SEPTEMBER 2021

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 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.

The results show that the tested security solutions performed well. With fewer malware and phishing emails seen in the wild during the period in which this test ran, the challenges came from non-English phishing campaigns and short duration malware campaigns.

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.)*

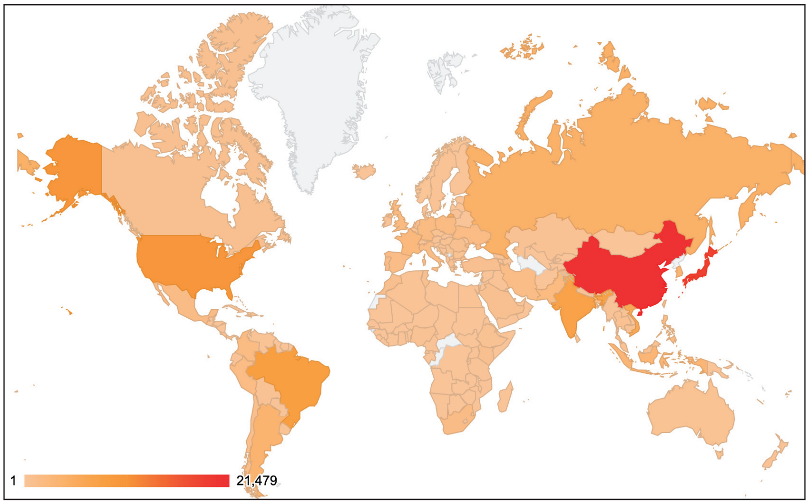
MALWARE AND PHISHING

During the period in which this test ran, we saw a decrease in the number of malware and phishing emails compared to previous tests. In the following sections we highlight a few cases that proved to be challenging for the tested solutions to block.

[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	China	15.53%
2	Japan	13.29%
3	United States	7.45%
4	Brazil	6.13%
5	India	5.37%
6	Vietnam	4.17%
7	Russian Federation	3.05%
8	Argentina	2.57%
9	Republic of Korea	2.21%
10	Indonesia	2.15%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

Dridex[2]

Attachment SHA256:

`3e5c3ca2dba4a97b5ce64954a2b4a01b29a140dacfc0401dcc75471545c1f49a`

`7c927ba1fcda33da30b47aed10a4d3b1ab4dcf5c157acc5ca6e90985a70b1eb1`

`22c9e35ef6579611c7d2e6db7e3d1c7c7cd203d84919c8f46eeb343583342be5`

Name:

`taxve_50694104_20210816_63660_25466460.xlsm`

`taxve_158762_20210816_581617912_0748186.xlsm`

`taxve_84492685_20210816_053880_415784.xlsm`

This was a spam campaign we saw active for only one day: 16 August. The campaign caught our attention because, for the first four hours after the initial occurrence, it managed to bypass the filters of the majority of the tested solutions.

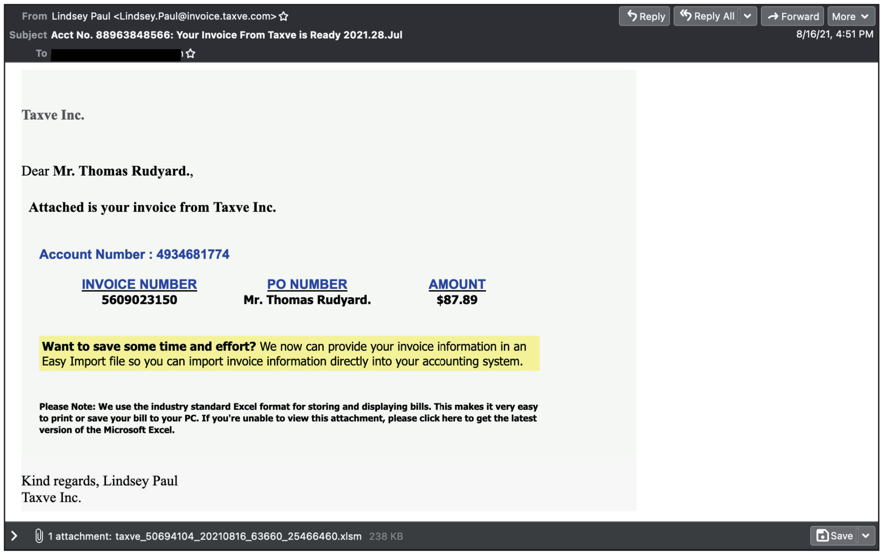
Zeppelin ransomware[3]

Attachment SHA256:

`84825c5810241c7a092119d19b92165b11774135d9557d7c54212bd6ccaa5a24`

Name: `3346.zip`

With little text and using a free email service, this malicious email was not part of a campaign – it occurred only once



From Lindsey Paul <Lindsey.Paul@invoice.taxve.com>

Subject **Acct No. 88963848566: Your Invoice From Taxve is Ready 2021.28.Jul**

8/16/21, 4:51 PM

To [redacted]

Taxve Inc.

Dear **Mr. Thomas Rudyard.**,

Attached is your invoice from Taxve Inc.

Account Number : 4934681774

INVOICE NUMBER	PO NUMBER	AMOUNT
5609023150	Mr. Thomas Rudyard.	$87.89

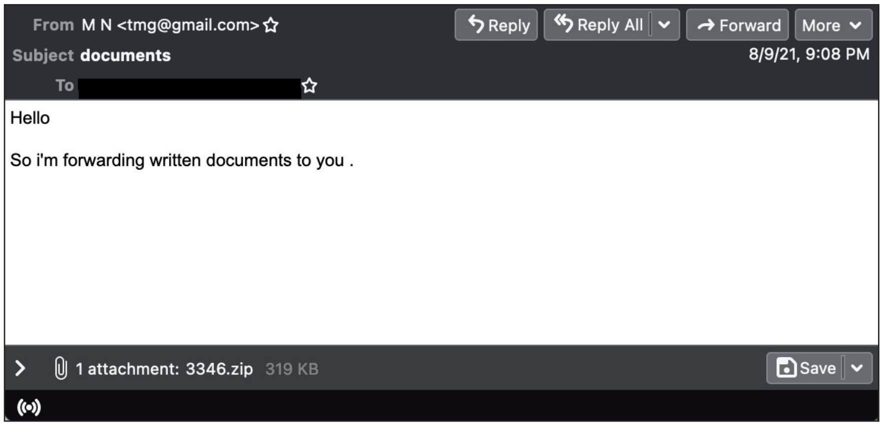
Want to save some time and effort? We now can provide your invoice information in an Easy Import file so you can import invoice information directly into your accounting system.

Please Note: We use the industry standard Excel format for storing and displaying bills. This makes it very easy to print or save your bill to your PC. If you're unable to view this attachment, please click here to get the latest version of the Microsoft Excel.

Kind regards, Lindsey Paul
Taxve Inc.

1 attachment: taxve_50694104_20210816_63660_25466460.xlsm 238 KB

Email from spam campaign with Dridex attachment.



From M N <tmg@gmail.com>

Subject **documents**

8/9/21, 9:08 PM

To [redacted]

Hello

So i'm forwarding written documents to you .

1 attachment: 3346.zip 319 KB

Email with attached archive containing a .js file that leads to Zeppelin ransomware.

[2] https://bazaar.abuse.ch/sample/3e5c3ca2dba4a97b5ce64954a2b4a01b29a140dacfc0401dcc75471545c1f49a
https://twitter.com/reecdeep/status/1427285423773175813

[3] https://tria.ge/210811-al1kb163g2/behavioral2

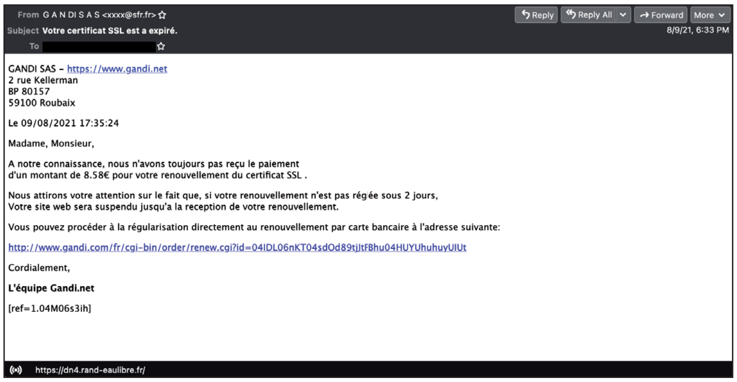
and was missed by half of the tested solutions. The archive contains a .js file that leads to a ransomware associated with the Buran family, more precisely, Zeppelin ransomware[4].

Non-English phishing

As mentioned in the last test report, we continue to see non-English phishing emails bypassing the filters of most of the tested solutions. Below are screenshots of three phishing campaigns that were active during the 16-day period in which this test ran.

RESULTS

The majority of tested solutions managed to block more than 99% of the spam samples. We highlight the performance of the new entry, *N-able Mail Assure*, which



From G A N DI S A S <xxxx@sfr.fr>
Subject Votre certificat SSL est a expiré.
To [redacted]
8/9/21, 6:33 PM

GANDI SAS – https://www.gandi.net
2 rue Kellerman
BP 80157
59100 Roubaix

Le 09/08/2021 17:35:24

Madame, Monsieur,

A notre connaissance, nous n'avons toujours pas reçu le paiement
d'un montant de 8.58€ pour votre renouvellement du certificat SSL .

Nous attirons votre attention sur le fait que, si votre renouvellement n'est pas régée sous 2 jours,
Votre site web sera suspendu jusqu'a la reception de votre renouvellement.

Vous pouvez procéder à la régularisation directement au renouvellement par carte bancaire à l'adresse suivante:

http://www.gandi.com/fr/cgi-bin/order/renew.cgi?id=04IDL06nKT04sdOd89tjJtFBhu04HUYUhuhuyUIUt

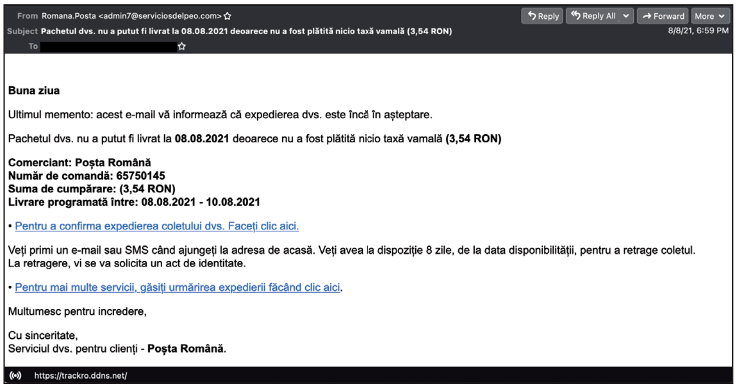
Cordialement,

L'équipe Gandi.net

[ref=1.04M06s3ih]

https://dn4.rand-eaulibre.fr/

French phishing email.



From Romana.Posta <admin7@serviciosdelpeo.com>
Subject Pachetul dvs. nu a putut fi livrat la 08.08.2021 deoarece nu a fost plătită nicio taxă vamală (3,54 RON)
To [redacted]
8/8/21, 6:59 PM

Buna ziua

Ultimul memento: acest e-mail vă informează că expedierea dvs. este încă în așteptare.

Pachetul dvs. nu a putut fi livrat la **08.08.2021** deoarece nu a fost plătită nicio taxă vamală **(3,54 RON)**

Comerciant: Poșta Română
Număr de comandă: 65750145
Suma de cumpărare: (3,54 RON)
Livrare programată între: 08.08.2021 - 10.08.2021

- Pentru a confirma expedierea coletului dvs. Faceți clic aici.

Veți primi un e-mail sau SMS când ajungeți la adresa de acasă. Veți avea la dispoziție 8 zile, de la data disponibilității, pentru a retrage coletul.
La retragere, vi se va solicita un act de identitate.

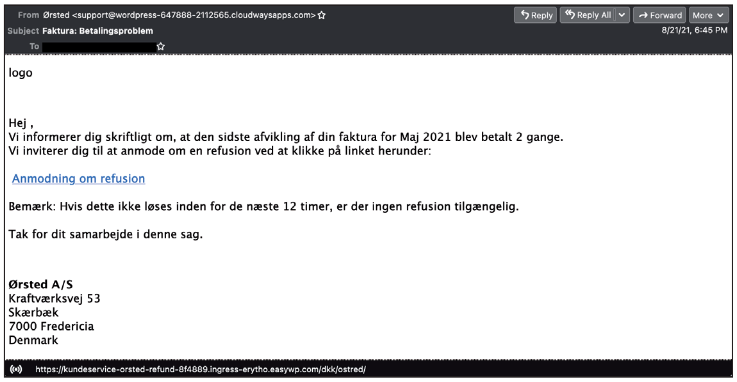
- Pentru mai multe servicii, găsiți urmărirea expedierii făcând clic aici.

Multumesc pentru incredere,

Cu sinceritate,
Serviciul dvs. pentru clienți - **Poșta Română**.

https://trackro.ddns.net/

Romanian phishing email.



From Ørsted <support@wordpress-647888-2112565.cloudwaysapps.com>
Subject Faktura: Betalingsproblem
To [redacted]
8/21/21, 6:45 PM

logo

Hej ,
Vi informerer dig skriftligt om, at den sidste afvikling af din faktura for Maj 2021 blev betalt 2 gange.
Vi inviterer dig til at anmode om en refusion ved at klikke på linket herunder:

Anmodning om refusion

Bemærk: Hvis dette ikke løses inden for de næste 12 timer, er der ingen refusion tilgængelig.

Tak for dit samarbejde i denne sag.

Ørsted A/S
Kraftværksvej 53
Skærbæk
7000 Fredericia
Denmark

https://kundeservice-orsted-refund-8f4889.ingress-erytho.easywp.com/dkk/ostred/

Danish phishing email.

[4] https://www.pcrisk.com/removal-guides/16540-zeppelin-ransomware

managed to block all the malware and phishing emails. Both *Cleanmail* and *Libraesva* also achieved a 100% malware catch rate.

Of the participating full solutions, five achieved a VBSpam award – *Axway*, *Cleanmail*, *Libraesva*, *Net at Work* and *Zerospam* – while a further three achieved a VBSpam+ award – *Bitdefender, Fortinet* and *N-able Mail Assure* – as did the custom configured solution, *Spamhaus DQS*.

Axway MailGate 5.6

vb Sept 2021 VERIFIED SPAM virusbtn.com

SC rate: 99.90%
FP rate: 0.17%
Final score: 99.05
Malware catch rate: 98.24%
Phishing catch rate: 99.01%
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.91%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Bitdefender Security for Mail Servers 3.1.7

vb Sept 2021 VERIFIED SPAM + virusbtn.com

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.94
Malware catch rate: 98.36%
Phishing catch rate: 99.43%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Cleanmail Domain Gateway

vb Sept 2021 VERIFIED SPAM virusbtn.com

SC rate: 99.99%
FP rate: 0.03%
Final score: 99.64
Malware catch rate: 100.00%
Phishing catch rate: 100.00%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.99%
Newsletters FP rate: 4.9%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Fortinet FortiMail

vb Sept 2021 VERIFIED SPAM + virusbtn.com

SC rate: 99.80%
FP rate: 0.00%
Final score: 99.80
Malware catch rate: 96.95%
Phishing catch rate: 98.30%
Project Honey Pot SC rate: 99.66%
Abusix SC rate: 99.84%
Newsletters FP rate: 0.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Libraesva ESG v.4.7

vb Sept 2021 VERIFIED SPAM virusbtn.com

SC rate: 99.88%
FP rate: 0.03%
Final score: 99.68
Malware catch rate: 100.00%
Phishing catch rate: 99.72%
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.92%
Newsletters FP rate: 1.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟡

N-able Mail Assure

vb Sept 2021 VERIFIED SPAM + virusbtn.com

SC rate: 99.87%
FP rate: 0.00%
Final score: 99.84
Malware catch rate: 100.00%
Phishing catch rate: 99.50%
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.90%
Newsletters FP rate: 1.0%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

NoSpamProxy

vb Sept 2021 VERIFIED SPAM virusbtn.com

SC rate: 99.84%
FP rate: 0.00%
Final score: 99.74
Malware catch rate: 98.36%
Phishing catch rate: 99.22%
Project Honey Pot SC rate: 99.83%
Abusix SC rate: 99.84%
Newsletters FP rate: 2.9%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Rspamd

SC rate: 97.08%
FP rate: 0.93%
Final score: 92.38
Malware catch rate: 87.69%
Phishing catch rate: 80.75%
Project Honey Pot SC rate: 94.33%
Abusix SC rate: 97.90%
Newsletters FP rate: 2.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

vb Sept 2021 VERIFIED SPAM + virusbtn.com

SC rate: 99.63%
FP rate: 0.00%
Final score: 99.60
Malware catch rate: 94.02%
Phishing catch rate: 97.59%
Project Honey Pot SC rate: 99.39%
Abusix SC rate: 99.70%
Newsletters FP rate: 1.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

vb Sept 2021 VERIFIED SPAM virusbtn.com

SC rate: 99.29%
FP rate: 0.14%
Final score: 98.57
Malware catch rate: 92.97%
Phishing catch rate: 96.39%
Project Honey Pot SC rate: 99.35%
Abusix SC rate: 99.27%
Newsletters FP rate: 1.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 98.77%
FP rate: 0.00%
Final score: 98.64
Malware catch rate: 95.78%
Phishing catch rate: 97.52%
Project Honey Pot SC rate: 98.03%
Abusix SC rate: 98.99%
Newsletters FP rate: 3.9%

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 August to 12am on 23 August 2021 (GMT).

The test corpus consisted of 147,208 emails. 144,192 of these were spam, 33,091 of which were provided by *Project Honey Pot*, with the remaining 111,101 spam emails provided by *Abusix*. There were 2,914 legitimate emails ('ham') and 102 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

136 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[5]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 853 emails from the spam corpus were found to contain a malicious attachment while 1,413 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[6].

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

[5] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review

[6] 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	2909	5	0.17%	140.2	143943	99.90%	99.05	SPAM Verified
Bitdefender	2914	0	0.00%	84.8	143998.4	99.94%	99.94	SPAM+ Verified
Cleanmail Domain Gateway	2913	1	0.03%	20.6	144062.6	99.99%	99.64	SPAM Verified
FortiMail	2914	0	0.00%	294.2	143789	99.80%	99.80	SPAM+ Verified
Libraesva	2913	1	0.03%	171	143912.2	99.88%	99.68	SPAM Verified
N-able Mail Assure	2914	0	0.00%	185	143898.2	99.87%	99.84	SPAM+ Verified
NoSpamProxy	2914	0	0.00%	227.4	143855.8	99.84%	99.74	SPAM Verified
Rspamd	2887	27	0.93%	4201.6	139881.6	97.08%	92.38	
Spamhaus DQS	2914	0	0.00%	530.4	143552.8	99.63%	99.60	SPAM+ Verified
ZEROSPAM	2910	4	0.14%	1027	143048.2	99.29%	98.57	SPAM Verified
Abusix Mail Intelligence*	2914	0	0.00%	1770	142313.2	98.77%	98.64	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%	15	98.24%	14	99.01%	42.2	99.87%	98	99.91%	0.26
Bitdefender	0	0.0%	14	98.36%	8	99.43%	3	99.99%	81.8	99.93%	0.23
Cleanmail Domain Gateway	5	4.9%	0	100.00%	0	100.00%	7.2	99.98%	13.4	99.99%	0.11
FortiMail	0	0.0%	26	96.95%	24	98.30%	111	99.66%	183.2	99.84%	0.42
Libraesva	1	1.0%	0	100.00%	4	99.72%	84.2	99.75%	86.8	99.92%	0.35
N-able Mail Assure	1	1.0%	0	100.00%	7	99.50%	76.8	99.77%	108.2	99.90%	0.32
NoSpamProxy	3	2.9%	14	98.36%	11	99.22%	54.6	99.83%	172.8	99.84%	0.36
Rspamd	3	2.9%	105	87.69%	272	80.75%	1873	94.33%	2328.6	97.90%	2.03
Spamhaus DQS	1	1.0%	51	94.02%	34	97.59%	200.4	99.39%	330	99.70%	0.69
ZEROSPAM	1	1.0%	60	92.97%	51	96.39%	216.4	99.35%	810.6	99.27%	1.01
Abusix Mail Intelligence[*]	4	3.9%	36	95.78%	35	97.52%	652.6	98.03%	1117.4	98.99%	1.52

[*] 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.

[†] 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	🟢	🟢	🟢	🟢
FortiMail	🟢	🟢	🟢	🟢
Libraesva	🟢	🟢	🟢	🟡
N-able Mail Assure	🟢	🟢	🟢	🟢
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	99.94
N-able Mail Assure	99.84
FortiMail	99.80
NoSpamProxy	99.74
Libraesva	99.68
Cleanmail	99.64
Spamhaus DQS	99.60
Axway	99.05
ZEROSPAM	98.57
Rspamd	92.38

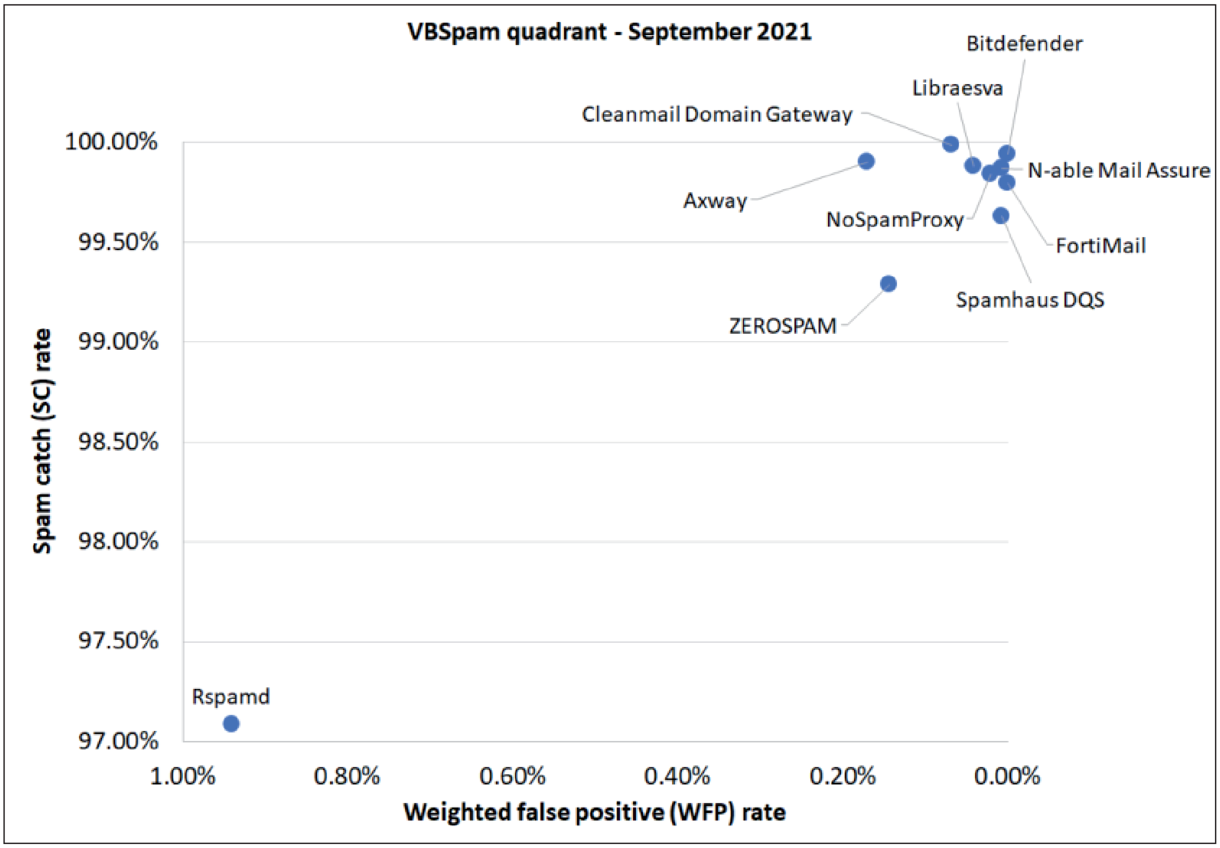
(Please refer to the text for full product names.)

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