails

We continue to see the same trend as we noted in previous reports: most of the missed phishing samples are in

#	Sender's IP country	Percentage of spam
1	Kazakhstan	20.69%
2	Russian Federation	8.93%
3	Uzbekistan	6.36%
4	China	5.98%
5	Kyrgyzstan	3.93%
6	Pakistan	3.68%
7	United States	3.40%
8	Islamic Republic of Iran	2.64%
9	Vietnam	2.64%
10	India	2.45%

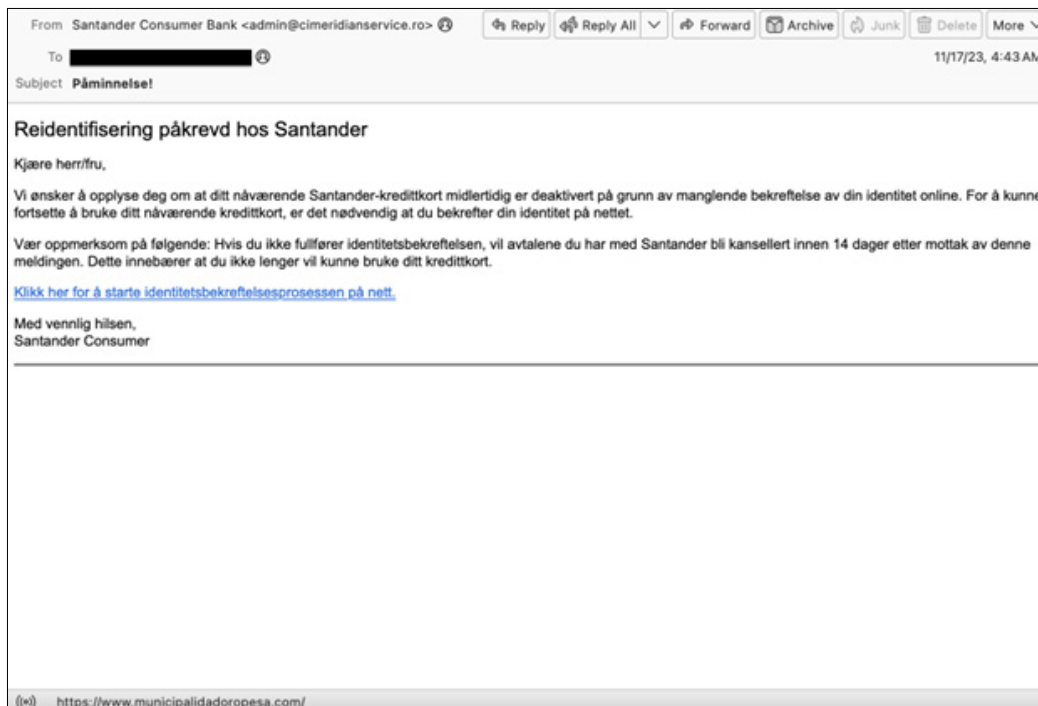
Top 10 countries from which spam was sent.



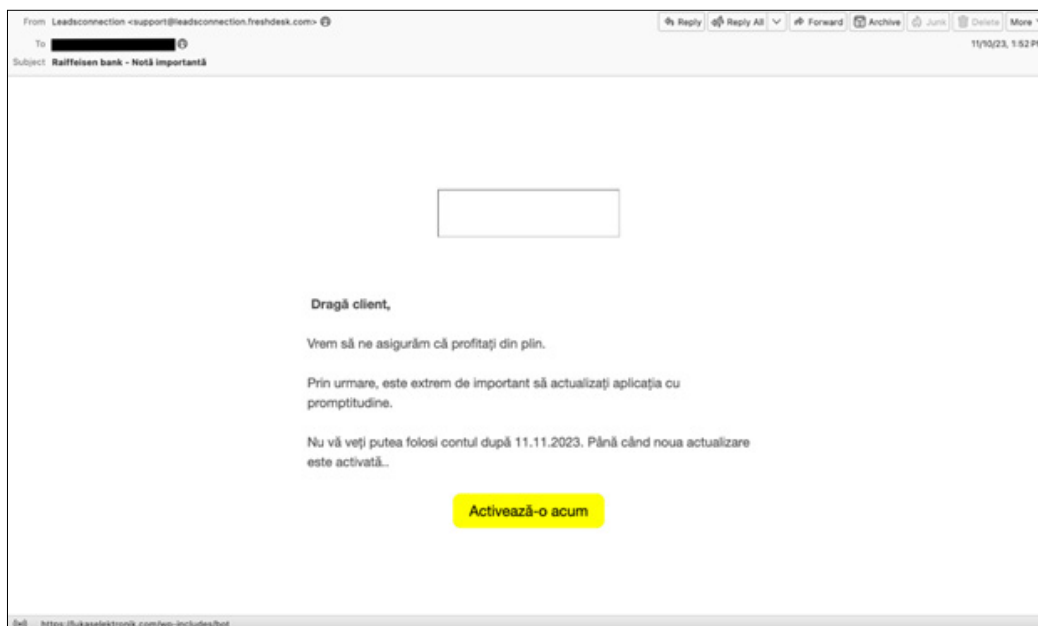
Geographical distribution of spam based on sender IP address.

languages other than English. The following screenshots show the phishing emails that evaded the filters of the

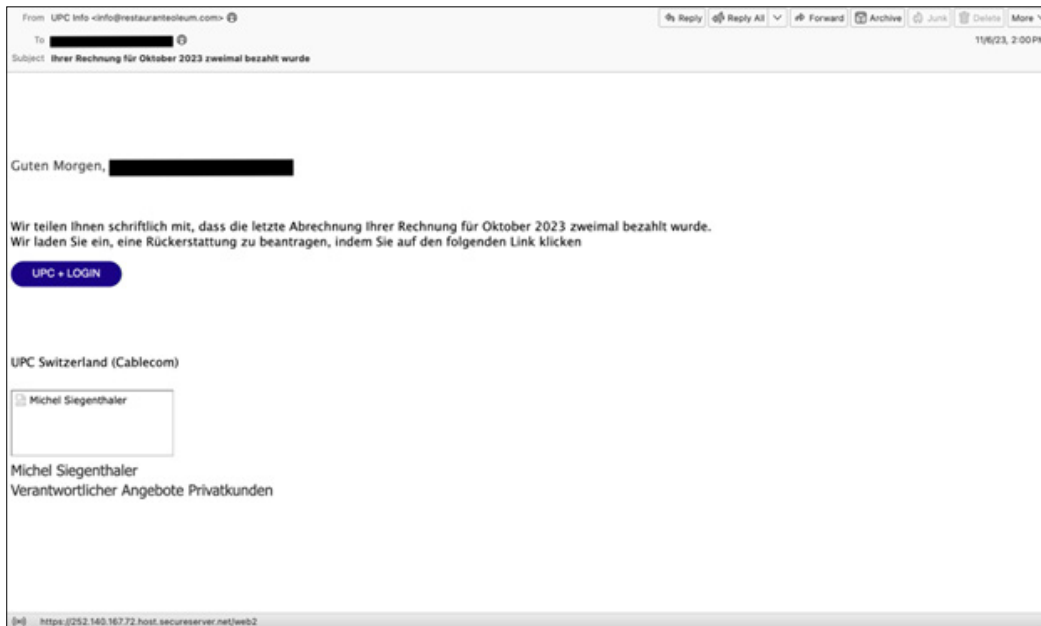
majority of the tested solutions: Norwegian, Romanian, German and Hungarian samples.



Norwegian phishing sample.



Romanian phishing sample.



German phishing sample.



Hungarian phishing sample.

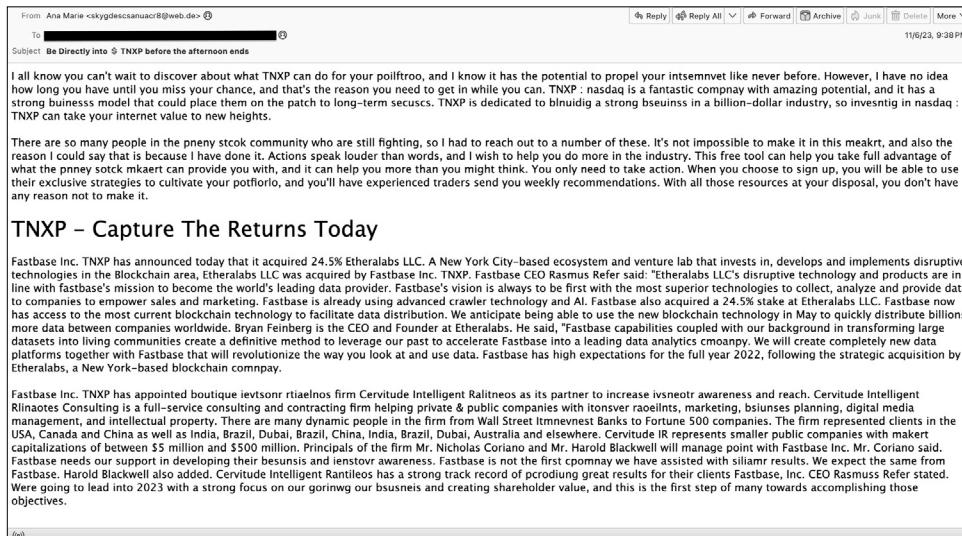
Financial spam

From time to time, we see short duration spam campaigns that are missed by the majority of the solutions we test. The emails advertise certain stocks that historically reached high values but which have now dropped to less than \$1. There are no URLs or attachments, and many of the words seem

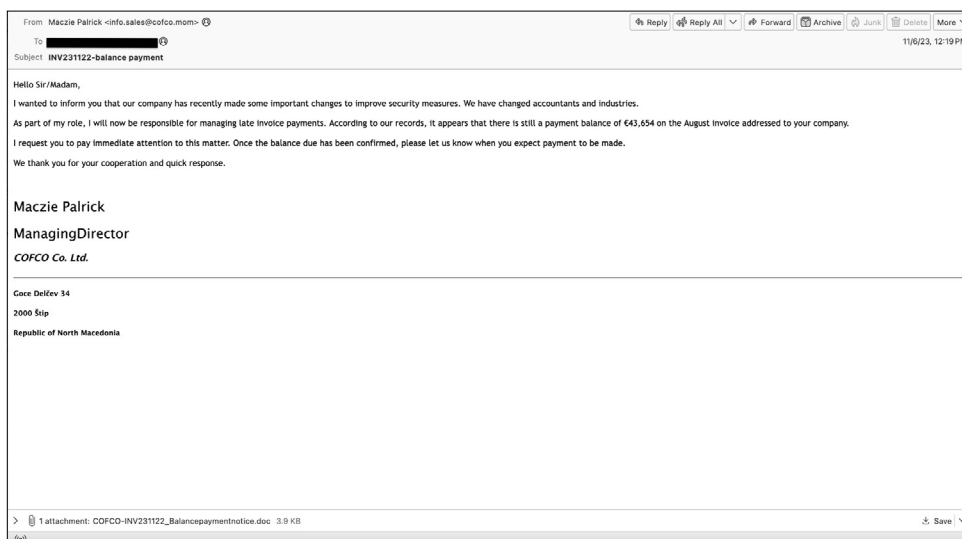
to be skewed on purpose, to make it challenging to filter.

LokiBot

Most of the tested solutions managed to successfully block all the malware samples. There was only one challenging sample that warrants a mention here.



Financial spam sample.



LokiBot sample.

The attachment contains a ‘.doc’ file using a macro to access an external link that downloads the payload, a ‘.exe’ file. The ‘.exe’ file is reported² to be linked to the LokiBot malware.

RESULTS

The majority of the tested solutions managed to achieve high catch rates both on overall spam samples and on the malware sub-category, with values higher than 99%. In

² <https://www.virustotal.com/gui/file/30de8327003cc6cb8d30fdea5758aafc01481714fd9c280278bafc70bb36f2cc/behavior>

particular, we highlight the performance of *SEPPmail.cloud Filter*, which missed only one phishing sample.

Of the participating full solutions, two achieved a VBSpam award – *SEPPmail.cloud Filter* and *Zoho Mail* – while six – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *N-able Mail Assure*, *N-Able SpamExperts* and *Net At Work NoSpamProxy* – were awarded a VBSpam+ certification, as was the custom configured solution *Spamhaus DQS*.

(Note: since, for a number of products, catch rates and/or final scores were very close to, whilst remaining a fraction below, 100%, in this test we quote all the spam-related scores with three decimal places.)

Bitdefender GravityZone Premium

SC rate: 99.990%
 FP rate: 0.00%
 Final score: 99.990
 Malware catch rate: 99.800%
 Phishing catch rate: 99.770%
 Project Honey Pot SC rate: 99.985%
 Abusix SC rate: 99.992%
 MXMailData SC rate: 99.770%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another impressive performance from *Bitdefender*, and the vendor's uninterrupted series of VBSpam+ awards continues in the Q4 2023 VBSpam test. While blocking 99.99% of the spam samples, the product correctly filtered all of the legitimate samples.



No malware sample was able to get past *Mimecast's* filters, and there were no false positives of any kind. With a final score of 99.967, *Mimecast* earns VBSpam+ certification for its performance in the Q4 2023 VBSpam Test.

N-able Mail Assure

SC rate: 99.982%
 FP rate: 0.00%
 Final score: 99.982
 Malware catch rate: 100.000%
 Phishing catch rate: 99.510%
 Project Honey Pot SC rate: 99.831%
 Abusix SC rate: 99.990%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

N-able Mail Assure continued the run of good performances in this test, earning the product another VBSpam+ award. Beside the 100% malware catch rate we highlight the lack of ham false positives and the higher than 99% phishing catch rate.



Fortinet FortiMail

SC rate: 99.995%
 FP rate: 0.00%
 Final score: 99.995
 Malware catch rate: 100.000%
 Phishing catch rate: 100.000%
 Project Honey Pot SC rate: 99.931%
 Abusix SC rate: 99.998%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was an almost perfect performance from *Fortinet* in this test: no false positives, a 100% catch rate on both malware and phishing, and only 13 false negatives. The product easily earns its VBSpam+ certification.



N-able SpamExperts

SC rate: 99.982%
 FP rate: 0.00%
 Final score: 99.982
 Malware catch rate: 100.000%
 Phishing catch rate: 99.510%
 Project Honey Pot SC rate: 99.831%
 Abusix SC rate: 99.990%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With identical scores to its sister product, *N-able SpamExperts* also earns VBSpam+ certification in this test.



Mimecast

SC rate: 99.967%
 FP rate: 0.00%
 Final score: 99.967
 Malware catch rate: 100.000%
 Phishing catch rate: 99.770%
 Project Honey Pot SC rate: 99.519%
 Abusix SC rate: 99.990%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Net At Work NoSpamProxy

SC rate: 99.988%
 FP rate: 0.00%
 Final score: 99.945
 Malware catch rate: 100.000%
 Phishing catch rate: 99.770%
 Project Honey Pot SC rate: 99.954%
 Abusix SC rate: 99.990%



MXMailData SC rate: 100.000%
Newsletters FP rate: 1.4%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another balanced performance for *Net at Work's* email security solution, resulting in another VBSpam+ award to add to its collection. Particularly of note were the lack of false positives and the higher than 99.9% spam catch rate.

Rspamd

SC rate: 98.750%
FP rate: 1.00%
Final score: 93.688
Malware catch rate: 65.740%
Phishing catch rate: 89.410%
Project Honey Pot SC rate: 89.585%
Abusix SC rate: 99.557%
MXMailData SC rate: 61.600%
Newsletters FP rate: 2.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The highlight for *Rspamd* in the Q4 2023 VBSpam Test was its 98.75% spam catch rate – the highest value achieved by the open-source product this year and one of the best since it joined the VBSpam test.

SEPPmail.cloud Filter

SC rate: 99.998%
FP rate: 0.04%
Final score: 99.739
Malware catch rate: 100.000%
Phishing catch rate: 99.960%
Project Honey Pot SC rate: 99.968%
Abusix SC rate: 100.000%
MXMailData SC rate: 100.000%
Newsletters FP rate: 1.4%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Only four spam samples were missed by *SEPPmail.cloud Filter* – a truly impressive performance and the best across all the 2023 quarterly VBSpam tests. A number of false positives brought the final score down a touch, but the product easily earns VBSpam certification.

Spamhaus Data Query Service + SpamAssassin

SC rate: 99.902%
FP rate: 0.00%
Final score: 99.902



Malware catch rate: 96.800%
Phishing catch rate: 97.930%
Project Honey Pot SC rate: 99.937%
Abusix SC rate: 99.934%
MXMailData SC rate: 96.040%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus SpamAssassin Data Query

Service (DQS) is a custom configured solution that integrates the *Spamhaus DQS* DNSBL service and the free open-source solution *SpamAssassin*. In this test no ham or newsletter samples were blocked by this combined solution. With a final score of 99.902 the product earns VBSpam+ certification.



Zoho Mail

SC rate: 99.816%
FP rate: 0.04%
Final score: 99.557
Malware catch rate: 99.690%
Phishing catch rate: 99.740%
Project Honey Pot SC rate: 98.427%
Abusix SC rate: 99.891%
MXMailData SC rate: 99.630%
Newsletters FP rate: 1.4%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail achieved higher than 99% catch rates not only on the overall spam samples but also on the malware and phishing sub-categories. Despite some false positives the product reached a final score of 99.557 and earns a VBSpam award.



Abusix Mail Intelligence

SC rate: 99.144%
FP rate: 0.00%
Final score: 99.144
Malware catch rate: 72.540%
Phishing catch rate: 97.780%
Project Honey Pot SC rate: 90.210%
Abusix SC rate: 99.871%
MXMailData SC rate: 69.800%
Newsletters FP rate: 0.0%

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 solution's 99.144% spam catch rate and lack of ham false positives are commendable.

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 4 November to 12am on 20 November 2023 (GMT).

The test corpus consisted of 264,270 emails. 261,902 of these were spam, 13,039 of which were provided by *Project Honey Pot*, 246,717 were provided by *Abusix* with the remaining 2,146 spam emails provided by *MXMailData*. There were 2,297 legitimate emails ('ham') and 71 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

35 emails in the spam corpus were considered 'unwanted' (see the June 2018 report³) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 2,560 emails from the spam corpus were found to contain a malicious attachment while 2,662 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 command⁴.

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.

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










© 2023 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/>

³ <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>.

⁴ http://www.postfix.org/XCLIENT_README.html

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender GravityZone Premium	2297	0	0.00%	27	261847	99.990%	99.990	
Fortinet FortiMail	2297	0	0.00%	13	261861	99.995%	99.995	
Mimecast	2297	0	0.00%	87.6	261786.4	99.967%	99.967	
N-able Mail Assure	2297	0	0.00%	46.4	261827.6	99.982%	99.982	
N-able SpamExperts	2297	0	0.00%	46.4	261827.6	99.982%	99.982	
Net At Work NoSpamProxy	2297	0	0.00%	31	261843	99.988%	99.945	
Rspamd	2274	23	1.00%	3272.8	258601.2	98.750%	93.688	
SEPPmail.cloud Filter	2296	1	0.04%	4.2	261869.8	99.998%	99.739	
Spamhaus DQS + SpamAssassin [‡]	2297	0	0.00%	257.2	261616.8	99.902%	99.902	
Zoho Mail	2296	1	0.04%	480.8	261393.2	99.816%	99.557	
Abusix Mail Intelligence*	2297	0	0.00%	2240.8	259633.2	99.144%	99.144	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.

	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 GravityZone Premium	0	0.0%	5	99.800%	6	99.770%	2	99.985%	20	99.992%	5	99.770%	0.08
Fortinet FortiMail	0	0.0%	0	100.000%	0	100.000%	9	99.931%	4	99.998%	0	100.000%	0.17
Mimecast	0	0.0%	0	100.000%	6	99.770%	62.6	99.519%	25	99.990%	0	100.000%	0.52
N-able Mail Assure	0	0.0%	0	100.000%	13	99.510%	22	99.831%	24.4	99.990%	0	100.000%	0.2
N-able SpamExperts	0	0.0%	0	100.000%	13	99.510%	22	99.831%	24.4	99.990%	0	100.000%	0.2
Net At Work NoSpamProxy	1	1.4%	0	100.000%	6	99.770%	6	99.954%	25	99.990%	0	100.000%	0.21
Rspamd	2	2.8%	877	65.740%	282	89.410%	1356.2	89.585%	1092.6	99.557%	824	61.600%	4.36
SEPPmail.cloud Filter	1	1.4%	0	100.000%	1	99.960%	4.2	99.968%	0	100.000%	0	100.000%	0.2
Spamhaus DQS + SpamAssassin*	0	0.0%	82	96.800%	55	97.930%	8.2	99.937%	164	99.934%	85	96.040%	0.68
Zoho Mail	1	1.4%	8	99.690%	7	99.740%	204.8	98.427%	268	99.891%	8	99.630%	1.02
Abusix Mail Intelligence*	0	0.0%	703	72.540%	59	97.780%	1274.8	90.210%	318	99.871%	648	69.800%	3.91

† 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.

	Speed			
	10%	50%	95%	98%
Bitdefender GravityZone Premium	●	●	●	●
Fortinet FortiMail	●	●	●	●
Mimecast	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
Net At Work NoSpamProxy	●	●	●	●
Rspamd	●	●	●	●
SEPPmail.cloud Filter	●	●	●	●
Spamhaus DQS + SpamAssassin [‡]	●	●	●	●
Zoho Mail	●	●	●	●

● 0–30 seconds; ● 30 seconds to two minutes; ● two minutes to 10 minutes; ● more than 10 minutes.

[‡]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	
Fortinet FortiMail	99.995
Bitdefender GravityZone Premium	99.990
N-able Mail Assure	99.982
N-able SpamExperts	99.982
Mimecast	99.967
Net At Work NoSpamProxy	99.945
Spamhaus DQS + SpamAssassin [‡]	99.902
SEPPmail.cloud Filter	99.739
Zoho Mail	99.557
Rspamd	93.688

[‡]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
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
Net At Work NoSpamProxy	32Guards & NoSpamProxy		√	√	√	√	√
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Bitdefender GravityZone Premium	Bitdefender	√				√		√	√
Fortinet FortiMail	Fortinet	√	√	√	√	√		√	√
Rspamd	None					√			
Spamhaus DQS + SpamAssassin [‡]	Optional	√	√	√					√

[‡]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.

