DECEMBER 2018

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW DECEMBER 2018

Martijn Grooten & Ionuţ Răileanu

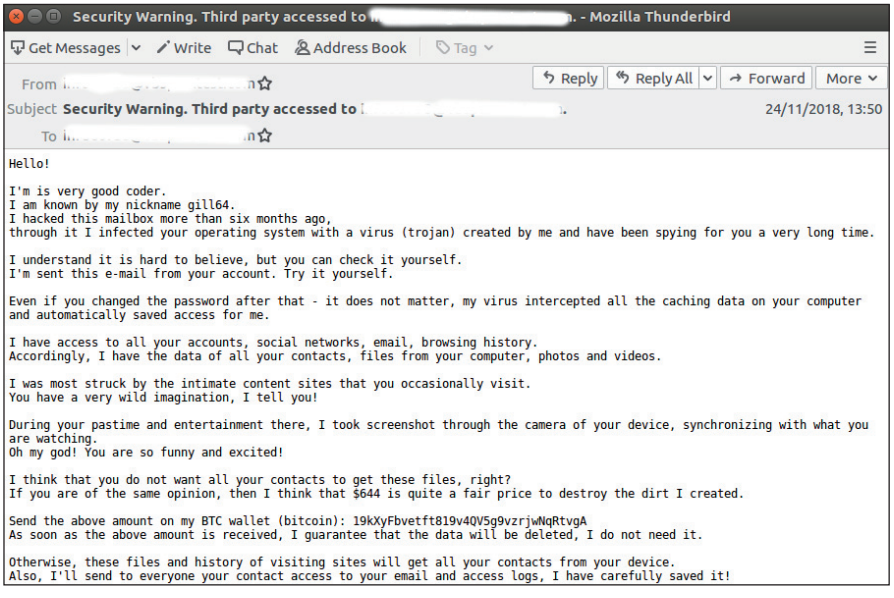
In this test – which forms part of *Virus Bulletin*'s continuously running security product test suite – 11 full email security solutions and eight blacklists of various kinds were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

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 very well. The news in this report is no exception, with all 11 full solutions obtaining a VBSpam award and seven of them performing well enough to earn a VBSpam+ award.

LESS IS MORE IN MALICIOUS EMAILS

In this test, all participating products were exposed to almost 300,000 spam emails. The typical spam email hasn't changed significantly in the past decade and generally promotes a medical product or a dating site, or offers some financial gain. The products promoted via spam are unwanted and often (though not always) illegal. Though opening and interacting with such emails is generally unwise and is not recommended, from a *computer security* point of view they aren't actually harmful.

It would certainly be unwise to interact with emails based on the sextortion scam, a great many instances of which we saw in this test – mostly the variant that didn't even include a password or part of a phone number to add credibility.



Typical sextortion email, a variant of which, including the user's password (obtained from a breached site), has been quite successful.

ISSN 1749-7027

But even falling for this kind of scam wouldn't harm your computer.

In any case, almost all of these emails were blocked by the products on test. The average product in this test missed fewer than one in every 1,000 spam emails, which serves as a reminder that spam, while not a problem that has been solved, is a very well mitigated one.

Things were a little bit different when it came to the almost 500 emails with a malicious attachment. Though the average product still blocked almost all of them, about one in every 230 such emails slipped through the filters. That is a huge difference and means that even a relatively small campaign of 100,000 emails would have seen more than 400 of them end up in users' inboxes.

In fact, it is the small size of such malicious campaigns that helps them to stay under the radar. The same is true for malicious campaigns where the payload is spread via a link, or where a link leads to a phishing page: because of their small size, they do a better job of staying under the radar.

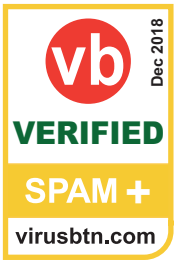
Thankfully, security is almost always multi-layered and before it can run and do any damage the typical piece of malware delivered via spam also requires some successful social engineering, and the bypassing of local security protections. Still, one is right to expect one's email security product to significantly reduce the number of emails that makes it to the user'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 seven of them – *Axway*, *Bitdefender*, *ESET*, *Fortinet*, *IBM*, *Libra Esva* and *Safemail* – performing well enough to achieve a VBSpam+ award.

You will find all performance details below, while for a historic overview of products' performance, we direct readers to: https://www.virusbulletin.com/testing/vbspam.

Axway MailGate 5.5.1



SC rate: 99.79%
FP rate: 0.00%
Final score: 99.71
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.74%
Newsletters FP rate: 1.8%
Malware SC rate: 97.84%
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: 99.95%
Newsletters FP rate: 0.5%
Malware SC rate: 99.57%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

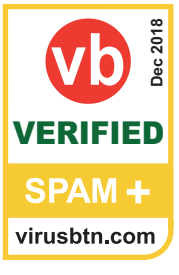
ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.9987%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Forcepoint Email Security Cloud

SC rate: 99.42%
FP rate: 0.12%
Final score: 98.84
Project Honey Pot SC rate: 99.33%
Abusix SC rate: 99.62%
Newsletters FP rate: 0.0%
Malware SC rate: 99.35%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail



SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%
Malware SC rate: 98.70%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky for Exchange

SC rate: 99.99%
FP rate: 0.02%
Final score: 99.89
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Secure Mail Gateway

SC rate: 99.99%
FP rate: 0.02%
Final score: 99.89
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libra Esva 4.4.0.0

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.8%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spin Safemail

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.5%
Malware SC rate: 99.78%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.90%
FP rate: 0.02%
Final score: 99.59
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.73%
Newsletters FP rate: 5.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM X-Force Combined

SC rate: 98.56%
FP rate: 0.00%
Final score: 98.56
Project Honey Pot SC rate: 99.33%
Abusix SC rate: 96.88%
Newsletters FP rate: 0.0%
Malware SC rate: 85.28%

IBM X-Force IP

SC rate: 96.23%
FP rate: 0.00%
Final score: 96.23
Project Honey Pot SC rate: 96.62%
Abusix SC rate: 95.37%
Newsletters FP rate: 0.0%
Malware SC rate: 85.28%

IBM X-Force URL

SC rate: 68.84%
FP rate: 0.00%
Final score: 68.84
Project Honey Pot SC rate: 86.18%
Abusix SC rate: 31.18%
Newsletters FP rate: 0.0%
Malware SC rate: 12.77%

Spamhaus ZEN+DBL

SC rate: 97.37%
FP rate: 0.00%
Final score: 97.37
Project Honey Pot SC rate: 98.14%
Abusix SC rate: 95.71%
Newsletters FP rate: 0.0%
Malware SC rate: 61.90%

Spamhaus DBL

SC rate: 9.56%
FP rate: 0.00%
Final score: 9.56
Project Honey Pot SC rate: 8.66%
Abusix SC rate: 11.53%
Newsletters FP rate: 0.0%
Malware SC rate: 47.40%

Spamhaus ZEN

SC rate: 96.75%
FP rate: 0.00%
Final score: 96.75
Project Honey Pot SC rate: 97.53%
Abusix SC rate: 95.07%
Newsletters FP rate: 0.0%
Malware SC rate: 61.90%

URIBL

SC rate: 14.30%
FP rate: 0.00%
Final score: 14.26
Project Honey Pot SC rate: 8.17%
Abusix SC rate: 27.59%
Newsletters FP rate: 0.9%
Malware SC rate: 49.35%

Zetascan

SC rate: 98.82%
FP rate: 0.16%
Final score: 98.04
Project Honey Pot SC rate: 98.93%
Abusix SC rate: 98.58%
Newsletters FP rate: 0.0%
Malware SC rate: 96.10%

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 10 November to 12am on 26 November 2018.

The test corpus consisted of 268,772 emails. 263,475 of these were spam, 180,362 of which were provided by *Project Honey Pot*, with the remaining 83,113 spam emails provided by *Abusix*. There were 5,077 legitimate emails ('ham') and 220 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

130 emails in the spam corpus were considered 'unwanted' (for an explanation of what is considered 'unwanted' please see the June 2018 VBSpam report) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 462 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[1]. Consequently, products were able to filter email in an environment that

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

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

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: Adrian Luca, Tony Oliveira, Ionuţ Răileanu
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	Final score	VBSpam
Axway	5077	0	0.00%	558.2	262812.8	99.79%	99.71	SPAM + Verified
Bitdefender	5077	0	0.00%	44.0	263327	99.98%	99.96	SPAM + Verified
ESET	5077	0	0.00%	20.0	263351	99.99%	99.99	SPAM + Verified
Forcepoint	5071	6	0.12%	1516.2	261854.8	99.42%	98.84	SPAM Verified
FortiMail	5077	0	0.00%	20.8	263350.2	99.99%	99.99	SPAM + Verified
IBM	5077	0	0.00%	101.4	263269.6	99.96%	99.96	SPAM + Verified
Kaspersky for Exchange	5076	1	0.02%	37.6	263333.4	99.99%	99.89	SPAM Verified
Kaspersky SMG	5076	1	0.02%	31.6	263339.4	99.99%	99.89	SPAM Verified
Libra Esva	5077	0	0.00%	23.6	263347.4	99.99%	99.91	SPAM + Verified
Spin	5077	0	0.00%	29.8	263341.2	99.99%	99.97	SPAM + Verified
ZEROSPAM	5076	1	0.02%	260.2	263110.8	99.90%	99.59	SPAM Verified
IBM X-Force Combined*	5077	0	0.00%	3793.2	259577.8	98.56%	98.56	N/A
IBM X-Force IP*	5077	0	0.00%	9935.6	253435.4	96.23%	96.23	N/A
IBM X-Force URL*	5077	0	0.00%	82054.4	181316.6	68.84%	68.84	N/A
Spamhaus ZEN+DBL*	5077	0	0.00%	6918.6	256452.4	97.37%	97.37	N/A
Spamhaus DBL*	5077	0	0.00%	238192.8	25178.2	9.56%	9.56	N/A
Spamhaus ZEN*	5077	0	0.00%	8551.6	254819.4	96.75%	96.75	N/A
URIBL*	5077	0	0.00%	225721.4	37649.6	14.30%	14.26	N/A
Zetascan*	5069	8	0.16%	3113.0	260258	98.82%	98.04	N/A

**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	4	1.8%	10	97.84%	344.2	99.81%	214	99.74%	0.48	●	●	●	●
Bitdefender	1	0.5%	2	99.57%	0	100.00%	44	99.95%	0.13	●	●	●	●
ESET	0	0.0%	0	100.00%	2.4	99.9987%	17.6	99.98%	0.12	●	●	●	●
Forcepoint	0	0.0%	3	99.35%	1202.2	99.33%	314	99.62%	0.49	●	●	●	●
FortiMail	0	0.0%	0	100.00%	0	100.00%	20.8	99.97%	0.05	●	●	●	●
IBM	0	0.0%	6	98.70%	34.2	99.98%	67.2	99.92%	0.18	●	●	●	●
Kaspersky for Exchange	0	0.0%	0	100.00%	4.6	99.997%	33	99.96%	0.07	●	●	●	●
Kaspersky SMG	0	0.0%	0	100.00%	4.6	99.997%	27	99.97%	0.07	●	●	●	●
Libra Esva	4	1.8%	0	100.00%	6.2	99.997%	17.4	99.98%	0.11	●	●	●	●
Spin	1	0.5%	1	99.78%	15.6	99.99%	14.2	99.98%	0.06	●	●	●	●
ZEROSPAM	11	5.0%	0	100.00%	35	99.98%	225.2	99.73%	0.25	●	●	●	●
IBM X-Force Combined*	0	0.0%	68	85.28%	1205.8	99.33%	2587.4	96.88%	5.71	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	68	85.28%	6091.8	96.62%	3843.8	95.37%	5.86	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	403	12.77%	24924	86.18%	57130.4	31.18%	11.66	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	176	61.90%	3357.2	98.14%	3561.4	95.71%	1.4	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	243	47.40%	164742.2	8.66%	73450.6	11.53%	4.35	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	176	61.90%	4457.2	97.53%	4094.4	95.07%	1.65	N/A	N/A	N/A	N/A
URIBL*	2	0.9%	234	49.35%	165610.2	8.17%	60111.2	27.59%	5.23	N/A	N/A	N/A	N/A
Zetascan*	0	0.0%	18	96.10%	1934.2	98.93%	1178.8	98.58%	0.92	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			√		√	√

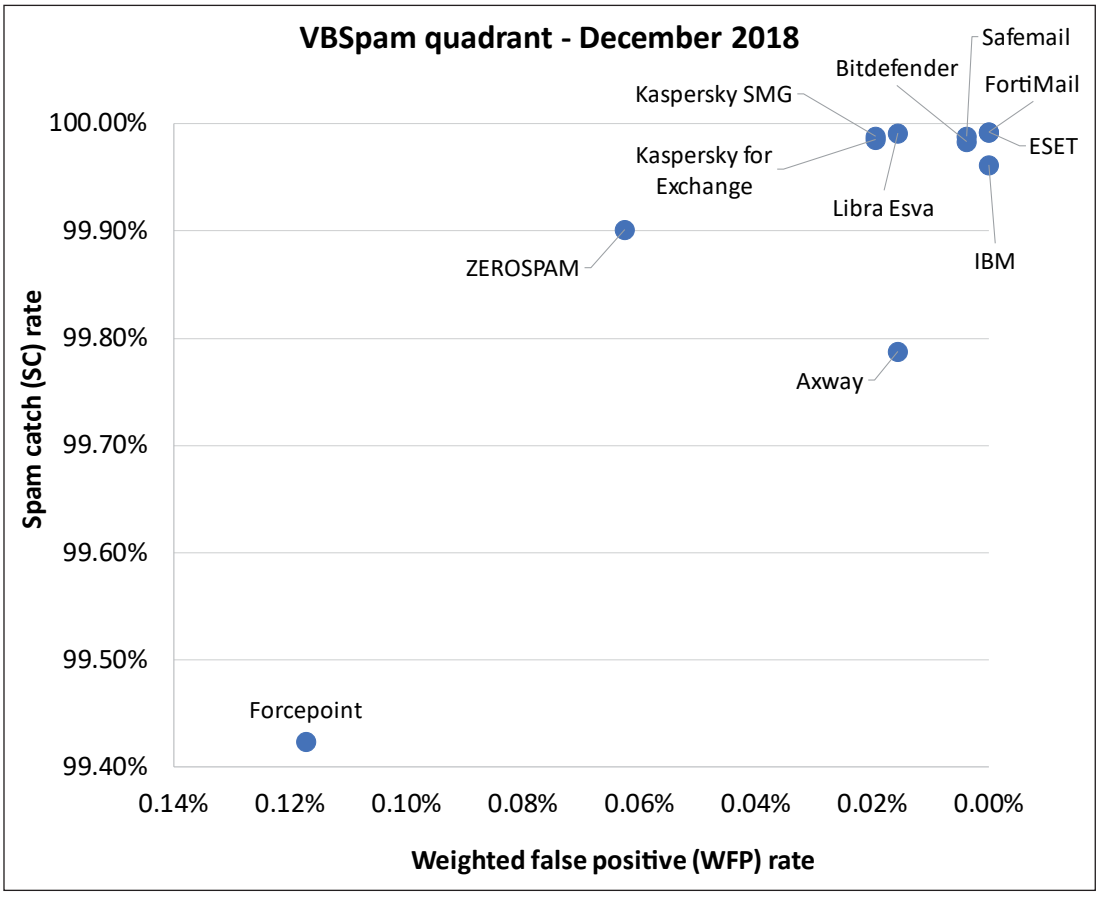
(Please refer to the text for full product names.)

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 SMG	Kaspersky Lab	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	

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

Products ranked by final score	
ESET	99.99
FortiMail	99.99
Spin	99.97
Bitdefender	99.96
IBM	99.96
Libra Esva	99.91
Kaspersky SMG	99.89
Kaspersky for Exchange	99.89
Axway	99.71
ZEROSPAM	99.59
Forcepoint	98.84

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



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