SEPTEMBER 2017

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW SEPTEMBER 2017

Martijn Grooten & Ionuţ Răileanu

Seeing a number of Chinese-language spam emails arrive in the inbox of a personal email account (where, for research purposes, barely any spam filtering takes place) reminded me recently of the first task of any spam filter: to keep our mailboxes tidy and thus reduce the likelihood of missing an email that is actually important.

On top of that, spam filters also play an essential role in improving our digital security, by blocking both phishing emails and those that carry malware.

For understandable reasons, security vendors increasingly focus on this aspect of filtering unwanted emails and thus often brand their solutions as 'email security solutions'. It is worth keeping in mind though that, apart from the content, there is no difference between spam that advertises counterfeit goods, spam that carries (or links to) malware, and spam that tries to lure you into entering your personal details on a fake website.

Thus, when we report that 'spam filters' block the overwhelming majority of spam, we mean this to include various kinds of untargeted malicious emails and thus to include the 'email security' part of the products.

In this test 14 full solutions were put through their paces, with four products achieving a VBSpam award, and no fewer than nine products achieving a VBSpam+ award.

THE MALWARE YOU NEVER SAW

August 2017, when this test was run, saw some fairly large malware-spreading campaigns. They used lures that have long been typical for such spam emails, such as missed voicemail messages or payment receipts. The attachments contained a zip or rar file, inside which a downloader was stored, which in turn would download second-stage malware – the real payload. In many cases (depending on the location of the victim[1]), this payload may have been the Locky ransomware.

Locky has been one of the most successful ransomware families and is one that you really don't want to get hit by:

[1] See https://www.virusbulletin.com/blog/2017/09/despite-profitability-ransomware-there-good-reason-why-mining-malware-thriving/.

Subject	From	Date
欢聚一堂	姜思玟	21/09/17 00:52
好伴云来	习婷秉	21/09/17 02:00
万箭穿心	宗以	21/09/17 02:14
惊起西窗眠不得	徐艾	21/09/17 02:46
便当日亲见霓裳	封显申	21/09/17 09:47
拳头上立得人胳膊上走得马	王灵伯	21/09/17 12:44
TransIP weer volledig zelfstandig	TransIP	21/09/17 18:42
☠wow How's it going	Curtis Novak	22/09/17 09:42
[redacted]) is now following you.	Keybase	22/09/17 12:28
杜郎俊赏	會更千	22/09/17 17:21
灯照离席	董瑗	22/09/17 19:31
春华秋实	鲁光	22/09/17 19:53
Professional help in case of losses in Forex.	Forex Help	22/09/17 21:19
老泪洒西州	余娜	22/09/17 21:41
更凄然	任芷怡	23/09/17 13:52
多少事	霍毕元	23/09/17 15:49
好个霜天	陈雁颖	02:17
踽踽独行	祝晶德	02:32
摸不着头脑	解兴	05:07

Chinese-language spam emails hitting the inbox of a personal email account.

ISSN 1749-7027

if you do, and you don't have a recent back-up, you'll have to pay hundreds of dollars to get your files back, as well as being left with the bad aftertaste of having paid a group of criminals.

But if you were using an email security solution, the chances of you being hit by Locky would have been very small: all but two full solutions in our test blocked each of the more than 7,000 emails in this campaign – the other two missed only a few.

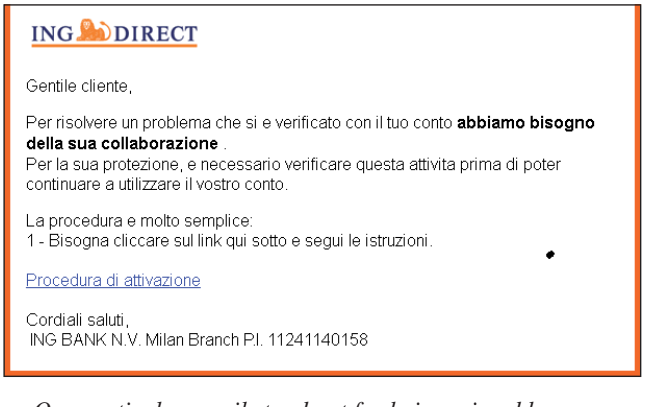
In fact, 99.9% of the emails were sent from an IP address that, at the time of sending, was listed on *Spamhaus*'s *ZEN* list. Lists like these are used by many ISPs to do some filtering before the emails reach their customers' inboxes.

Locky is one of the most well analysed malware families out there, and this is for a large part because it is sent to many spam traps. And it definitely has its victims – but their numbers are probably many times smaller than the size of the campaign might suggest.

Among the other spam, catch rates were good too, with most products catching 99.9% or more – though as always, we like to point out that numbers in our tests do not automatically translate to a real-world scenario.

No product had a perfect score though, and one particular email stood out for being missed by many products. It looked like a phishing email (the link had stopped working when we analysed it), but the body of the email contained no text, just a single image, embedded as a data URI, thus leaving little opportunity for a content filter to block the email.

Moreover, the email was sent from a compromised server in Chile and linked to another compromised server in Brazil: both the use of compromised servers and the fact that such servers were located in non-Western countries meant that they were more easily overlooked.


ING DIRECT

Gentile cliente,

Per risolvere un problema che si e verificato con il tuo conto **abbiamo bisogno della sua collaborazione** .
Per la sua protezione, e necessario verificare questa attivita prima di poter continuare a utilizzare il vostro conto.

La procedura e molto semplice:
1 - Bisogna cliccare sul link qui sotto e segui le istruzioni.

Procedura di attivazione

Cordiali saluti,
ING BANK N.V. Milan Branch P.I. 11241140158

One particular email stood out for being missed by many products.

RESULTS

This was a good month for all products but one in the test: catch rates for most products were very close to 100%, with only three products generating false positives.

OnlyMyEmail, *ESET, Fortinet* and *Bitdefender* each missed fewer than ten spam emails among the corpus of over 280,000 emails. They, as well as *Axway*, *IBM*, the two *Kaspersky* products and *Libra Esva*, earn a VBSpam+ award.

Forcepoint's *Email Security Cloud* product was new to the test. *Forcepoint*, previously known as *Websense* and *Raytheon|Websense*, saw its cloud offering easily earn a VBSpam award in its first participation, and the company will no doubt be pleased with the fact that all emails carrying malware were blocked.

CYREN, the product of a relatively recent merger of *Commtouch*, *Eleven* and *Frisk*, was also new to the test and made a bit of a false start, missing thousands of emails, mostly from a single Chinese language campaign. Based on our observation of the product in the months preceding the test, we believe that this was a rather unfortunate incident, nevertheless we were not able to award it a VBSpam award on this occasion.

Axway MailGate 5.5.1

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.92
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.4%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6

SC rate: 99.997%
FP rate: 0.00%
Final score: 99.997
Project Honey Pot SC rate: 99.996%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

CYREN

SC rate: 96.80%
FP rate: 0.00%
Final score: 96.80
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 91.16%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 99.998%
Newsletters FP rate: 0.0%
Malware SC rate: 99.99%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Forcepoint Email Security Cloud

SC rate: 99.79%
FP rate: 0.20%
Final score: 98.80
Project Honey Pot SC rate: 99.67%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.4%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 99.997%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

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

Libra Esva 4.1.0.0

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.9996%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.999%
Newsletters FP rate: 0.4%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Scrollout F1

SC rate: 99.98%
FP rate: 0.09%
Final score: 99.29
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.99%
Newsletters FP rate: 5.6%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamTitan 6.00

SC rate: 99.77%
FP rate: 0.06%
Final score: 99.47
Project Honey Pot SC rate: 99.67%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 99.92%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.98%
FP rate: 0.02%
Final score: 99.83
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.999%
Newsletters FP rate: 1.8%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM X-Force Combined

SC rate: 96.51%
FP rate: 0.02%
Final score: 96.44
Project Honey Pot SC rate: 98.90%
Abusix SC rate: 92.12%
Newsletters FP rate: 0.0%
Malware SC rate: 98.39%

IBM X-Force IP

SC rate: 95.26%
FP rate: 0.02%
Final score: 95.18
Project Honey Pot SC rate: 97.06%
Abusix SC rate: 91.94%
Newsletters FP rate: 0.0%
Malware SC rate: 98.33%

IBM X-Force URL

SC rate: 56.85%
FP rate: 0.00%
Final score: 56.85
Project Honey Pot SC rate: 76.66%
Abusix SC rate: 20.57%
Newsletters FP rate: 0.0%
Malware SC rate: 1.13%

Spamhaus DBL

SC rate: 7.55%
FP rate: 0.00%
Final score: 7.55
Project Honey Pot SC rate: 7.07%
Abusix SC rate: 8.44%
Newsletters FP rate: 0.0%
Malware SC rate: 0.57%

Spamhaus ZEN

SC rate: 96.88%
FP rate: 0.00%
Final score: 96.88
Project Honey Pot SC rate: 95.32%

Abusix SC rate: 99.74%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%

Spamhaus ZEN+DBL

SC rate: 97.19%
FP rate: 0.00%
Final score: 97.19
Project Honey Pot SC rate: 95.79%
Abusix SC rate: 99.77%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%

URIBL (MX Tools)

SC rate: 57.55%
FP rate: 0.05%
Final score: 57.33
Project Honey Pot SC rate: 71.37%
Abusix SC rate: 32.25%
Newsletters FP rate: 0.0%
Malware SC rate: 0.16%

CONCLUSION

For most participating vendors and most end-users alike, this report contains good news: spam, including most malicious emails, is dealt with rather well. Both spam and malware are notoriously volatile though, and we will continue to keep a close eye on filters' performance.

The next test report, which is due to be published in December 2017, will continue to look at all aspects of spam. Those interested in submitting a product are asked to contact martijn.grooten@virusbulletin.com.

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 12 August to 12am on 28 August 2017.

The test corpus consisted of 290,532 emails. 283,605 of these were spam, 183,440 of which were provided by *Project Honey Pot*, with the remaining 100,165 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 6,642 legitimate emails ('ham') and 285 newsletters.

Moreover, 7,320 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[2]. 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)

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

[2] 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

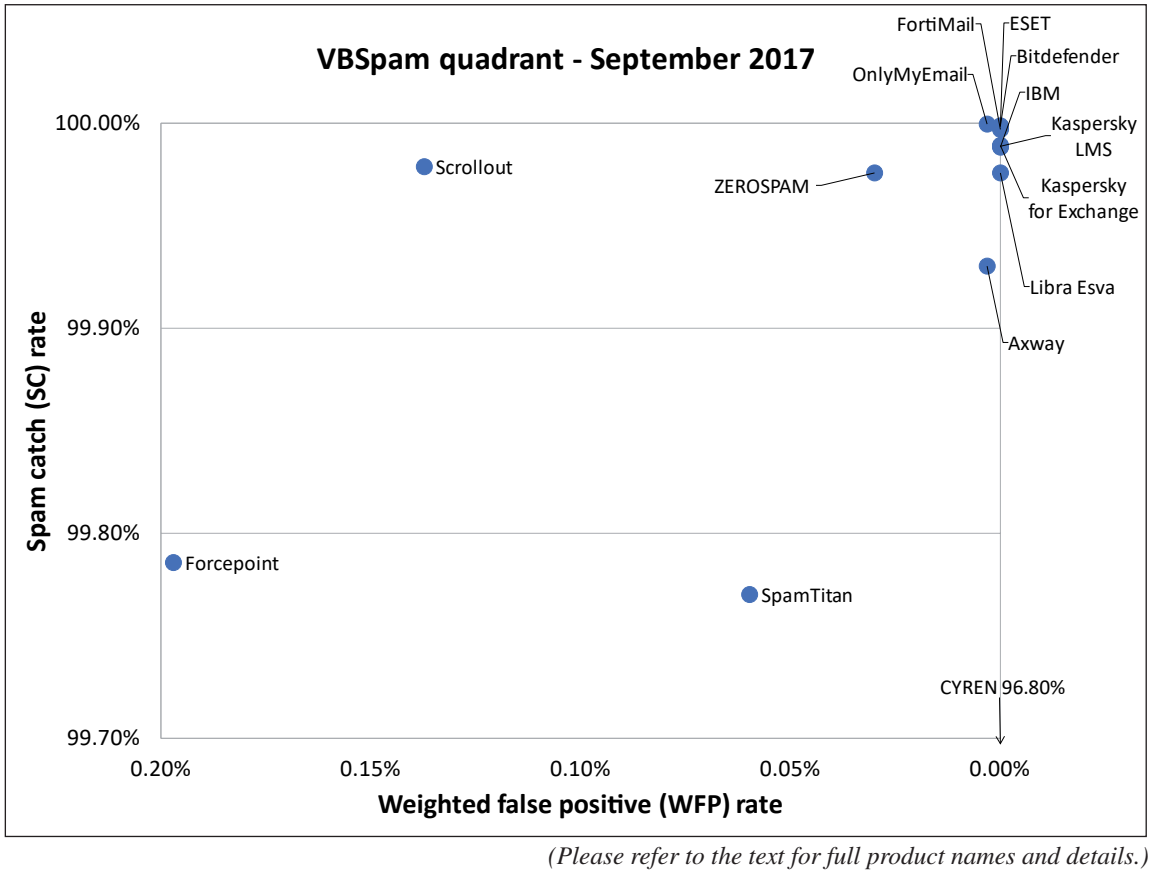
Developer: Lian Sebe

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

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

Product	Final score
ESET	99.999
FortiMail	99.999
Bitdefender	99.997
Kaspersky for Exchange	99.99
Kaspersky LMS	99.99
IBM	99.99
OnlyMyEmail	99.98
Libra Esva	99.98
Axway	99.92
ZEROSPAM	99.83
SpamTitan	99.47
Scrollout	99.29
Forcepoint	98.80
CYREN	96.80

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



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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	6642	0	0.00%	197	283408	99.93%	SPAM + Verified	99.92
Bitdefender	6642	0	0.00%	8	283597	99.997%	SPAM + Verified	99.997
CYREN	6642	0	0.00%	9063	274542	96.80%	X	96.80
ESET	6642	0	0.00%	3	283602	99.999%	SPAM + Verified	99.999
Forcepoint	6629	13	0.20%	607	282998	99.79%	SPAM Verified	99.80
FortiMail	6631	0	0.00%	4	282731	99.999%	SPAM + Verified	99.999
IBM	6642	0	0.00%	33	283572	99.99%	SPAM + Verified	99.99
Kaspersky for Exchange	6642	0	0.00%	30	283575	99.99%	SPAM + Verified	99.99
Kaspersky LMS	6642	0	0.00%	31	283574	99.99%	SPAM + Verified	99.99
Libra Esva	6642	0	0.00%	68	283537	99.98%	SPAM + Verified	99.98
OnlyMyEmail	6642	0	0.00%	1	283604	99.9996%	SPAM + Verified	99.98
Scrollout	6636	6	0.09%	60	283545	99.98%	SPAM Verified	99.29
SpamTitan	6638	4	0.06%	652	282953	99.77%	SPAM Verified	99.47
ZEROSPAM	6641	1	0.02%	68	283537	99.98%	SPAM Verified	99.83
IBM X-Force Combined*	6641	1	0.02%	9897	273708	96.51%	N/A	96.44
IBM X-Force IP*	6641	1	0.02%	13455	270150	95.26%	N/A	95.18
IBM X-Force - URL*	6642	0	0.00%	122376	161229	56.85%	N/A	56.85
Spamhaus DBL*	6642	0	0.00%	262183	21422	7.55%	N/A	7.55
Spamhaus ZEN*	6642	0	0.00%	8849	274756	96.88%	N/A	96.88
Spamhaus ZEN+DBL*	6642	0	0.00%	7958	275647	97.19%	N/A	97.19
URIBL*	6639	3	0.05%	120386	163219	57.55%	N/A	57.33

**The IBM X-Force, Spamhaus and URIBL 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	1	0.4%	0	100.00%	93	99.95%	104	99.90%	0.23	●	●	●	●
Bitdefender	0	0.0%	0	100.00%	7	99.996%	1	99.999%	0.02	●	●	●	●
CYREN	0	0.0%	0	100.00%	213	99.88%	8850	91.16%	5.63	●	●	●	●
ESET	0	0.0%	1	99.99%	1	99.999%	2	99.998%	0.01	●	●	●	●
Forcepoint	1	0.4%	0	100.00%	597	99.67%	10	99.99%	0.29	●	●	●	●
FortiMail	0	0.0%	0	100.00%	1	99.999%	3	99.997%	0.01	●	●	●	●
IBM	0	0.0%	0	100.00%	33	99.98%	0	100.00%	0.05	●	●	●	●
Kaspersky for Exchange	0	0.0%	0	100.00%	14	99.99%	16	99.98%	0.04	●	●	●	●
Kaspersky LMS	0	0.0%	0	100.00%	16	99.99%	15	99.99%	0.05	●	●	●	●
Libra Esva	0	0.0%	0	100.00%	61	99.97%	7	99.99%	0.08	●	●	●	●
OnlyMyEmail	1	0.4%	0	100.00%	0	100.00%	1	99.999%	0.01	●	●	●	●
Scrollout	16	5.6%	0	100.00%	52	99.97%	8	99.99%	0.07	●	●	●	●
SpamTitan	0	0.0%	6	99.92%	607	99.67%	45	99.96%	0.64	●	●	●	●
ZEROSPAM	5	1.8%	0	100.00%	67	99.96%	1	99.999%	0.17	●	●	●	●
IBM X-Force Combined*	0	0.0%	118	98.39%	2009	98.90%	7888	92.12%	4.81	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	122	98.33%	5386	97.06%	8069	91.94%	5.48	N/A	N/A	N/A	N/A
IBM X-Force - URL*	0	0.0%	7237	1.13%	42818	76.66%	79558	20.57%	18.58	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	7278	0.57%	170472	7.07%	91711	8.44%	8.44	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	7	99.90%	8592	95.32%	257	99.74%	2.56	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	7	99.90%	7725	95.79%	233	99.77%	2.46	N/A	N/A	N/A	N/A
URIBL*	0	0.0%	7308	0.16%	52524	71.37%	67862	32.25%	18.25	N/A	N/A	N/A	N/A

** The Spamhaus products, IBM X-Force and URIBL 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.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Forcepoint	Forcepoint Advanced Malware Detection		√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Secure MailCube	DrWeb; proprietary	√	√	√		√	√
ZEROSPAM	ClamAV			√		√	√

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
CYREN	CYREN			√			√		√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√	√	√		√	√
GFI MailEssentials	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky for Exchange	Kaspersky Lab	√		√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
NoSpamProxy	CYREN			√			√		√
Scrollout	ClamAV			√		√		√	√
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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