SEPTEMBER 2018

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 2018

Martijn Grooten & Ionuţ Răileanu

In this test – which forms part of *Virus Bulletin*'s continuously running security product test suite – 12 full email security solutions and eight blacklists of various kinds were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

The news in these test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, especially against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with all 12 full solutions obtaining a VBSpam award and an impressive nine of them performing well enough to earn a VBSpam+ award.

MALICIOUS ATTACHMENTS

Though the 'bulk' of the more than 300,000 spam emails in this test were non-malicious, more than 2,000 emails did contain a malicious attachment.

When it comes to their deceptive message, malicious spam emails haven't changed in years: they continue be the kinds of emails one might expect to receive from a previously unknown sender, with an attachment which seems important enough to open. Examples – all of which were seen in this test – include scanned faxes[1], tax processing errors[2] and due invoices[3].

Emails that appear to contain due invoices are an example of a trend that has been seen for some time, where malicious *Office* documents are protected with a (very basic) password. However, as we have noted before, even if an anti-malware engine is not able to detect the attachment as malware, there are many other indicators that lead to most of these emails being blocked.

Apart from the 'usual suspects' (.doc, .pdf and .zip) in the attachment types seen, we also noted some less common attachment types, such as .iso and .arj – although these too have been seen before[4,5]. Again, though these unusual file types could result in the attachment not being detected as malware, there are other indicators that lead to most of these emails being blocked.

Indeed, only 34 of the emails with an attachment (less than two per cent) were missed by at least one full email security product in this test and each blocked at least 98.5 per cent of emails with a malicious attachment.

UNWANTED EMAILS

As described in the last VBSpam review, the test included some emails where the content of the emails themselves wasn't particularly spammy but where the recipient spam trap implied a not quite perfect operation by the sender. These are included in the test with a weight of 0.2 and reflect the all-too-common situation where, even with a supposedly 'perfect' spam filter, there are still many unwanted emails in one's inbox.

RESULTS

Performance in this test was good across the board, with catch rates for many products exceeding 99.9%. All participating full solutions achieved a VBSpam award with no fewer than nine performing well enough to earn a VBSpam+ award. You will find all details below, while for a historic overview of products' performance, we direct readers to our website: https://www.virusbulletin.com/testing/vbspam.

[1] https://myonlinesecurity.co.uk/fake-scanned-from-a-xerox-multifunction-printer-delivers-trickbot/.
[2] https://myonlinesecurity.co.uk/fake-hmrc-submission-5dw8-f36n-mg2a-9hj-not-processed-delivers-trickbot/.
[3] https://www.malware-traffic-analysis.net/2018/08/21/index2.html.
[4] https://isc.sans.edu/diary/rss/22636.
[5] https://blog.dynamoo.com/2014/09/overdue-invoice-6767390-spam-has.html.

ISSN 1749-7027

Axway MailGate 5.5.1

SC rate: 99.62%
FP rate: 0.04%
Final score: 99.42
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.44%
Newsletters FP rate: 0.0%
Malware SC rate: 98.71%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.4%
Malware SC rate: 99.95%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 99.95%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Forcepoint Email Security Cloud

SC rate: 99.70%
FP rate: 0.04%
Final score: 99.44
Project Honey Pot SC rate: 99.65%
Abusix SC rate: 99.76%
Newsletters FP rate: 1.3%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Malware SC rate: 99.67%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky for Exchange

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Linux Mail Security 8.0

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libra Esva 4.4.0.0

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.92
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.96%
Newsletters FP rate: 1.3%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spin Safemail

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Trustwave

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.95%
Newsletters FP rate: 1.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.88%
FP rate: 0.08%
Final score: 99.34
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.80%
Newsletters FP rate: 3.0%
Malware SC rate: 99.76%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM X-Force Combined

SC rate: 92.77%
FP rate: 0.00%
Final score: 92.77
Project Honey Pot SC rate: 90.89%
Abusix SC rate: 94.91%
Newsletters FP rate: 0.0%
Malware SC rate: 91.58%

IBM X-Force IP

SC rate: 88.04%
FP rate: 0.00%
Final score: 88.04
Project Honey Pot SC rate: 86.25%
Abusix SC rate: 90.07%
Newsletters FP rate: 0.0%
Malware SC rate: 91.58%

IBM X-Force URL

SC rate: 36.79%
FP rate: 0.00%
Final score: 36.79
Project Honey Pot SC rate: 26.87%
Abusix SC rate: 48.10%
Newsletters FP rate: 0.0%
Malware SC rate: 0.91%

Spamhaus DBL

SC rate: 25.14%
FP rate: 0.00%
Final score: 25.14
Project Honey Pot SC rate: 17.41%
Abusix SC rate: 33.96%
Newsletters FP rate: 0.0%
Malware SC rate: 6.17%

Spamhaus ZEN

SC rate: 96.56%
FP rate: 0.00%
Final score: 96.56
Project Honey Pot SC rate: 96.77%
Abusix SC rate: 96.32%
Newsletters FP rate: 0.0%
Malware SC rate: 31.47%

Spamhaus ZEN+DBL

SC rate: 97.31%
FP rate: 0.00%
Final score: 97.31
Project Honey Pot SC rate: 97.88%
Abusix SC rate: 96.66%
Newsletters FP rate: 0.0%
Malware SC rate: 31.52%

URIBL (MX Tools)

SC rate: 28.88%
FP rate: 0.02%
Final score: 28.77
Project Honey Pot SC rate: 17.74%
Abusix SC rate: 41.58%
Newsletters FP rate: 0.4%
Malware SC rate: 6.07%

Zetascan (MX Tools)

SC rate: 99.02%
FP rate: 0.18%
Final score: 98.10
Project Honey Pot SC rate: 98.82%
Abusix SC rate: 99.25%
Newsletters FP rate: 2.2%
Malware SC rate: 99.00%

APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

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

The test ran for 16 days, from 12am on 11 August to 12am on 27 August 2018.

The test corpus consisted of 331,231 emails. 326,006 of these were spam, 173,634 of which were provided by *Project Honey Pot*, with the remaining 152,372 spam emails provided by *Abusix*. There were 4,993 legitimate emails ('ham') and 232 newsletters.

141 emails in the spam corpus were considered 'unwanted' (emails contained in the spam feed that appeared legitimate in terms of both content and sender) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 2,091 emails from the spam corpus were found to contain a malicious attachment; though we report separate performance metrics on this corpus, 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]. Consequently, products were able to filter email in an environment that was very close to one in which they would be deployed in the real world.

For those products running in our lab, we 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 positives 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:

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

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

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.

Editor: Martijn Grooten

Head of Testing: Peter Karsai

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	4991	2	0.04%	1233.0	324668.2	99.62%	SPAM Verified	99.42
Bitdefender	4993	0	0.00%	60.6	325840.6	99.98%	SPAM + Verified	99.96
ESET	4993	0	0.00%	30.2	325871	99.99%	SPAM + Verified	99.99
Forcepoint	4991	2	0.04%	975.6	324925.6	99.70%	SPAM Verified	99.44
FortiMail	4993	0	0.00%	65.0	325836.2	99.98%	SPAM + Verified	99.98
IBM	4993	0	0.00%	150.2	325751	99.95%	SPAM + Verified	99.95
Kaspersky for Exchange	4993	0	0.00%	30.4	325870.8	99.99%	SPAM + Verified	99.99
Kaspersky LMS	4993	0	0.00%	28.4	325872.8	99.99%	SPAM + Verified	99.99
Libra Esva	4993	0	0.00%	74.6	325826.6	99.98%	SPAM + Verified	99.92
Safemail	4993	0	0.00%	33.4	325867.8	99.99%	SPAM + Verified	99.91
Trustwave	4993	0	0.00%	91.8	325809.4	99.97%	SPAM + Verified	99.89
ZEROSPAM	4989	4	0.08%	389.6	325511.6	99.88%	SPAM Verified	99.34
IBM X-Force Combined*	4993	0	0.00%	23572.8	302328.4	92.77%	N/A	92.77
IBM X-Force IP*	4993	0	0.00%	38993.4	286907.8	88.04%	N/A	88.04
IBM X-Force URL*	4993	0	0.00%	206008.0	119893.2	36.79%	N/A	36.79
Spamhaus DBL*	4993	0	0.00%	243967.4	81933.8	25.14%	N/A	25.14
Spamhaus ZEN*	4993	0	0.00%	11205.2	314696	96.56%	N/A	96.56
Spamhaus ZEN+DBL*	4993	0	0.00%	8760.4	317140.8	97.31%	N/A	97.31
URIBL*	4992	1	0.02%	231788.6	94112.6	28.88%	N/A	28.77
Zetascan*	4982	9	0.18%	3183.2	322718	99.02%	N/A	98.10

**The IBM X-Force, Spamhaus, URIBL and Zetascan products are partial solutions and their performance should not be compared with that of other products.*

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

	Newsletters		Malware		Project Honey Pot		Abusix		STDev†	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	0	0.0%	27	98.71%	374.2	99.78%	858.8	99.44%	1.18	●	●	●	●
Bitdefender	1	0.4%	1	99.95%	5	99.997%	55.6	99.96%	0.24	●	●	●	●
ESET	0	0.0%	1	99.95%	0.2	99.9999%	30	99.98%	0.22	●	●	●	●
Forcepoint	3	1.3%	0	100.00%	607	99.65%	368.6	99.76%	0.54	●	●	●	●
FortiMail	0	0.0%	0	100.00%	2.2	99.999%	62.8	99.96%	0.24	●	●	●	●
IBM	0	0.0%	7	99.67%	36.6	99.98%	113.6	99.93%	0.26	●	●	●	●
Kaspersky for Exchange	0	0.0%	2	99.90%	1.4	99.999%	29	99.98%	0.22	●	●	●	●
Kaspersky LMS	0	0.0%	2	99.90%	1.4	99.999%	27	99.98%	0.21	●	●	●	●
Libra Esva	3	1.3%	0	100.00%	6.6	99.996%	68	99.96%	0.25	●	●	●	●
Safemail	4	1.7%	0	100.00%	10.6	99.99%	22.8	99.99%	0.21	●	●	●	●
Trustwave	4	1.7%	0	100.00%	17.6	99.99%	74.2	99.95%	0.24	●	●	●	●
ZEROSPAM	7	3.0%	5	99.76%	81.2	99.95%	308.4	99.80%	0.53	●	●	●	●
IBM X-Force Combined*	0	0.0%	176	91.58%	15814.4	90.89%	7758.4	94.91%	13.62	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	176	91.58%	23876.4	86.25%	15117	90.07%	20.02	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	2072	0.91%	126969.2	26.87%	79038.8	48.10%	19.58	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	1962	6.17%	143402.2	17.41%	100565.2	33.96%	21.98	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	1433	31.47%	5603.2	96.77%	5602	96.32%	4.22	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	1432	31.52%	3676.2	97.88%	5084.2	96.66%	3.46	N/A	N/A	N/A	N/A
URIBL*	1	0.4%	1964	6.07%	142827.2	17.74%	88961.4	41.58%	22.45	N/A	N/A	N/A	N/A
Zetascan*	5	2.2%	21	99.00%	2042.2	98.82%	1141	99.25%	1.58	N/A	N/A	N/A	N/A

** The IBM X-Force, Spamhaus, URIBL and Zetascan are partial solutions and their performance should not be compared with that of other products. None of the queries to the IP blacklists included any information on the attachments; hence their 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.

● *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.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Forcepoint	Forcepoint Advanced Malware Detection		√	√	√	√	√
Safemail	ClamAV; proprietary	√	√	√	√	√	√
ZEROSPAM	ClamAV			√		√	√

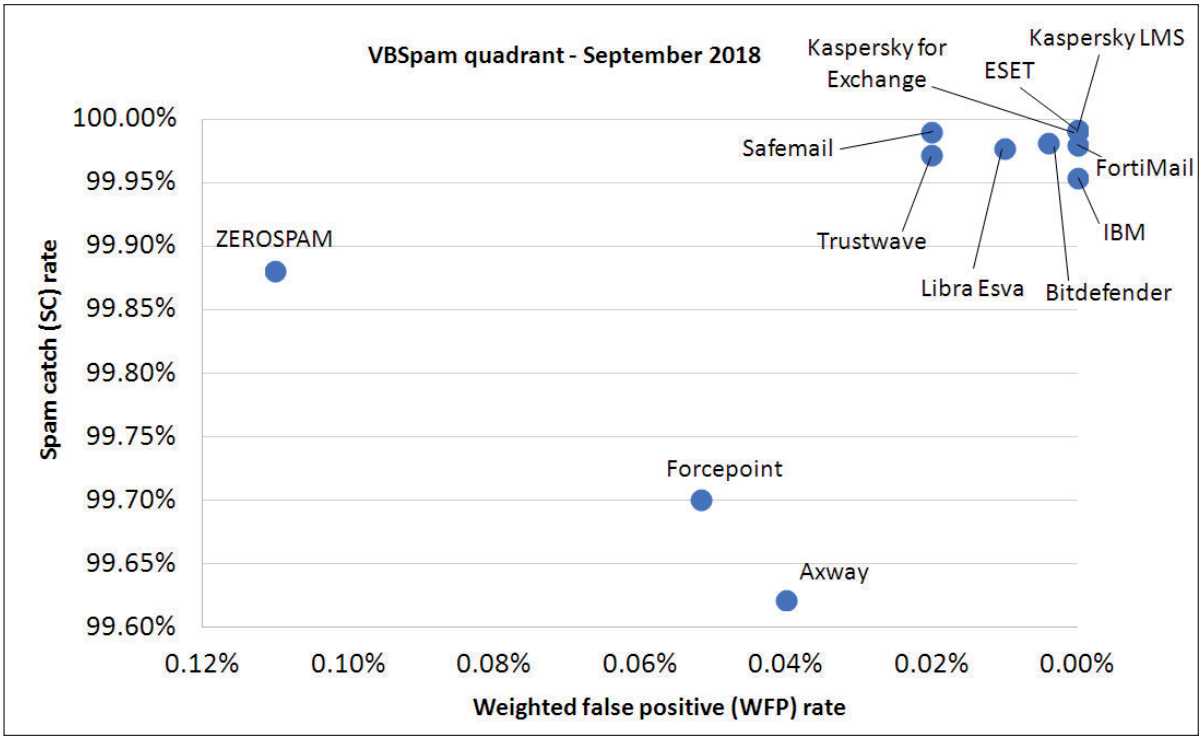
(Please refer to the text for full product names.)

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√	√	√		√	√
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky for Exchange	Kaspersky Lab	√		√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√	√	√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Trustwave	Support for multiple third-party engines	√	√	√	√	√	√	√	√

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

Products ranked by final score	
Kaspersky LMS	99.99
ESET	99.99
Kaspersky for Exchange	99.99
FortiMail	99.98
Bitdefender	99.96
IBM	99.95
Libra Esva	99.92
Safemail	99.91
Trustwave	99.89
Forcepoint Email Security Cloud	99.44
Axway	99.42
ZEROSPAM	99.34

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



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