

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 2025

Ionuț Răileanu & Adrian Luca

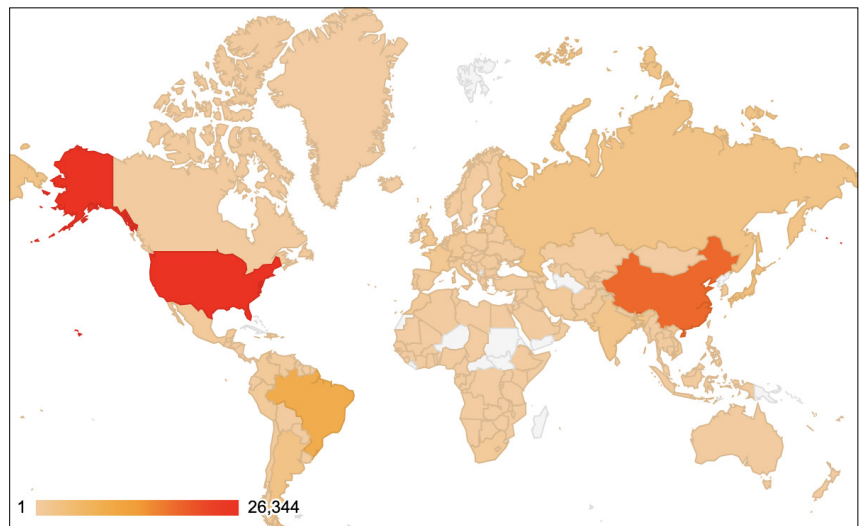
In the Q3 2025 VBSpam test – which forms part of *Virus Bulletin's* continuously running security product test suite – we measured the performance of a number of email security solutions against various streams of wanted, unwanted and malicious emails. Half of the solutions we tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished). The solutions tested publicly – and included in this report – were nine full email security solutions and one open-source solution.

Overall, we continue to see good performance from the tested solutions, which manage to keep up with the latest threats. We note that adversaries are increasingly blending social engineering with technical evasion – using familiar brands to lower skepticism while hiding malicious logic in unconventional file formats – to bypass security filters and coerce end-user interaction.

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 test¹. (*Note: these statistics are relevant only to the spam samples we received during the test period.*)

¹ For a number of samples (10,088 spam samples; 9.71% of the total) we were unable to find data about geographical location based on IP address.

#	Sender's IP country	Percentage of spam
1	United States	25.37%
2	China	17.56%
3	Brazil	8.53%
4	Japan	3.23%
5	Argentina	2.56%
6	Russian Federation	2.37%
7	India	2.04%
8	France	1.38%
9	United Kingdom	1.37%
10	Germany	1.04%



Top 10 countries from which spam was sent.

Geographical distribution of spam based on sender IP address.

AMTSO STANDARD COMPLIANCE

This test was executed in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the AMTSO website:

- **AMTSO Test ID:** AMTSO-LS1-TP157
- **Link:** <https://www.amtso.org/tests/virus-bulletin-vbspam-q3-2025/>

HIGHLIGHTS

Google Classroom BEC²

The spam campaign that was missed by the majority of the tested solutions involved emails exploiting the *Google Classroom* service. We detected it being active from 6 to 14 August.

The emails appear to be from *Google Classroom* (no-reply@classroom.google[.]com), but the subject and body reference a *WhatsApp* contact for bulk orders, which is not aligned with *Google Classroom*'s purpose.

² <https://blog.checkpoint.com/email-security/phishing-in-the-classroom-115000-emails-exploit-google-classroom-to-target-13500-organizations/>

The messages urge the recipient to send a 'full offer' to a specific *WhatsApp* number. This tactic is an attempt to move the conversation outside email security controls, where attackers can phish for personal or business data, trick victims into financial fraud, or distribute malware.

The emails contain links that appear to point to *Google* accounts and *Google Classroom*, but are heavily parameterized redirects (notifications.googleapis.com/email/redirect?...).

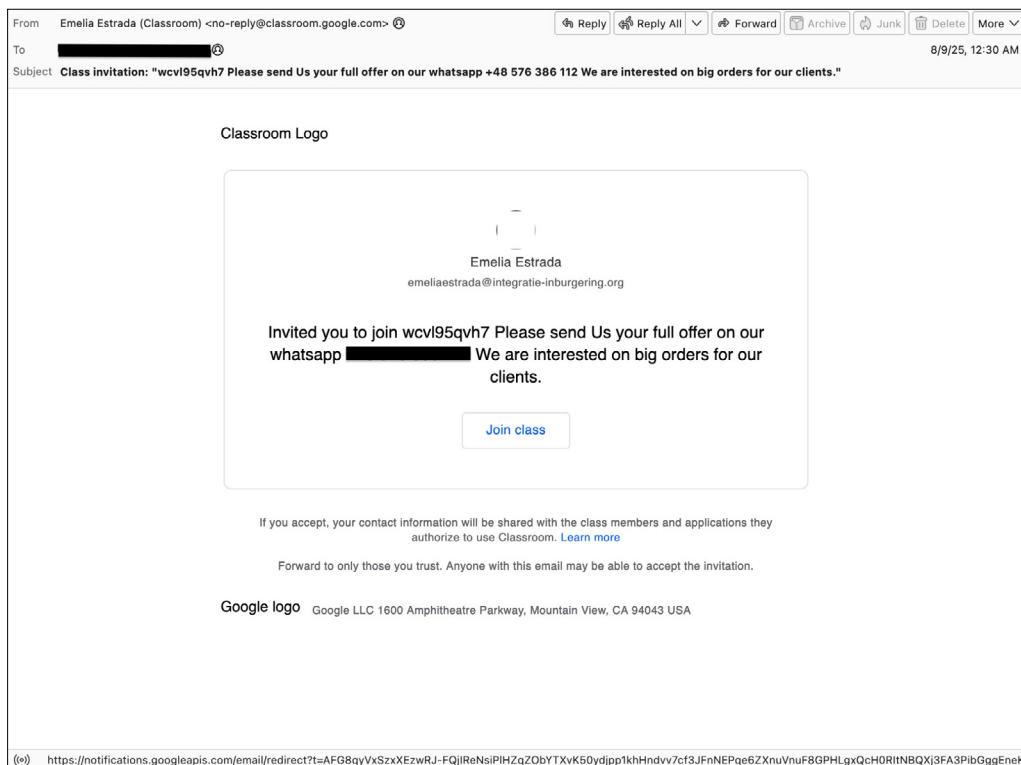
The text warns 'if you accept [the invitation], your contact information will be shared'. This suggests attackers are trying to collect personal information, potentially exposing email addresses, names and contacts.

Malicious SVG attachments

A recent phishing campaign leveraged a malicious SVG email attachment masquerading as a missed call notification. Instead of containing a harmless graphic, the file embedded heavily obfuscated JavaScript designed to execute when opened in a browser or compatible viewer.

The script attempted to run meaningless 'JSFuck'-style³ code that was deliberately crafted to fail, forcing execution into a fallback routine that redirected victims to

³ <https://jsfuck.com/>



Google Classroom phishing email.

Bitdefender GravityZone Premium

SC rate: 99.990%
 FP rate: 0.00%
 Final score: 99.990
 Malware catch rate: 100.000%
 Phishing catch rate: 99.997%
 Project Honey Pot SC rate: 99.993%
 Abusix SC rate: 99.984%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender's product achieved excellent results in this test, earning a well-deserved VBSpam+ award. Notably, it recorded no false negatives on the malware corpus and zero false positives of any kind.



Fortinet FortiMail

SC rate: 99.929%
 FP rate: 0.00%
 Final score: 99.929
 Malware catch rate: 100.000%
 Phishing catch rate: 99.940%
 Project Honey Pot SC rate: 99.924%
 Abusix SC rate: 99.944%
 MXMailData SC rate: 99.880%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet's filters successfully blocked all malware samples and produced no false positives. This performance earned *FortiMail* a VBSpam+ certification for the Q3 2025 VBSpam test, with a final score of 99.929.



N-able Mail Assure

SC rate: 99.967%
 FP rate: 0.00%
 Final score: 99.967
 Malware catch rate: 100.000%
 Phishing catch rate: 99.990%
 Project Honey Pot SC rate: 99.993%
 Abusix SC rate: 99.908%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



N-able Mail Assure demonstrated excellent all-round performance with a 99.96% spam detection rate, zero false positives, and a final score of 99.967 – easily earning VBSpam+ certification.

N-able SpamExperts

SC rate: 99.969%
 FP rate: 0.00%
 Final score: 99.969
 Malware catch rate: 100.000%
 Phishing catch rate: 99.990%
 Project Honey Pot SC rate: 99.993%
 Abusix SC rate: 99.915%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With similarly impressive scores to those of its sister product, *N-able SpamExperts* also earns VBSpam+ certification.



Net at Work NoSpamProxy

SC rate: 99.981%
 FP rate: 0.00%
 Final score: 99.981
 Malware catch rate: 100.000%
 Phishing catch rate: 99.997%
 Project Honey Pot SC rate: 99.982%
 Abusix SC rate: 99.977%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

NoSpamProxy earns VBSpam+ certification with a final score of 99.981, having blocked all malware samples and having produced no false positives.



Rspamd

SC rate: 89.429%
 FP rate: 0.56%
 Final score: 86.575
 Malware catch rate: 73.060%
 Phishing catch rate: 95.750%
 Project Honey Pot SC rate: 88.345%
 Abusix SC rate: 94.037%
 MXMailData SC rate: 68.200%
 Newsletters FP rate: 3.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The open-source *Rspamd* found dealing with the malware samples a challenge. However, we continue to see good performances from the solution on the overall spam corpus, in this case blocking more than 89% of the samples.

Rspamd Premium

SC rate: 98.250%
 FP rate: 0.16%
 Final score: 97.457
 Malware catch rate: 99.100%
 Phishing catch rate: 99.190%
 Project Honey Pot SC rate: 98.209%
 Abusix SC rate: 99.245%
 MXMailData SC rate: 89.820%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The upgraded *Rspamd* configuration significantly outperformed the basic version, successfully blocking 98.25% of spam samples and achieving a final score of 97.457.

SEPPmail.cloudfilter

SC rate: 99.983%
 FP rate: 0.00%
 Final score: 99.983
 Malware catch rate: 100.000%
 Phishing catch rate: 100.000%
 Project Honey Pot SC rate: 99.975%
 Abusix SC rate: 100.000%
 MXMailData SC rate: 99.970%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SEPPmail.cloudfilter achieved VBSpam+ certification in this test, successfully blocking all malware and phishing samples and producing zero false positives.

Sophos Email

SC rate: 99.970%
 FP rate: 0.24%
 Final score: 98.781
 Malware catch rate: 99.820%
 Phishing catch rate: 100.000%
 Project Honey Pot SC rate: 99.968%
 Abusix SC rate: 99.974%
 MXMailData SC rate: 99.970%



Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos Email earned VBSpam certification in this test, successfully blocking all phishing samples and missing only one malware sample.

Zoho Mail

SC rate: 99.426%
 FP rate: 0.08%
 Final score: 98.951
 Malware catch rate: 99.820%
 Phishing catch rate: 99.870%
 Project Honey Pot SC rate: 99.254%
 Abusix SC rate: 99.740%
 MXMailData SC rate: 99.940%
 Newsletters FP rate: 3.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail earned VBSpam certification in this test, achieving higher than 99% catch rates on the malware and phishing samples as well as on the overall spam corpus.



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-ver30/>.

The test ran for 16 days, from 12am on 2 August to 12am on 18 August 2025 (GMT).

The test corpus consisted of 105,131 emails. 103,843 of these were spam, 68,502 of which were provided by *Project Honey Pot*, 31,913 were provided by *Abusix*, with the remaining 3,428 spam emails provided by *MXMailData*. There were 1,255 legitimate emails ('ham') and 33 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

20 emails in the spam corpus were considered 'unwanted' (see the June 2018 report⁵) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 553 emails from the spam corpus were found to contain a malicious attachment while 30,353 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.

⁵ <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 command⁶.

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:

$$\text{Final score} = \text{SC} - (5 \times \text{WFP})$$

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: Klaudia Kittí Csia, Adrian Luca, Ionuț Răileanu
 Senior Threat Analyst: Norbert Biro
 Operations Manager: Bálint Tanos
 Sales Executive: Allison Sketchley
 Marketing Manager: David Kelemen
 Editorial Assistant: Helen Martin

© 2025 Virus Bulletin Ltd, Manor House, Howbery Business Park,
 Wallingford OX10 8BA, UK
 Tel: +44 20 3920 6348 Email: editorial@virusbulletin.com
 Web: <https://www.virusbulletin.com/>

⁶http://www.postfix.org/XCLIENT_README.html

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender GravityZone Premium	1255	0	0.00%	10	103817	99.990%	99.990	
Fortinet FortiMail	1255	0	0.00%	74	103753	99.929%	99.929	
N-able Mail Assure	1255	0	0.00%	34.2	103792.8	99.967%	99.967	
N-able SpamExperts	1255	0	0.00%	32.2	103794.8	99.969%	99.969	
Net at Work NoSpamProxy	1255	0	0.00%	19.6	103807.4	99.981%	99.981	
Rspamd	1248	7	0.56%	10975.8	92851.2	89.429%	86.575	
Rspamd Premium	1253	2	0.16%	1817	102010	98.250%	97.457	
SEPPmail.cloudfilter	1255	0	0.00%	18	103809	99.983%	99.983	
Sophos Email	1252	3	0.24%	31.4	103795.6	99.970%	98.781	
Zoho Mail	1254	1	0.08%	595.8	103231.2	99.426%	98.951	

	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%	0	100.000%	1	99.997%	5	99.993%	5	99.984%	0	100.000%	0.11
Fortinet FortiMail	0	0.0%	0	100.000%	17	99.940%	52	99.924%	18	99.944%	4	99.880%	0.34
N-able Mail Assure	0	0.0%	0	100.000%	3	99.990%	5	99.993%	29.2	99.908%	0	100.000%	0.18
N-able SpamExperts	0	0.0%	0	100.000%	3	99.990%	5	99.993%	27.2	99.915%	0	100.000%	0.18
Net at Work NoSpamProxy	0	0.0%	0	100.000%	1	99.997%	12.2	99.982%	7.4	99.977%	0	100.000%	0.29
Rspamd	1	3.0%	149	73.060%	1289	95.750%	7983.2	88.345%	1902.6	94.037%	1090	68.200%	7.15
Rspamd Premium	0	0.0%	5	99.100%	245	99.190%	1227	98.209%	241	99.245%	349	89.820%	1.73
SEPPmail.cloudfilter	0	0.0%	0	100.000%	0	100.000%	17	99.975%	0	100.000%	1	99.970%	0.37
Sophos Email	0	0.0%	1	99.820%	0	100.000%	22	99.968%	8.4	99.974%	1	99.970%	0.12
Zoho Mail	1	3.0%	1	99.820%	38	99.870%	510.8	99.254%	83	99.740%	2	99.940%	0.84

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

	Speed			
	10%	50%	95%	98%
Bitdefender GravityZone Premium	●	●	●	●
Fortinet FortiMail	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
Net at Work NoSpamProxy	●	●	●	●
Rspamd	●	●	●	●
Rspamd Premium	●	●	●	●
SEPPmail.cloudfilter	●	●	●	●
Sophos Email	●	●	●	●
Zoho Mail	●	●	●	●

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

Products ranked by final score	
Bitdefender GravityZone Premium	99.990
SEPPmail.cloudfilter	99.983
Net at Work NoSpamProxy	99.981
N-able SpamExperts	99.969
N-able Mail Assure	99.967
Fortinet FortiMail	99.929
Zoho Mail	98.951
Sophos Email	98.781
Rspamd Premium	97.457
Rspamd	86.575

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
Net at Work NoSpamProxy	32Guards & NoSpamProxy		√	√	√	√	√
Rspamd Premium	ClamAV		√	√	√	√	√
SEPPmail.cloudfilter	SEPPmail, ClamAV & ESET	√	√	√	√	√	√
Sophos Email	Sophos	√	√	√	√	√	√
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					√			

