

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2020

Ionuț Răileanu

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – nine full email security solutions and four blacklists of various kinds, all of which had opted to be included in our public testing, were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

Email spam is the leading cause of malware infection. As a first line of defence, email security products have to be on full alert every day since new threats and spam techniques are constantly being developed.

The results detailed in the VBSpam test reports generally indicate that email security products are doing a good job of blocking the majority of spam emails. But in this report we

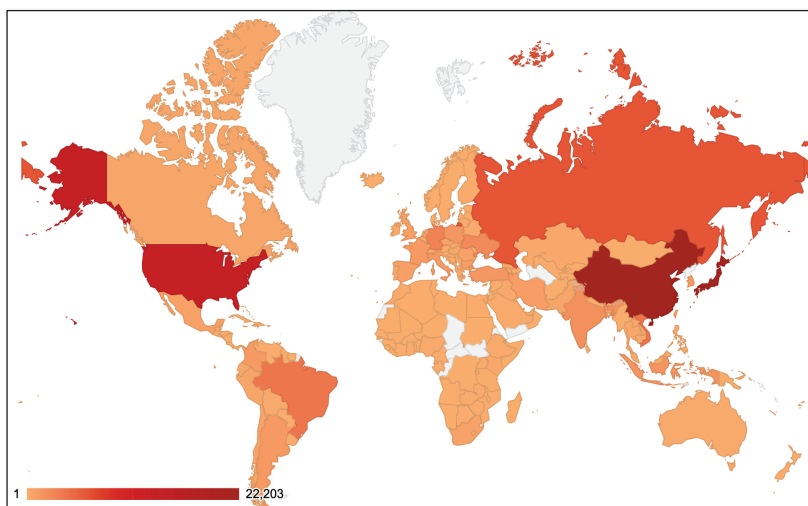
will pay more attention to the emails that evaded detection and we'll look briefly at their particularities.

The challenging times people all over the world have been going through in recent months, as well as the high level of interest in anything related to COVID-19, was reflected in spam emails. Overall, 2% of the spam emails we saw in the test contained the words 'covid' or 'coronavirus' either in the subject or in the text of the email. The number of these emails decreased gradually after peaking at the beginning of the test (for the first three days of the test 6% of spam emails daily contained such a reference). The good news is that the majority of these emails were blocked by the security products we tested. Screenshots on the following page show some examples of the COVID-19 related emails that we saw.

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 test. *(Note: these statistics are relevant only to the spam samples we received in real time and shouldn't be seen as attribution of intent.)*

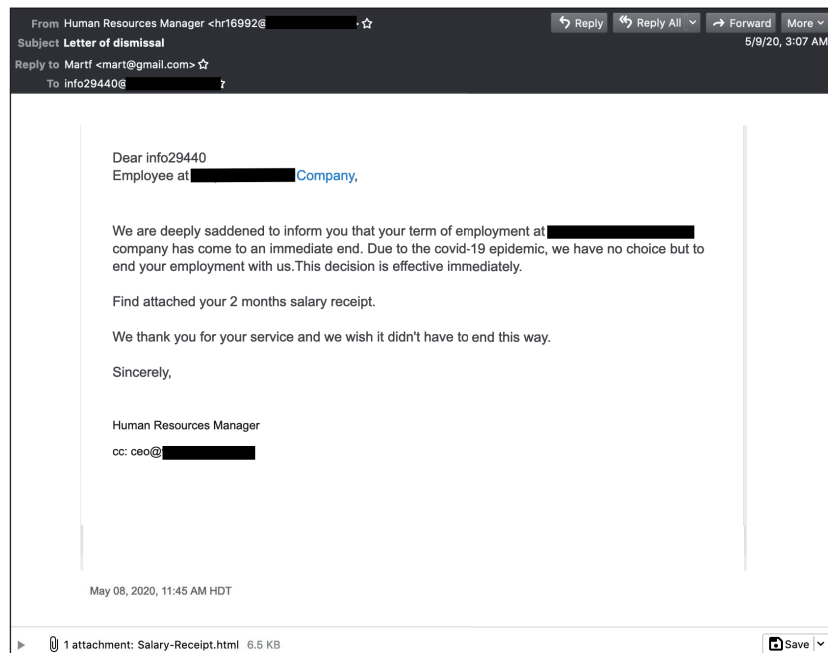
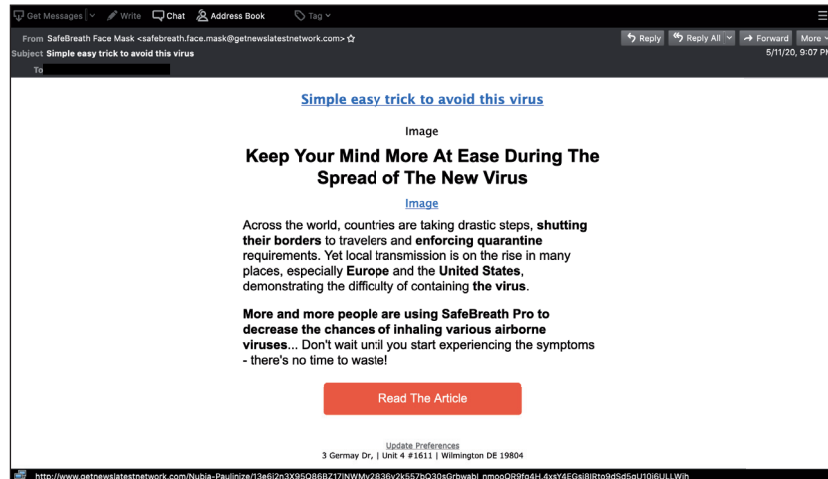
#	Sender's IP country	Percentage of spam
1	China	19.42%
2	Japan	19.27%
3	United States	11.77%
4	Russian Federation	5.57%
5	Vietnam	3.52%
6	Brazil	3.52%
7	Germany	2.65%
8	Ukraine	2.15%
9	India	1.72%
10	Indonesia	1.45%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.





Examples of the COVID-19 related emails seen during the test.

MALWARE AND PHISHING

In this test we continue to highlight the email security solutions' performance against malware and phishing emails. In these two categories we consider emails with a malicious attachment or containing links that either lead to a site with a fake login page (traditional phishing) or that download malware. Also considered as phishing are those emails with an HTML or PDF attachment that doesn't display malicious behaviour itself, but which contains links that lead to a phishing site.

The following are some of the most challenging malware and phishing emails we saw in the test.

Zloader

Subjects:

- Payment 3334205 for sent invoice 3334205 is accepted
- Case 6210596: invoice 6210596 is freezed
- 6730779 contract invoicing assumed
- Duplicated sent invoice #246650
- Given invoice 9667913 successfully compensated

Attachments:

- doc_1205_3334205.xls: 610372b5665c7f6a5489b47c8b60b871125b2619c37f197062548a31ed966c58

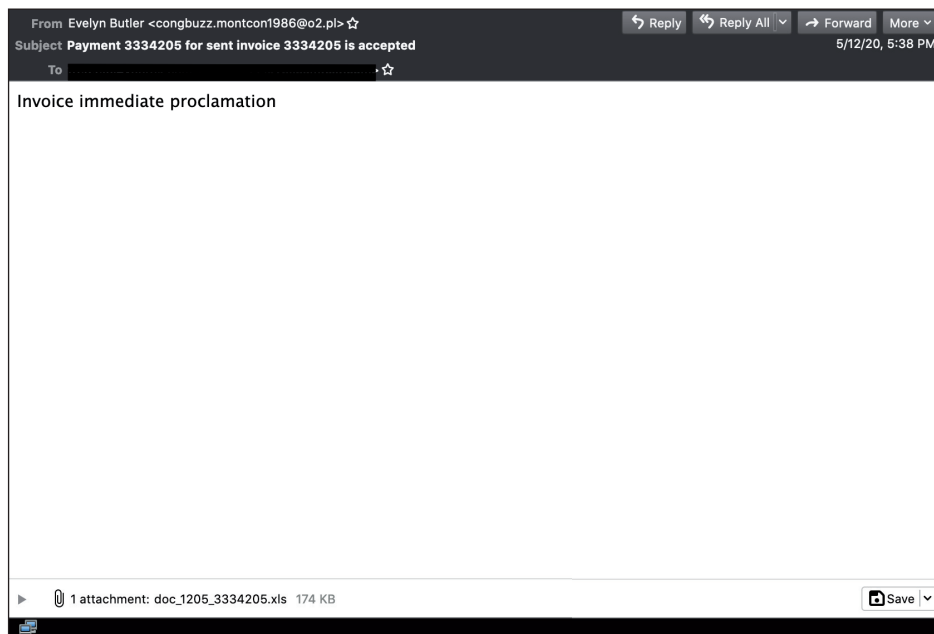
- Doc_2020-05-13_6730779.xls: f30f4e94fcd25cd86003aa1ace6fe6ebbc01f158c189998b2389d2a63b6504a
- doc_2020-05-20-6210596.xls: 7ab0f38042955786dcffb1b12a2129fc6a25bb720180df7d0a04cff3507bdff0
- document_2924.xls: c71e4dd1889fdb77bb3257c9edfda5ae1c76f10d1253bae18feb6d54b72e33c1
- Inv_2020-05-20-9667913.xls: e6c74bfa6961f0a9cc4b8e40099ad9513dbfef2d3a3be15c62c98b4399f283fe

MAIL FROM:

- congbuzz[.]montcon1986@o2[.]pl
- sapla[.]fastbang1970@o2[.]pl
- wripun[.]stello1987@wp[.]pl
- tocu[.]trigag1987@wp[.]pl
- snarous[.]osog1980@wp[.]pl

Dates of occurrence and number of products that correctly blocked it:

- 12 May; two products: *Abusix Mail Intelligence rspamd* and *IBM*.
- 13 May; three products: *Abusix Mail Intelligence rspamd*, *IBM* and *Libraesva*.

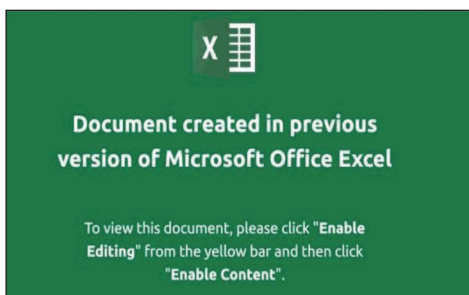


Example of a Zloader malicious email.

- 13 May; one product: *IBM*.
- 20 May; five products: *Axway, Bitdefender, IBM, Libraesva* and *Zerospam*.

Malware features:

- The XLS attachments contain calls to the external malicious URLs `hxxp://mycoursera[.]in/wp-content/uploads/2020/05/wp-front[.]php` and `hxxp://stoplazyconf[.]com/wp-front[.]php`.
- The malware also modified the *Windows* registry `qa623L.reg`.
- From this behaviour it looks as if it is associated with *Zloader* malware, a variant of the banking malware *Zeus*.

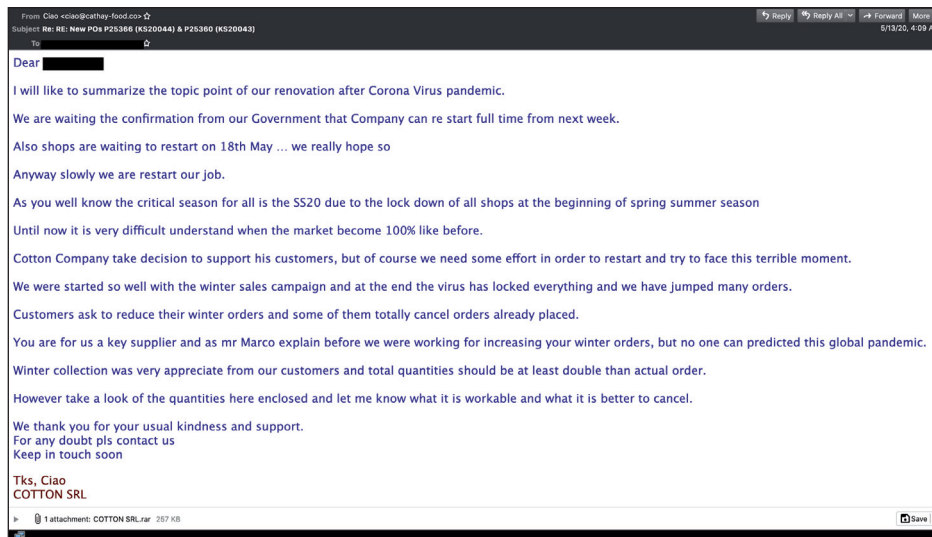


Screenshot of the malicious XLS file when first opened.

Spyware

Subject:

- Re: RE: New POs P25366 (KS20044) & P25360 (KS20043)



Spyware email.

Attachment:

- COTTON SRL.rar: 7f51e5cc81a251dfaefa461150dc8187cef23b14b06cd242fc327d276325a04b

MAIL FROM:

- ciao@cathay-food[.]co

Date of occurrence and number of products that correctly blocked it:

- 13 May; five products: *Abusix Mail Intelligence rspamd, Bitdefender, Fortinet, Libraesva* and *Zerospam*.

Malware features:

- The attachment is a RAR archive that contains an executable file.
- It tries to open an external URL from the domain `doverax[.]com`.
- The malicious behaviour consists of spyware software that is installed while exploiting this backdoor.

Trojan banker

Subject:

- Документы вторник

Attachment:

- Proekt dogovora aprel'-maj.001: fc6b23ea38834fcc728c8416175329256da06005597030997225388933061ef8

MAIL FROM:

- prvs=14089b37a3=alpinashop@alpina-group[.]ru

Date of occurrence and number of products that correctly blocked it:

- 19 May; four products: *Axway, Fortinet, IBM and Libraesva.*

Malware features:

- The attached file is a RAR archive with a ‘.001’ extension.

- It accesses the external URL

hxxp://195[.]123[.]240[.]92/viewtopic[.]php, from where it downloads the payload.

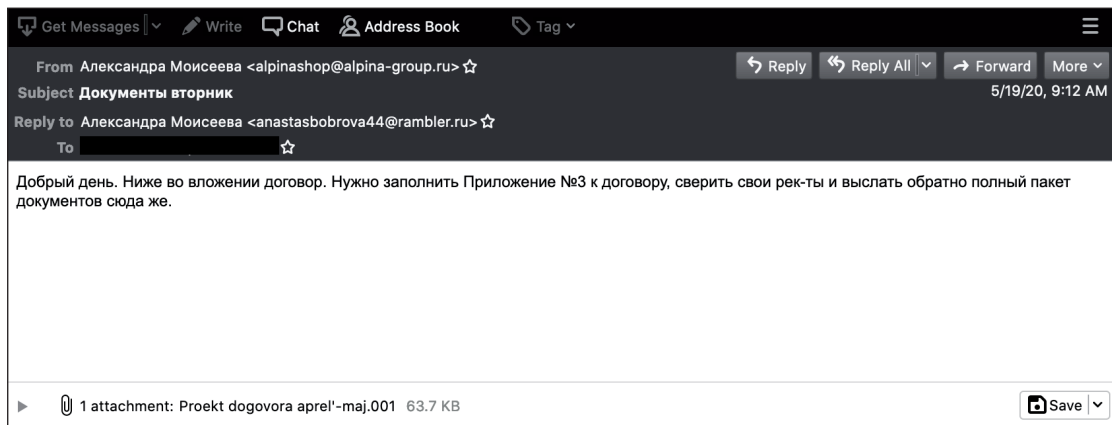
Phishing

Subject:

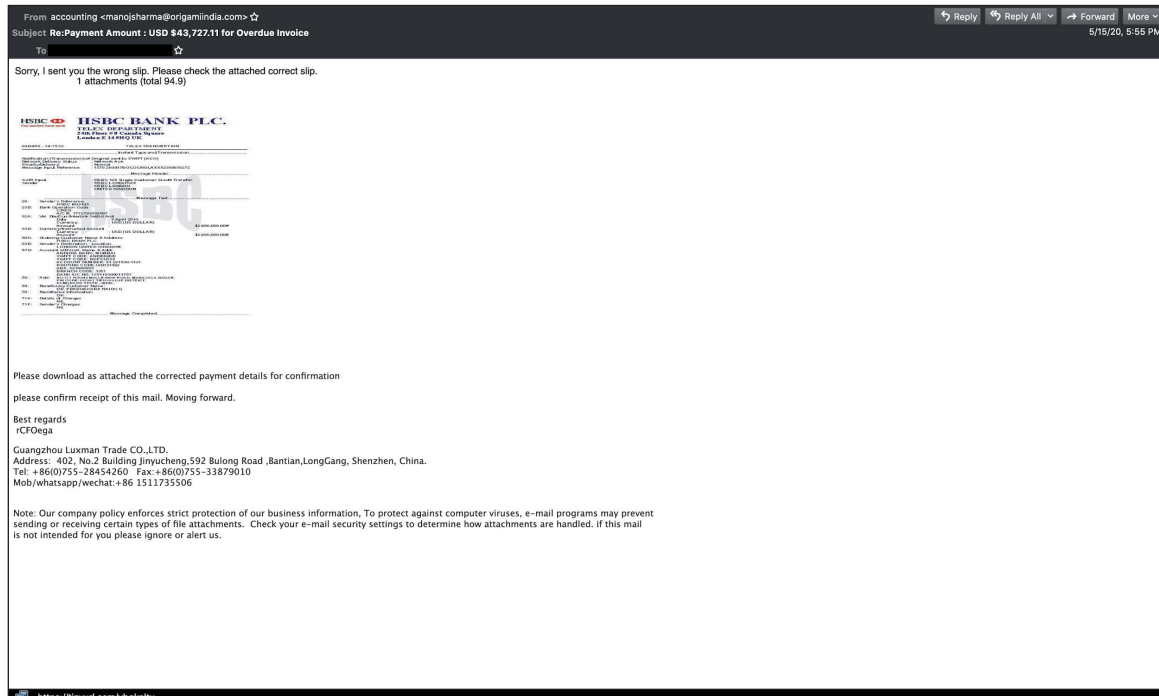
- Re:Payment Amount : USD \$43,727.11 for Overdue Invoice

Malicious URL:

- hxxps://tinyurl[.]com/ybqknltnu



Trojan banker email.



Phishing email.

MAIL FROM:

- manojsharma@origamiindia.com

Date of occurrence and number of products that correctly blocked it:

- 15 May; three products: *Axway*, *Fortinet* and *Libraesva*.

Malware features:

- The shortened URL redirects to a phishing URL:
hxxps://beyondone[.]ca/img/img/index[.]php.
- We couldn't track the malicious behaviour any further, since this URL is no longer accessible.

Netflix phishing

Subject:

- Netflix: We're sorry to say goodbye - IMPORTANT: Your account is on hold. Your Netflix.ca (#205-5245001-0426740) has been dispatched.

Malicious URL:

- hxxp://yapichemforum[.]com/esigned

MAIL FROM:

- rachel_galloway@msn.com

Date of occurrence and number of products that correctly blocked it:

- 19 May; five products: *Axway*, *Abusix Mail Intelligence rspamd*, *IBM*, *Libraesva* and *ZEROSPAM*.

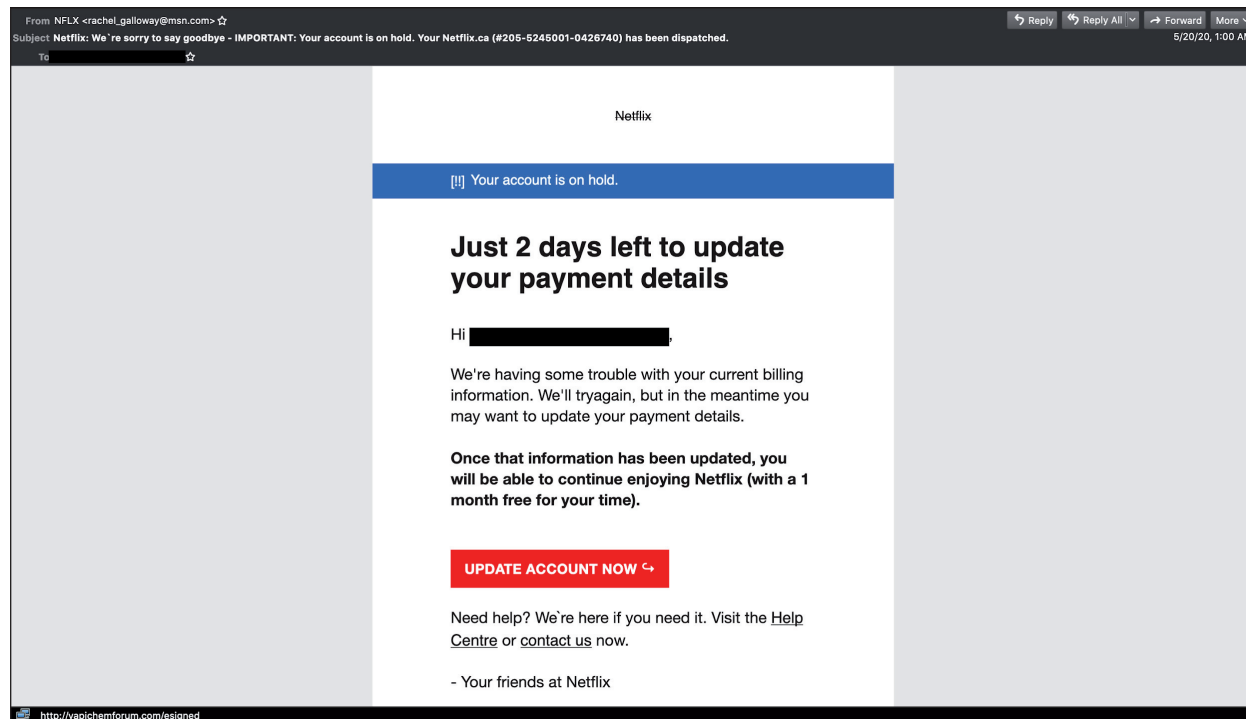
Malware features:

- The URL currently leads to an expired domain.
- This 'Netflix phishing' campaign has previously been seen in our test – it caught our attention on this occasion because it was missed by more products than usual.

RESULTS

Spam catch rates continued to be high, with the majority of products blocking more than 99% of the spam, but the catch rates on malware and phishing were significantly lower.

Four of the participating full solutions achieved a VBSpam award, while two – *Bitdefender* and *Fortinet* – performed well enough to achieve a VBSpam+ award.



Netflix phishing email.

Abusix Mail Intelligence rspamd

SC rate: 98.68%
FP rate: 0.52%
Final score: 95.86
Malware catch rate: 96.72%
Phishing catch rate: 95.60%
Project Honey Pot SC rate: 99.09%
Abusix SC rate: 98.49%
Newsletters FP rate: 8.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Axway MailGate 5.6

SC rate: 99.43%
FP rate: 0.00%
Final score: 99.43
Malware catch rate: 93.71%
Phishing catch rate: 97.07%
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.26%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.76%
FP rate: 0.00%
Final score: 99.76
Malware catch rate: 96.07%
Phishing catch rate: 98.22%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.66%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.84%
FP rate: 0.00%
Final score: 99.84
Malware catch rate: 98.43%
Phishing catch rate: 98.01%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.79%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.53%
FP rate: 0.02%
Final score: 99.45
Malware catch rate: 99.08%
Phishing catch rate: 98.32%
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.34%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libraesva ESG v.4.7

SC rate: 99.62%
FP rate: 0.02%
Final score: 99.54
Malware catch rate: 99.74%
Phishing catch rate: 99.58%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.45%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 95.58%
FP rate: 0.02%
Final score: 95.50
Malware catch rate: 92.01%
Phishing catch rate: 83.35%
Project Honey Pot SC rate: 99.25%
Abusix SC rate: 93.89%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus rsync

SC rate: 93.54%
FP rate: 0.00%
Final score: 93.54
Malware catch rate: 86.37%
Phishing catch rate: 73.93%
Project Honey Pot SC rate: 98.48%
Abusix SC rate: 91.26%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ZEROSPAM

SC rate: 98.48%
FP rate: 0.00%
Final score: 98.45
Malware catch rate: 99.21%
Phishing catch rate: 98.22%
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 97.80%
Newsletters FP rate: 1.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Abusix Mail Intelligence

SC rate: 98.72%
FP rate: 0.13%
Final score: 98.06
Malware catch rate: 93.45%
Phishing catch rate: 95.29%
Project Honey Pot SC rate: 98.58%
Abusix SC rate: 98.78%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 94.35%
FP rate: 0.00%
Final score: 94.35
Malware catch rate: 86.63%
Phishing catch rate: 80.31%
Project Honey Pot SC rate: 99.35%
Abusix SC rate: 92.04%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 92.12%
FP rate: 0.00%
Final score: 92.12
Malware catch rate: 85.98%
Phishing catch rate: 74.87%
Project Honey Pot SC rate: 98.55%
Abusix SC rate: 89.17%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 61.96%
FP rate: 0.00%

IBM X-Force URL contd.

Final score: 61.96
Malware catch rate: 5.77%
Phishing catch rate: 30.68%
Project Honey Pot SC rate: 93.76%
Abusix SC rate: 47.32%
Newsletters FP rate: 0.0%

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-ver20>.

The test ran for 16 days, from 12am on 9 May to 12am on 25 May 2020.

The test corpus consisted of 123,158 emails. 116,896 of these were spam, 36,825 of which were provided by *Project Honey Pot*, with the remaining 80,071 spam emails provided by *Abusix*. There were 6,105 legitimate emails ('ham') and 157 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

278 emails in the spam corpus were considered 'unwanted' (see the June 2018 report¹) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 763 emails from the spam corpus were found to contain a malicious attachment while 955 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.

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 command².

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

¹ <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>

² http://www.postfix.org/XCLIENT_README.html

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: Gyula Hachbold, Adrian Luca, Csaba Mészáros, Tony Oliveira, Ionuț Răileanu







Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

© 2020 Virus Bulletin Ltd, Manor House - Office 6, Howbery Business Park, Wallingford OX10 8BA, UK

Tel: +44 20 3920 6348 Email: editorial@virusbulletin.com

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Abusix Mail Intelligence rspamd	6031	74	0.52%	1538	115135.6	98.68%	95.86	
Axway	6105	0	0.00%	663	116010.6	99.43%	99.43	
Bitdefender	6105	0	0.00%	277.2	116396.4	99.76%	99.76	
FortiMail	6105	0	0.00%	188.4	116485.2	99.84%	99.84	
IBM	6104	1	0.02%	546.8	116126.8	99.53%	99.45	
Libraesva	6104	1	0.02%	443	116230.6	99.62%	99.54	
Spamhaus DQS	6104	1	0.02%	5157.2	111516.4	95.58%	95.50	
Spamhaus rsync	6105	0	0.00%	7537.4	109136.2	93.54%	93.54	
ZEROSPAM	6105	0	0.00%	1775	114888.6	98.48%	98.45	
Abusix Mail Intelligence*	6056	49	0.13%	1499.2	115174.4	98.72%	98.06	N/A
IBM X-Force Combined*	6105	0	0.00%	6597.8	110075.8	94.35%	94.35	N/A
IBM X-Force IP*	6105	0	0.00%	9188.2	107485.4	92.12%	92.12	N/A
IBM X-Force URL*	6105	0	0.00%	44378.6	72295	61.96%	61.96	N/A

*These 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		Phishing		Project Honey Pot		Abusix		STDev [†]
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Abusix Mail Intelligence rspamd	13	8.3%	25	96.72%	42	95.60%	334.4	99.09%	1203.6	98.49%	1.39
Axway	0	0.0%	48	93.71%	28	97.07%	70.6	99.81%	592.4	99.26%	0.88
Bitdefender	0	0.0%	30	96.07%	17	98.22%	6	99.98%	271.2	99.66%	0.63
FortiMail	0	0.0%	12	98.43%	19	98.01%	21.2	99.94%	167.2	99.79%	0.42
IBM	0	0.0%	7	99.08%	16	98.32%	21	99.94%	525.8	99.34%	2.7
Libraesva	0	0.0%	2	99.74%	4	99.58%	7	99.98%	436	99.45%	0.61
Spamhaus DQS	0	0.0%	61	92.01%	159	83.35%	276.6	99.25%	4880.6	93.89%	3.85
Spamhaus rsync	0	0.0%	104	86.37%	249	73.93%	560	98.48%	6977.4	91.26%	5.62
ZEROSPAM	2	1.3%	6	99.21%	17	98.22%	14	99.96%	1761	97.80%	1.83
Abusix Mail Intelligence*	0	0.0%	50	93.45%	45	95.29%	522.2	98.58%	977	98.78%	1.7
IBM X-Force Combined*	0	0.0%	102	86.63%	188	80.31%	240.2	99.35%	6357.6	92.04%	5.08
IBM X-Force IP*	0	0.0%	107	85.98%	240	74.87%	534	98.55%	8654.2	89.17%	5.54
IBM X-Force URL*	0	0.0%	719	5.77%	662	30.68%	2297.6	93.76%	42081	47.32%	12.06

*These products 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.

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

	Speed			
	10%	50%	95%	98%
Abusix Mail Intelligence rspamd	●	●	●	●
Axway	●	●	●	●
Bitdefender	●	●	●	●
FortiMail	●	●	●	●
IBM	●	●	●	●
Libraesva	●	●	●	●
Spamhaus DQS	●	●	●	●
Spamhaus rsync	●	●	●	●
ZEROSPAM	●	●	●	●

● 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.)

Products ranked by final score	
FortiMail	99.84
Bitdefender	99.76
Libraesva	99.54
IBM	99.45
Axway	99.43
ZEROSPAM	98.45
Abusix Mail Intelligence rspamd	95.86
Spamhaus DQS	95.50
Spamhaus rsync	93.54

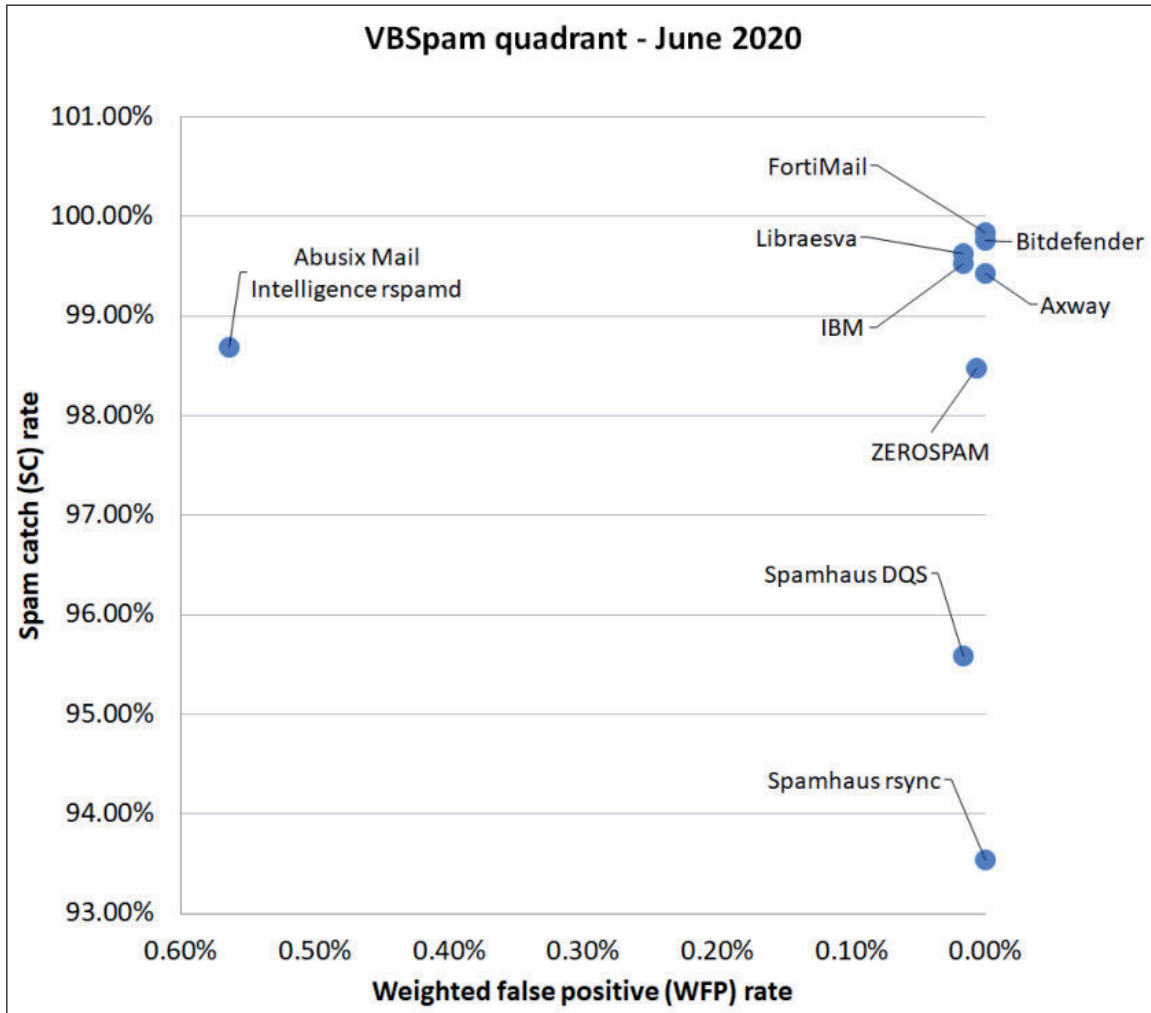
(Please refer to the text for full product names and details.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
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	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Libraesva	ClamAV; others optional		√	√		√		√	
Spamhaus DQS	Optional	√	√	√					√
Spamhaus rsync	Optional	√	√	√					√

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



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