MARCH 2018

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MARCH 2018

Martijn Grooten & Ionuţ Răileanu

'Don't open email attachments or click on links in emails from strangers' – this is a common piece of security advice which, if followed to the letter, would prevent a lot of malware infections. However, the piece of advice ignores two important points: first, that authenticating the source of an email (and thus determining whether it came from a stranger) is notoriously hard for an untrained user. And second, that email attachments are *meant* to be opened and links in emails are *meant* to be clicked.

From phishing awareness training to better user interfaces in email clients, there are many things an organization can do to reduce the risk of a malware infection via email. If done right, such measures could have a significant long-term impact.

Still, one would want to avoid the situation where users have to make a decision several times a day as to whether or not to trust an email. That is why email security products (or spam filters) have such an important task and, in general, they do a good job of blocking such malicious emails.

Yet, as shown in this report, while catch rates of malicious and non-malicious spam may be very high, some emails with a malicious payload still manage to bypass several products.

In this test, 11 full email security products were lined up on the *Virus Bulletin* test bench, as well as eight blacklists of various kinds. Each of the 11 full products reached the required standard to achieve a VBSpam award, and six of them performed so well they achieved a VBSpam+ award.

USING A MONKEY TO GET MALWARE INTO THE INBOX

In this test, all but one of the participating full products blocked all emails with a malicious attachment[1], showing how well email security products perform when it comes to keeping most malicious attachments out of users' inboxes.

But attachments aren't the only way for malware to spread via emails. Another method is to use links. Emails that contain such links tend to be blocked widely as well; delivering emails simply scales very badly, especially if the emails are unwanted or malicious.

However, sometimes spammers find a way around this. Recently, there have been a number of malicious email campaigns that have used the infrastructure of *MailChimp*, a popular email service provider used by many legitimate organizations to send newsletters[2]. Thanks to *MailChimp*'s respectable reputation – both in terms of its brand and in terms of the cleanliness of its IP space and its domains – the emails sent via its servers are not as likely to be blocked as regular malicious spam, sent from botnets, would be.

Indeed, among the spam emails most commonly missed by the participating products were a few dozen emails sent through *MailChimp* and with an apparent malicious payload. We say 'apparent' as the links had been taken down by the time we analysed the emails. However, circumstantial evidence suggests that, at the time of delivery, these links pointed to active malware.

Credit goes to the *OnlyMyEmail* and *Bitdefender* products, both of which blocked all of these malicious emails.

RESULTS

Though spam catch rates continued to be very high overall, for most products they were lower than they had been in the last test; the *MailChimp* campaign is a good illustration of that.

Once again, *OnlyMyEmail* achieved the highest catch rate, missing only six spam emails, none of which appeared to be malicious. All other products missed at least 40 spam emails.

[1] DNS blacklists (also referred to as 'partial solutions') don't see the attachments and their performance on these emails is thus less relevant.

[2] https://www.virusbulletin.com/blog/2018/03/using-mailchimp-makes-malware-campaigns-little-bit-more-successful/

ISSN 1749-7027

Six products combined a spam catch rate of 99.5% or higher with a complete absence of false positives in the ham set, and a low false positive rate in the 'newsletter' category. These products – *Bitdefender*, *ESET*, *FortiMail*, *IBM* and both *Kaspersky* products – each earned a VBSpam+ award.

New in this test report is *Zetascan*, whose *Zetascan Query Service* aggregates various IP- and domain-based blacklists. Since *Zetascan* isn't exposed to the full emails, we consider it a partial solution (indeed, it is intended to be integrated into an existing solution).

Axway MailGate 5.5.1

SC rate: 99.44%
FP rate: 0.01%
Final score: 99.25
Project Honey Pot SC rate: 99.37%
Abusix SC rate: 99.59%
Newsletters FP rate: 3.3%
Malware SC rate: 93.61%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.86%
Newsletters FP rate: 0.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Forcepoint Email Security Cloud

SC rate: 98.81%
FP rate: 0.12%
Final score: 98.16
Project Honey Pot SC rate: 98.71%
Abusix SC rate: 99.02%
Newsletters FP rate: 0.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.86%
FP rate: 0.00%
Final score: 99.86
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.60%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.88%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky for Exchange

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Linux Mail Security 8.0

SC rate: 99.93%
FP rate: 0.00%
Final score: 99.93
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libra Esva 4.1.0.0

SC rate: 99.80%
FP rate: 0.01%
Final score: 99.73
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.55%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.99%
FP rate: 0.06%
Final score: 99.68
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.1%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.64%
FP rate: 0.00%
Final score: 99.55
Project Honey Pot SC rate: 99.70%
Abusix SC rate: 99.51%
Newsletters FP rate: 2.6%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM X-Force Combined

SC rate: 95.63%
FP rate: 0.03%
Final score: 95.49
Project Honey Pot SC rate: 95.42%
Abusix SC rate: 96.05%
Newsletters FP rate: 0.0%
Malware SC rate: 86.30%

IBM X-Force IP

SC rate: 83.83%
FP rate: 0.01%
Final score: 83.76
Project Honey Pot SC rate: 78.65%
Abusix SC rate: 94.52%
Newsletters FP rate: 0.0%
Malware SC rate: 86.30%

IBM X-Force URL

SC rate: 84.96%
FP rate: 0.01%
Final score: 84.89
Project Honey Pot SC rate: 86.39%
Abusix SC rate: 82.01%
Newsletters FP rate: 0.0%
Malware SC rate: 31.51%

Spamhaus DBL

SC rate: 33.04%
FP rate: 0.00%
Final score: 33.04
Project Honey Pot SC rate: 46.16%
Abusix SC rate: 5.98%
Newsletters FP rate: 0.0%
Malware SC rate: 31.96%

Spamhaus ZEN

SC rate: 84.46%
FP rate: 0.00%
Final score: 84.46
Project Honey Pot SC rate: 79.27%

Spamhaus ZEN contd.

Abusix SC rate: 95.15%
Newsletters FP rate: 0.0%
Malware SC rate: 84.93%

Spamhaus ZEN+DBL

SC rate: 92.42%
FP rate: 0.00%
Final score: 92.42
Project Honey Pot SC rate: 90.81%
Abusix SC rate: 95.72%
Newsletters FP rate: 0.0%
Malware SC rate: 85.84%

URIBL

SC rate: 35.55%
FP rate: 0.00%
Final score: 35.55
Project Honey Pot SC rate: 47.80%
Abusix SC rate: 10.28%
Newsletters FP rate: 0.0%
Malware SC rate: 31.05%

Zetascan

SC rate: 79.81%
FP rate: 0.21%
Final score: 78.71
Project Honey Pot SC rate: 72.40%
Abusix SC rate: 95.08%
Newsletters FP rate: 1.9%
Malware SC rate: 47.03%

CONCLUSION

This VBSpam report once again shows how well various products block unwanted and sometimes malicious emails. Yet, it also shows that some emails, even some with a malicious payload, managed to bypass several products. In the fight against malware spammers, we are winning the battle, but it's certainly not 'game over'.

Via the VBSpam tests we will continue to provide participants – including several that are tested privately – with feedback on their products' performance against various kinds of malicious emails. In the coming weeks and months, there is likely to be a lot of focus on those emails with a malicious attachment or link.

The next test report, which is to be published in June 2018, 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 10 February to 12am on 26 February 2018.

The test corpus consisted of 88,390 emails. 80,874 of these were spam, 54,468 of which were provided by *Project Honey Pot*, with the remaining 26,406 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 7,246 legitimate emails ('ham') and 270 newsletters.

Moreover, 219 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[3]. 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

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

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

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	7245	1	0.01%	451	80423	99.44%	SPAM Verified	99.25
Bitdefender	7246	0	0.00%	58	80816	99.93%	SPAM + Verified	99.90
ESET	7246	0	0.00%	42	80832	99.95%	SPAM + Verified	99.95
Forcepoint	7237	9	0.12%	964	79910	98.81%	SPAM Verified	98.16
FortiMail	7246	0	0.00%	111	80763	99.86%	SPAM + Verified	99.86
IBM Lotus Protector	7246	0	0.00%	54	80820	99.93%	SPAM + Verified	99.93
Kaspersky for Exchange	7246	0	0.00%	56	80818	99.93%	SPAM + Verified	99.93
Kaspersky LMS	7246	0	0.00%	56	80818	99.93%	SPAM + Verified	99.93
Libra Esva	7245	1	0.01%	162	80712	99.80%	SPAM Verified	99.73
OnlyMyEmail	7242	4	0.06%	6	80868	99.99%	SPAM Verified	99.68
ZEROSPAM	7246	0	0.00%	290	80584	99.64%	SPAM Verified	99.55
IBM X-Force Combined*	7244	2	0.03%	3534	77340	95.63%	N/A	95.49
IBM X-Force IP*	7245	1	0.01%	13076	67798	83.83%	N/A	83.76
IBM X-Force URL*	7245	1	0.01%	12164	68710	84.96%	N/A	84.89
Spamhaus DBL*	7246	0	0.00%	54151	26723	33.04%	N/A	33.04
Spamhaus ZEN*	7246	0	0.00%	12571	68303	84.46%	N/A	84.46
Spamhaus ZEN+DBL*	7246	0	0.00%	6133	74741	92.42%	N/A	92.42
URIBL*	7246	0	0.00%	52127	28747	35.55%	N/A	35.55
Zetascan*	7231	15	0.21%	16331	64543	79.81%	N/A	78.71

**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			Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	STDev†	10%	50%	95%	98%
Axway	9	3.3%	14	93.61%	342	99.37%	109	99.59%	1.09	●	●	●	●
Bitdefender	2	0.7%	0	100.00%	20	99.96%	38	99.86%	0.24	●	●	●	●
ESET	0	0.0%	0	100.00%	15	99.97%	27	99.90%	0.28	●	●	●	●
Forcepoint	2	0.7%	0	100.00%	704	98.71%	260	99.02%	1.76	●	●	●	●
FortiMail	0	0.0%	0	100.00%	5	99.99%	106	99.60%	0.51	●	●	●	●
IBM Lotus Protector	0	0.0%	0	100.00%	22	99.96%	32	99.88%	0.37	●	●	●	●
Kaspersky for Exchange	0	0.0%	0	100.00%	21	99.96%	35	99.87%	0.41	●	●	●	●
Kaspersky LMS	0	0.0%	0	100.00%	22	99.96%	34	99.87%	0.41	●	●	●	●
Libra Esva	0	0.0%	0	100.00%	43	99.92%	119	99.55%	0.84	●	●	●	●
OnlyMyEmail	3	1.1%	0	100.00%	3	99.99%	3	99.99%	0.05	●	●	●	●
ZEROSPAM	7	2.6%	0	100.00%	161	99.70%	129	99.51%	1.65	●	●	●	●
IBM X-Force Combined*	0	0.0%	30	86.30%	2492	95.42%	1042	96.05%	8.68	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	30	86.30%	11628	78.65%	1448	94.52%	10.48	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	150	31.51%	7414	86.39%	4750	82.01%	12.79	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	149	31.96%	29324	46.16%	24827	5.98%	13.69	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	33	84.93%	11290	79.27%	1281	95.15%	9.51	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	31	85.84%	5003	90.81%	1130	95.72%	6.49	N/A	N/A	N/A	N/A
URIBL*	0	0.0%	151	31.05%	28435	47.80%	23692	10.28%	14.48	N/A	N/A	N/A	N/A
Zetascan*	5	1.9%	116	47.03%	15031	72.40%	1300	95.08%	9.72	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		√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
ZEROSPAM	ClamAV			√		√	√

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

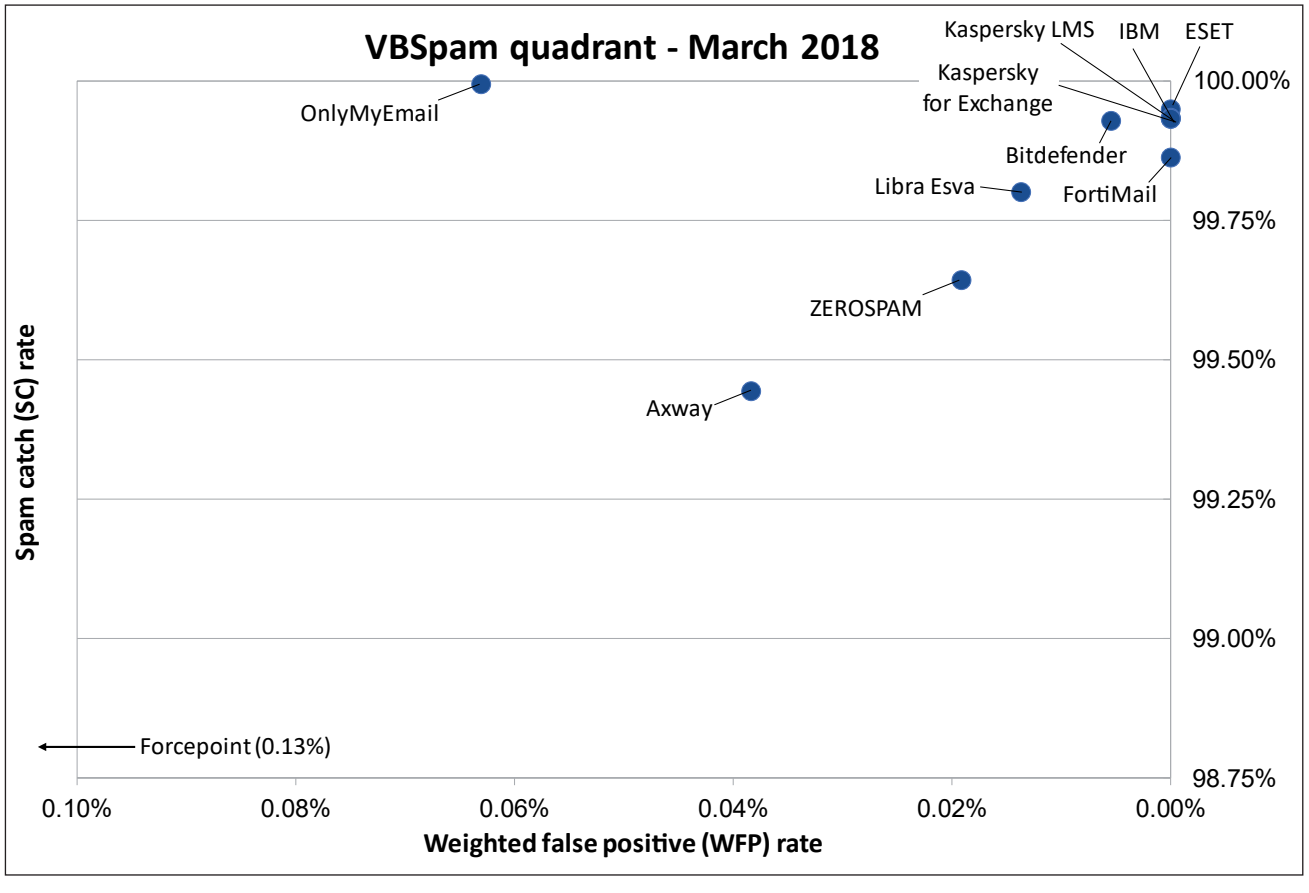
(Please refer to the text for full product names.)

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
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		√	√		√		√	

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

Products ranked by final score	
ESET	99.95
IBM	99.93
Kaspersky for Exchange	99.93
Kaspersky LMS	99.93
Bitdefender	99.90
FortiMail	99.86
Libra Esva	99.73
OnlyMyEmail	99.68
ZEROSPAM	99.55
Axway	99.25
Forcepoint	98.16

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



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