JUNE 2021

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2021

Ionuţ Răileanu & Adrian Luca

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

It is encouraging that we continue to see good performance by the security solutions on up-to-date spam campaigns.

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

However, as we highlight in this report, the malware and phishing landscape is more complex and presents a greater challenge for the products.

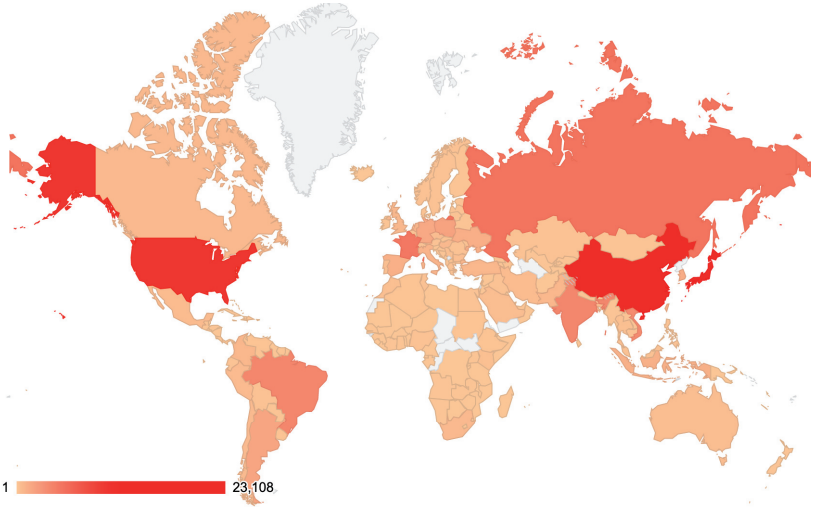
For some additional background to this report, the table and map below show the geographical distribution (based on sender IP address) of the spam emails seen in the test. *(Note: these statistics are relevant only to the spam samples we received during the test period.)*

MALWARE AND PHISHING

In this section we briefly highlight the malware and phishing samples that proved to be the most difficult for the tested solutions to block. Without the intention for this analysis to be exhaustive, we list here the particularities of some test samples that our research proved to be linked to existing threat actors.

#	Sender's IP country	Percentage of spam
1	China	21.51%
2	Japan	18.88%
3	United States	9.21%
4	Russian Federation	4.73%
5	France	4.50%
6	Brazil	3.53%
7	India	3.48%
8	Vietnam	3.19%
9	Hong Kong	2.02%
10	Poland	1.79%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

Office downloader

Attachment SHA256: `6166dd44bc6d71b976b6e62c33d8ce16687738809753f8c3f7dd81cd170be371`

Name: `PREP LIST.docx`

This email isn't part of a campaign. It caught our attention because four products failed to correctly block it. The URL from the macro file attached to the docx document, hxxp://bit[.]do/fQNsR, which redirects to hxxp://cloudstroageofofficedocumenttransfer[.]mangospot[.]net/gt/v[.]dot, was reported to be related to different malware samples.

Loki

Attachment SHA256: `90fae7829904a5b7ee85cd953124bac939546445e5397cc33e36c0978eaf6923`

Name: `PO_210513-LG01.lzh`

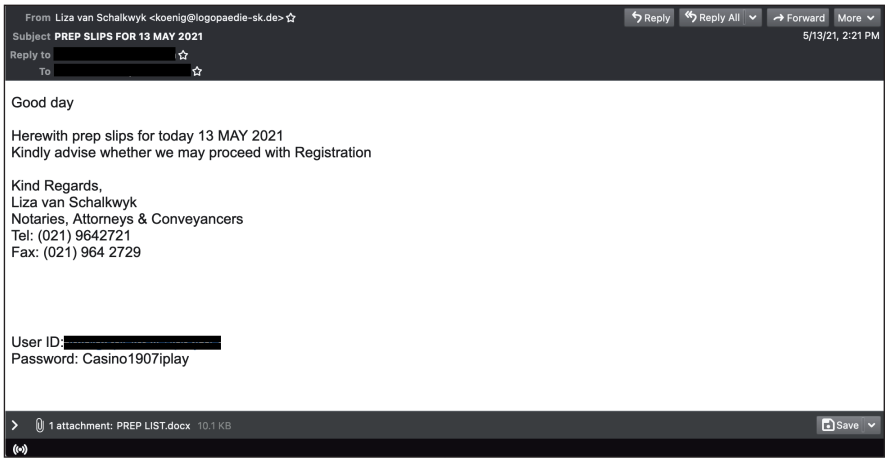
This email is part of a malware campaign targeting Korean-speaking users. The attached lzh file contains an exe file that is used to infect the victim's machine. We observed it active on 13 May.

Quakbot infected attachments

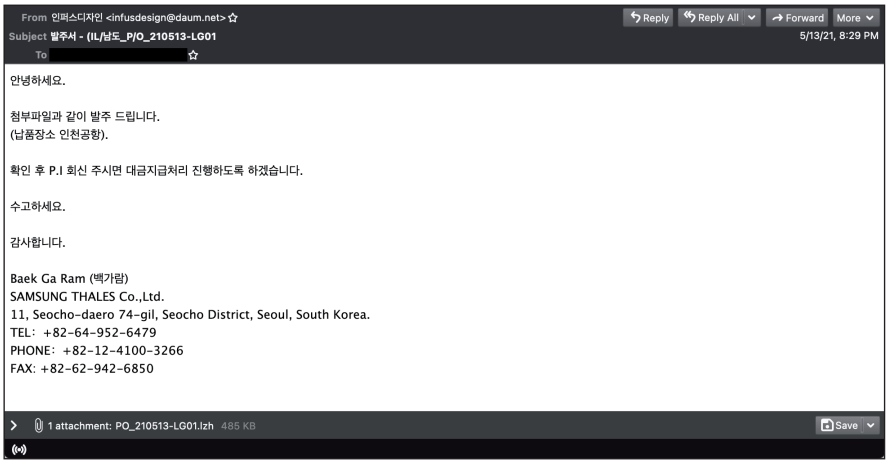
Attachment SHA256: `7275dd8635d1ad64f258069bd74768e77d7b5dbbec1a92fb684ee861d9b3304a`

Name: `Documents_1556816880_1960631962.xlsb`

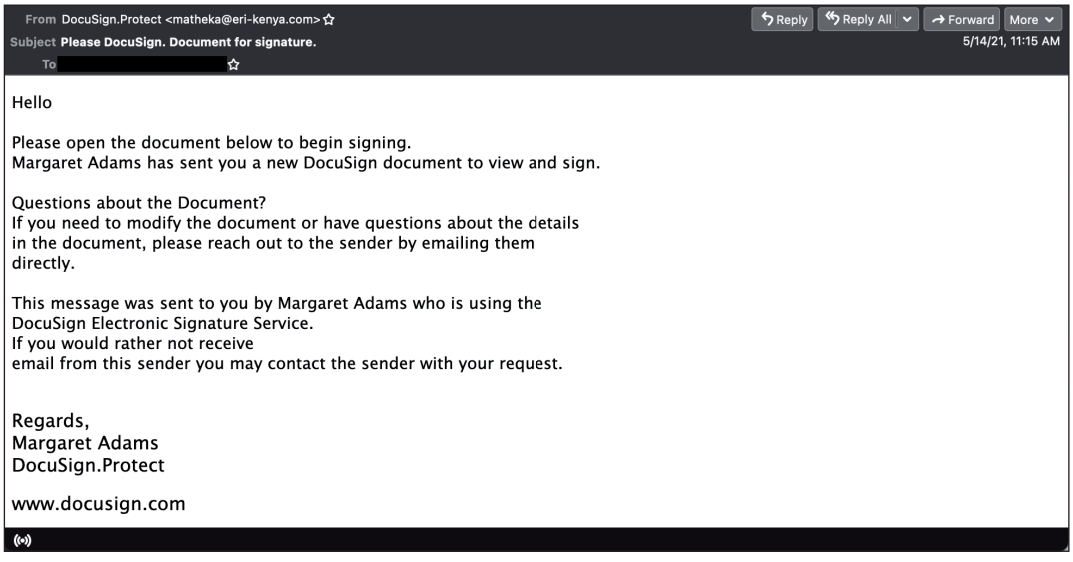
This malware campaign was active from 13 to 16 May. One of its peculiarities is that the emails were sent from different geo-located IP addresses. It is also the largest malware campaign we observed in this test period. The majority of the emails missed by the tested solutions were from 14 and 15 May.



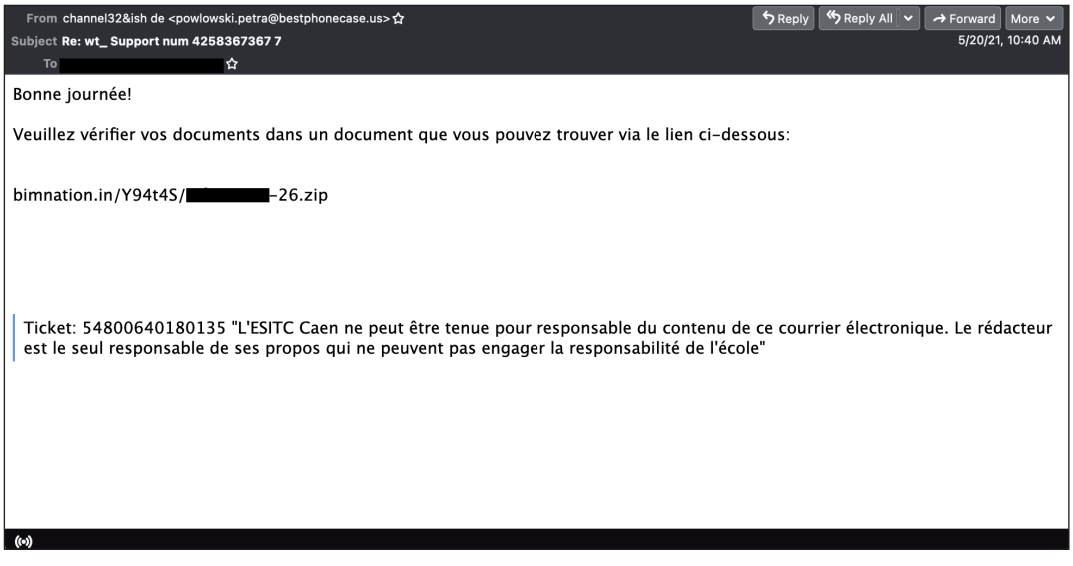
Email with attachment related to different malware samples.



Part of a malware campaign targeting Korean-speaking users.



Email with Quakbot infected attachments.



Quakbot phishing email.

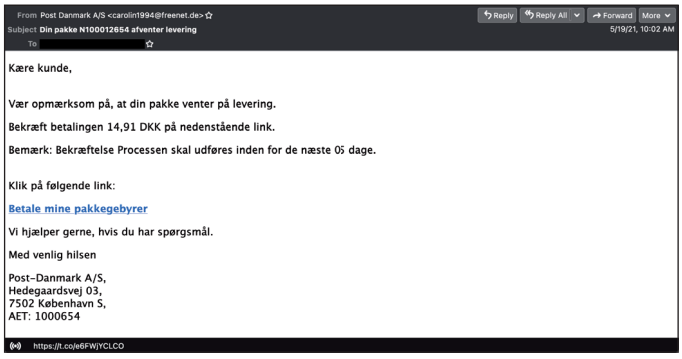
Quakbot phishing

Domains: musicaparalapaz[.]org, huntercapital[.]co[.]uk, bimnation[.]in

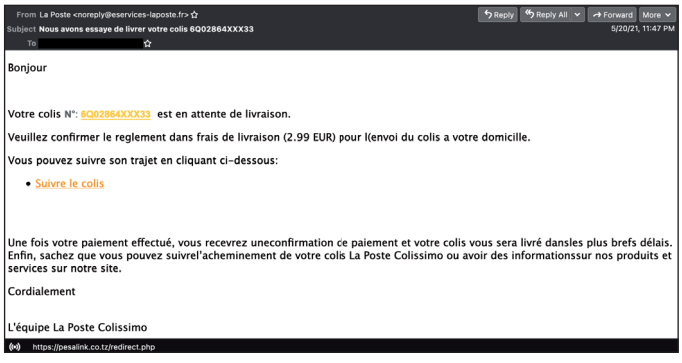
This phishing campaign evaded the filters of most of the tested solutions. We first spotted it on 12 May and it remained active throughout the rest of the test. One of its features is a URL leading to a zip archive named after the username of the email recipient. The domains from these emails have been reported to be linked to Qbot.

Non-English phishing

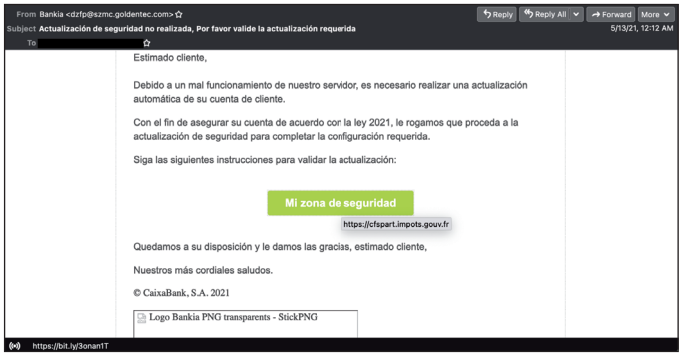
In this test we saw an increase in the number of non-English phishing emails that failed to be blocked by the tested security solutions. Usually the email subjects related to postal services or banking, and in many cases the links used URL shortening services.



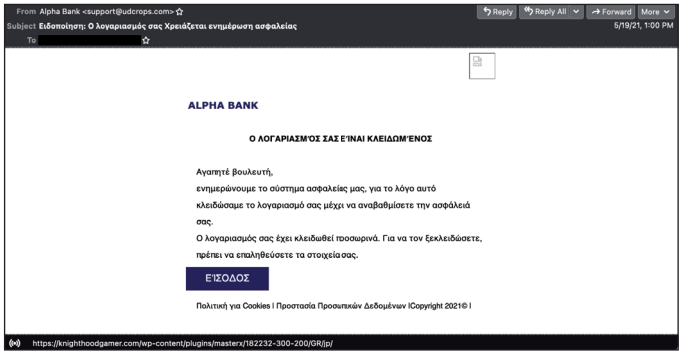
Danish phishing email.



French phishing email



Spanish phishing email



Greek phishing email

RESULTS

The majority of the tested solutions blocked more than 99% of the spam samples. We highlight the performance of *Libraesva*, which managed a 100% catch rate on the malware samples, and *Cleanmail Domain Gateway,* which missed only two phishing emails.

Three of the participating full solutions – *Cleanmail Domain Gateway, NoSpamProxy* and *ZEROSPAM* – achieved a VBSpam award, as did the custom configured solution, *Spamhaus DQS*, while a further five full solutions achieved a VBSpam+ award: *Axway*, *Bitdefender*, *Cyren eXpurgate*, *Fortinet* and *Libraesva*.

Axway MailGate 5.6

SC rate: 99.66%
FP rate: 0.00%
Final score: 99.66
Malware catch rate: 94.97%
Phishing catch rate: 98.45%
Project Honey Pot SC rate: 99.76%
Abusix SC rate: 99.62%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.86%
FP rate: 0.00%
Final score: 99.86
Malware catch rate: 99.53%
Phishing catch rate: 98.65%
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.81%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Cleanmail Domain Gateway

SC rate: 99.98%
FP rate: 0.03%
Final score: 99.85
Malware catch rate: 99.87%
Phishing catch rate: 99.87%
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Cyren eXpurgate

SC rate: 99.60%
FP rate: 0.00%
Final score: 99.60
Malware catch rate: 97.05%
Phishing catch rate: 95.68%
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.56%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.61%
FP rate: 0.00%
Final score: 99.61
Malware catch rate: 98.39%
Phishing catch rate: 96.71%
Project Honey Pot SC rate: 99.51%
Abusix SC rate: 99.65%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libraesva ESG v.4.7

SC rate: 99.78%
FP rate: 0.00%
Final score: 99.76
Malware catch rate: 100.00%
Phishing catch rate: 98.26%
Project Honey Pot SC rate: 99.74%
Abusix SC rate: 99.80%
Newsletters FP rate: 0.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

NoSpamProxy

SC rate: 99.19%
FP rate: 0.00%
Final score: 99.19
Malware catch rate: 97.99%
Phishing catch rate: 97.94%
Project Honey Pot SC rate: 99.74%
Abusix SC rate: 98.99%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Rspamd

SC rate: 92.39%
FP rate: 1.19%
Final score: 86.40
Malware catch rate: 86.78%
Phishing catch rate: 84.79%
Project Honey Pot SC rate: 96.01%
Abusix SC rate: 91.11%
Newsletters FP rate: 2.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 99.00%
FP rate: 0.00%
Final score: 99.00
Malware catch rate: 98.19%
Phishing catch rate: 95.62%
Project Honey Pot SC rate: 99.09%
Abusix SC rate: 98.97%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 98.93%
FP rate: 0.08%
Final score: 98.50
Malware catch rate: 98.59%
Phishing catch rate: 97.74%
Project Honey Pot SC rate: 99.19%
Abusix SC rate: 98.84%
Newsletters FP rate: 1.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 98.31%
FP rate: 0.15%
Final score: 97.50
Malware catch rate: 81.61%
Phishing catch rate: 97.94%
Project Honey Pot SC rate: 98.14%
Abusix SC rate: 98.37%
Newsletters FP rate: 1.8%

APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

The full VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/vbspam-methodology-ver20.

The test ran for 16 days, from 12am on 8 May to 12am on 24 May 2021 (GMT).

The test corpus consisted of 114,939 emails. 110,875 of these were spam, 29,003 of which were provided by Project Honey Pot, with the remaining 81,872 spam emails provided by Abusix. There were 3,953 legitimate emails ('ham') and 111 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

201 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[2]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 1,490 emails from the spam corpus were found to contain a malicious attachment while 1,552 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[3].

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

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

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:

- (green) = up to 30 seconds
- (yellow) = 30 seconds to two minutes
- (orange) = two to ten minutes
- (red) = more than ten minutes

Products earn VBSpam certification if the value of the final score is at least 98 and the 'delivery speed colours' at 10 and 50 per cent are green or yellow and that at 95 per cent is green, yellow or orange.

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives, no more than 2.5% false positives among the newsletters and 'delivery speed colours' of green at 10 and 50 per cent and green or yellow at 95 and 98 per cent earn a VBSpam+ award.

Head of Testing: Peter Karsai

Security Test Engineers: Gyula Hachbold, Adrian Luca, Csaba Mészáros, Tony Oliveira, Ionuţ Răileanu

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

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

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Axway	3953	0	0.00%	378.4	110335.8	99.66%	99.66	SPAM + Verified
Bitdefender	3953	0	0.00%	157.6	110556.6	99.86%	99.86	SPAM + Verified
Cleanmail Domain Gateway	3952	1	0.03%	25.2	110689	99.98%	99.85	SPAM Verified
Cyren eXpurgate	3953	0	0.00%	441.8	110272.4	99.60%	99.60	SPAM + Verified
FortiMail	3953	0	0.00%	428.2	110286	99.61%	99.61	SPAM + Verified
Libraesva	3953	0	0.00%	241.6	110472.6	99.78%	99.76	SPAM + Verified
NoSpamProxy	3953	0	0.00%	900.2	109814	99.19%	99.19	SPAM Verified
Rspamd	3906	47	1.19%	8427.6	102286.6	92.39%	86.40	
Spamhaus DQS	3953	0	0.00%	1108.6	109605.6	99.00%	99.00	SPAM Verified
ZEROSPAM	3950	3	0.08%	1184.8	109521.4	98.93%	98.50	SPAM Verified
Abusix Mail Intelligence*	3947	6	0.15%	1875.6	108838.6	98.31%	97.50	N/A

**This product is a partial solution and its performance should not be compared with that of other products.*
(Please refer to the text for full product names and details.)

	Newsletters		Malware		Phishing		Project Honey Pot		Abusix		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway	0	0.0%	75	94.97%	24	98.45%	70.2	99.76%	308.2	99.62%	0.77
Bitdefender	0	0.0%	7	99.53%	21	98.65%	0	100.00%	157.6	99.81%	0.31
Cleanmail Domain Gateway	0	0.0%	2	99.87%	2	99.87%	7.4	99.97%	17.8	99.98%	0.15
Cyren eXpurgate	0	0.0%	44	97.05%	67	95.68%	83.2	99.71%	358.6	99.56%	0.69
FortiMail	0	0.0%	24	98.39%	51	96.71%	142.2	99.51%	286	99.65%	0.54
Libraesva	1	0.9%	0	100.00%	27	98.26%	76.6	99.74%	165	99.80%	0.46
NoSpamProxy	0	0.0%	30	97.99%	32	97.94%	75.4	99.74%	824.8	98.99%	1.06
Rspamd	3	2.7%	197	86.78%	236	84.79%	1154.8	96.01%	7272.8	91.11%	4.02
Spamhaus DQS	0	0.0%	27	98.19%	68	95.62%	264.6	99.09%	844	98.97%	1.28
ZEROSPAM	2	1.8%	21	98.59%	35	97.74%	234	99.19%	950.8	98.84%	1.36
Abusix Mail Intelligence*	2	1.8%	274	81.61%	32	97.94%	539.2	98.14%	1336.4	98.37%	1.92

**This product is a partial solution and its performance should not be compared with that of other products. None of the queries to the IP blocklists included any information on the attachments; hence its performance on the malware corpus is added purely for information.*

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

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

	Speed			
	10%	**50%**	**95%**	**98%**
Axway	●	●	●	●
Bitdefender	●	●	●	●
Cleanmail Domain Gateway	●	●	●	●
Cyren eXpurgate	●	●	●	●
FortiMail	●	●	●	●
Libraesva	●	●	●	●
NoSpamProxy	●	●	●	●
Rspamd	●	●	●	●
Spamhaus DQS	●	●	●	●
ZEROSPAM	●	●	●	●

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

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

Products ranked by final score	
Bitdefender	99.86
Cleanmail Domain Gateway	99.85
Libraesva	99.76
Axway	99.66
FortiMail	99.61
Cyren eXpurgate	99.60
NoSpamProxy	99.19
Spamhaus DQS	99.00
ZEROSPAM	98.50
Rspamd	86.40

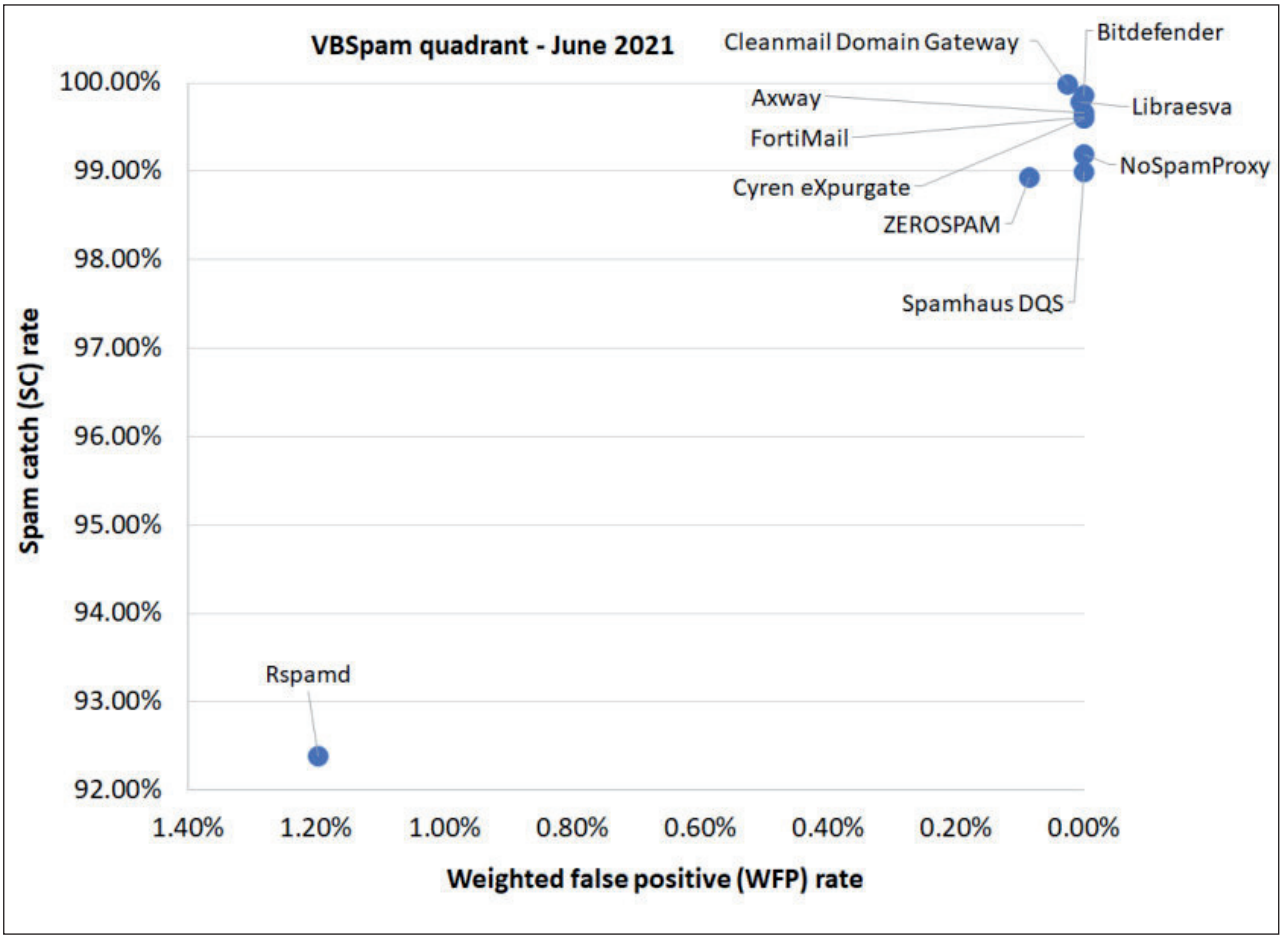
(Please refer to the text for full product names.)

Hosted solutions	**Anti-malware**	**IPv6**	**DKIM**	**SPF**	**DMARC**	**Multiple MX-records**	**Multiple locations**
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
Cyren eXpurgate	Avira SAVAPI	√	√	√	√	√	
NoSpamProxy	Heimdall		√	√	√		
ZEROSPAM	ClamAV		√	√	√	√	√

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
Libraesva	ClamAV; others optional		√	√		√		√	
Rspamd	None					√			
Spamhaus DQS	Optional	√	√	√					√

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



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