DECEMBER 2020

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW DECEMBER 2020

Ionuţ Răileanu

In this test – which forms part of *Virus Bulletin*'s continuously running security product test suite – six full email security solutions, one custom configured solution[1] and four blacklists of various kinds elected to be publicly tested against various streams of wanted, unwanted and malicious emails, the results for which are included in this report.

Filtering the large bulk of spam emails is a task that the security solutions covered in this report managed to accomplish very well. However, spam is still the most common attack vector and the most sophisticated threats don't come in bulk. By malware and phishing emails we relate to these rare spam emails, which are usually more difficult to be filtered, so to have a better view of the tested solutions, we recommend to check these catch rates too. The novelty in this test is an increase of phishing emails that use legitimate services (e.g. *Google Docs*) to deliver the malicious payloads.

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.)*

[1] *Spamhaus DQS* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

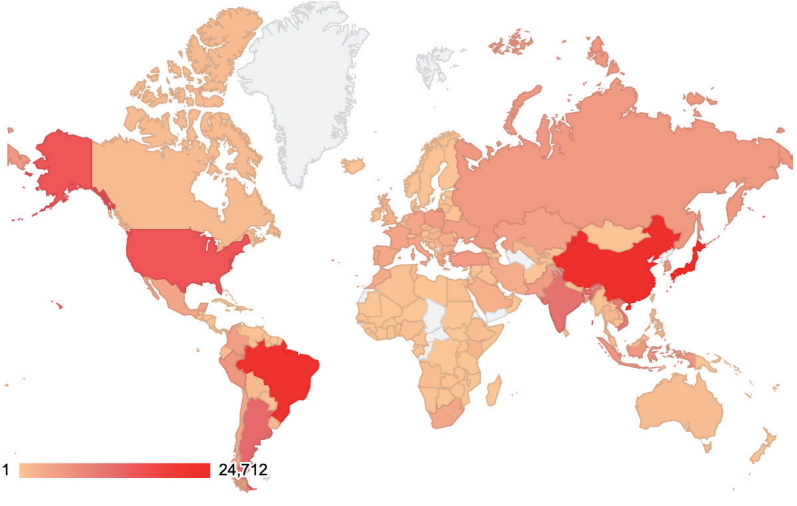
MALWARE AND PHISHING

In this section we present some of malware and phishing emails that proved the most challenging for the products in the test.[2] By 'malware' we mean those emails containing a malicious attachment. By 'phishing' we mean emails that contain URLs that lead to malware, as well as those that impersonate a legitimate institution/individual and those that attempt to steal a user's credentials.

[2] This analysis is not intended to be exhaustive research on these samples but rather a short overview of the most commonly missed malware and phishing emails in the test.

#	Sender's IP country	Percentage of spam
1	Japan	8.65%
2	China	8.47%
3	Brazil	7.82%
4	United States	5.38%
5	Argentina	4.38%
6	India	3.90%
7	Vietnam	3.21%
8	Peru	2.14%
9	Republic of Korea	2.09%
10	Indonesia	1.99%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

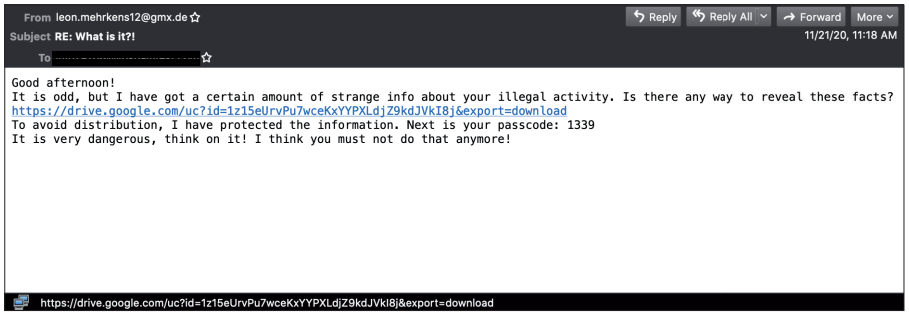
ISSN 1749-7027

Google docs URLs with password-protected files

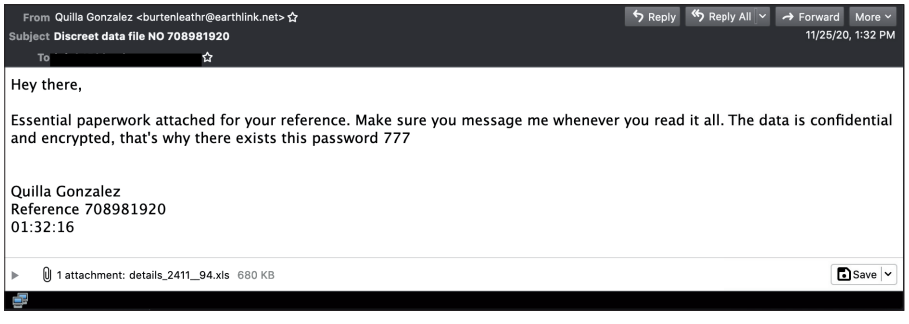
This phishing campaign was the most challenging for the security solutions we tested. The *Google Docs* URLs were active for a short period of time and downloaded a password-protected zip archive. We found similarities with other spam campaigns of this kind that were active during the same period (20 – 23 November), but we weren't able to obtain more for our analysis as the URLs were unavailable at the time of our research.

zLoader

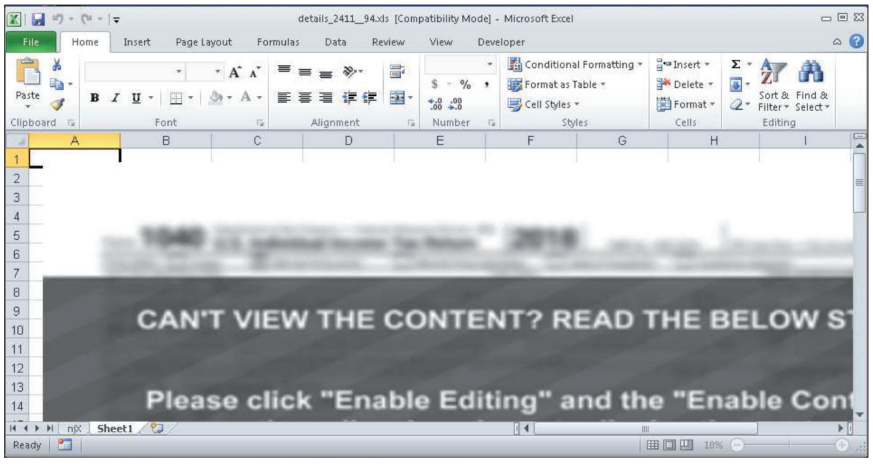
The majority of the security solutions in our test failed to correctly filter emails of this kind. The attached .XLS file is password protected (with the password provided in the content of the email) and, when opened, it tries to send a request to purefile24[.]top, a domain that has been reported in connection with zLoader. At the time of our analysis, no malicious payload was downloaded from that domain.



Example of a phishing email containing legitimate URLs.



Example of a zLoader malspam.



Screenshot of an opened XLS file that leads to zLoader.

RESULTS

Spam catch rates were high, with all of the products blocking more than 99% of the spam, but those on malware and phishing were significantly lower. Of the participating full solutions, one achieved a VBSpam award – *ZEROSPAM* – while a further six performed well enough to achieve a VBSpam+ award: *Axway*, *Bitdefender*, *Fortinet*, *IBM Lotus Protector*, *Libraesva* and *Spamhaus DQS*.

Axway MailGate 5.6

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Malware catch rate: 86.01%
Phishing catch rate: 98.10%
Project Honey Pot SC rate: 99.89%
Abusix SC rate: 99.81%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.92%
FP rate: 0.00%
Final score: 99.92
Malware catch rate: 98.60%
Phishing catch rate: 98.95%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.89%
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: 99.22%
Phishing catch rate: 96.96%
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.81%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.86%
FP rate: 0.00%
Final score: 99.86
Malware catch rate: 98.82%
Phishing catch rate: 98.34%
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.84%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libraesva ESG v.4.7

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Malware catch rate: 99.94%
Phishing catch rate: 98.81%
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 99.59%
FP rate: 0.00%
Final score: 99.49
Malware catch rate: 98.94%
Phishing catch rate: 97.05%
Project Honey Pot SC rate: 99.30%
Abusix SC rate: 99.59%
Newsletters FP rate: 0.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.54%
FP rate: 0.02%
Final score: 99.36
Malware catch rate: 99.66%
Phishing catch rate: 98.57%
Project Honey Pot SC rate: 99.21%
Abusix SC rate: 99.53%
Newsletters FP rate: 0.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 99.25%
FP rate: 0.19%
Final score: 98.35
Malware catch rate: 97.20%
Phishing catch rate: 97.72%
Project Honey Pot SC rate: 95.51%
Abusix SC rate: 99.78%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 98.08%
FP rate: 0.02%
Final score: 97.98
Malware catch rate: 87.30%
Phishing catch rate: 88.60%
Project Honey Pot SC rate: 98.25%
Abusix SC rate: 98.01%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 96.19%
FP rate: 0.02%
Final score: 96.08
Malware catch rate: 87.02%
Phishing catch rate: 87.32%
Project Honey Pot SC rate: 97.24%
Abusix SC rate: 95.99%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 65.30%
FP rate: 0.00%
Final score: 65.30
Malware catch rate: 3.53%
Phishing catch rate: 17.34%
Project Honey Pot SC rate: 76.22%
Abusix SC rate: 63.64%
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 19 days, from 12am on 7 November to 12am on 26 November 2020 (GMT).

The test corpus consisted of 291,075 emails. 285,669 of these were spam, 36,705 of which were provided by *Project Honey Pot*, with the remaining 248,964 spam emails provided by *Abusix*. There were 4,853 legitimate emails ('ham') and 553 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

426 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[3]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 1,787 emails from the spam corpus were found to contain a malicious attachment while 2,105 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 command[4].

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 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:

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)

[3] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review
[4] http://www.postfix.org/XCLIENT_README.html

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, Ionuţ Răileanu

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

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
Axway	4853	0	0.00%	501.8	284826.4	99.82%	99.82	
Bitdefender	4853	0	0.00%	240	285088.2	99.92%	99.92	
FortiMail	4853	0	0.00%	467	284861.2	99.84%	99.84	
IBM	4853	0	0.00%	388.6	284939.6	99.86%	99.86	
Libraesva	4853	0	0.00%	242.8	285085.4	99.91%	99.91	
Spamhaus DQS	4853	0	0.00%	1158.2	284169	99.59%	99.49	
ZEROSPAM	4852	1	0.02%	1298.6	284013.6	99.54%	99.36	
Abusix Mail Intelligence*	4844	9	0.19%	2126.6	283201.6	99.25%	98.35	N/A
IBM X-Force Combined*	4852	1	0.02%	5469.4	279858.8	98.08%	97.98	N/A
IBM X-Force IP*	4852	1	0.02%	10884.8	274443.4	96.19%	96.08	N/A
IBM BL - URL*	4853	0	0.00%	99019.2	186309	65.30%	65.30	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	
Axway	0	0.0%	250	86.01%	40	98.10%	41	99.89%	460.8	99.81%	1.32
Bitdefender	0	0.0%	25	98.60%	22	98.95%	4	99.99%	236	99.89%	0.28
FortiMail	0	0.0%	14	99.22%	64	96.96%	97	99.73%	370	99.81%	0.84
IBM	0	0.0%	21	98.82%	35	98.34%	97.8	99.73%	290.8	99.84%	0.54
Libraesva	0	0.0%	1	99.94%	25	98.81%	37.6	99.90%	205.2	99.90%	0.38
Spamhaus DQS	5	0.9%	19	98.94%	62	97.05%	256.8	99.30%	901.4	99.59%	1.00
ZEROSPAM	4	0.7%	6	99.66%	30	98.57%	289.4	99.21%	1009.2	99.53%	1.41
Abusix Mail Intelligence*	0	0.0%	50	97.20%	48	97.72%	1641.4	95.51%	485.2	99.78%	1.27
IBM X-Force Combined*	0	0.0%	227	87.30%	240	88.60%	641	98.25%	4828.4	98.01%	2.69
IBM X-Force IP*	0	0.0%	232	87.02%	267	87.32%	1010.8	97.24%	9874	95.99%	4.39
IBM BL - URL*	0	0.0%	1724	3.53%	1740	17.34%	8703	76.22%	90316.2	63.64%	17.39

**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%
Axway	●	●	●	●
Bitdefender	●	●	●	●
FortiMail	●	●	●	●
IBM	●	●	●	●
Libraesva	●	●	●	●
Spamhaus DQS	●	●	●	●
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	
Bitdefender	99.92
Libraesva	99.91
IBM	99.86
FortiMail	99.84
Axway	99.82
Spamhaus DQS	99.49
ZEROSPAM	99.36

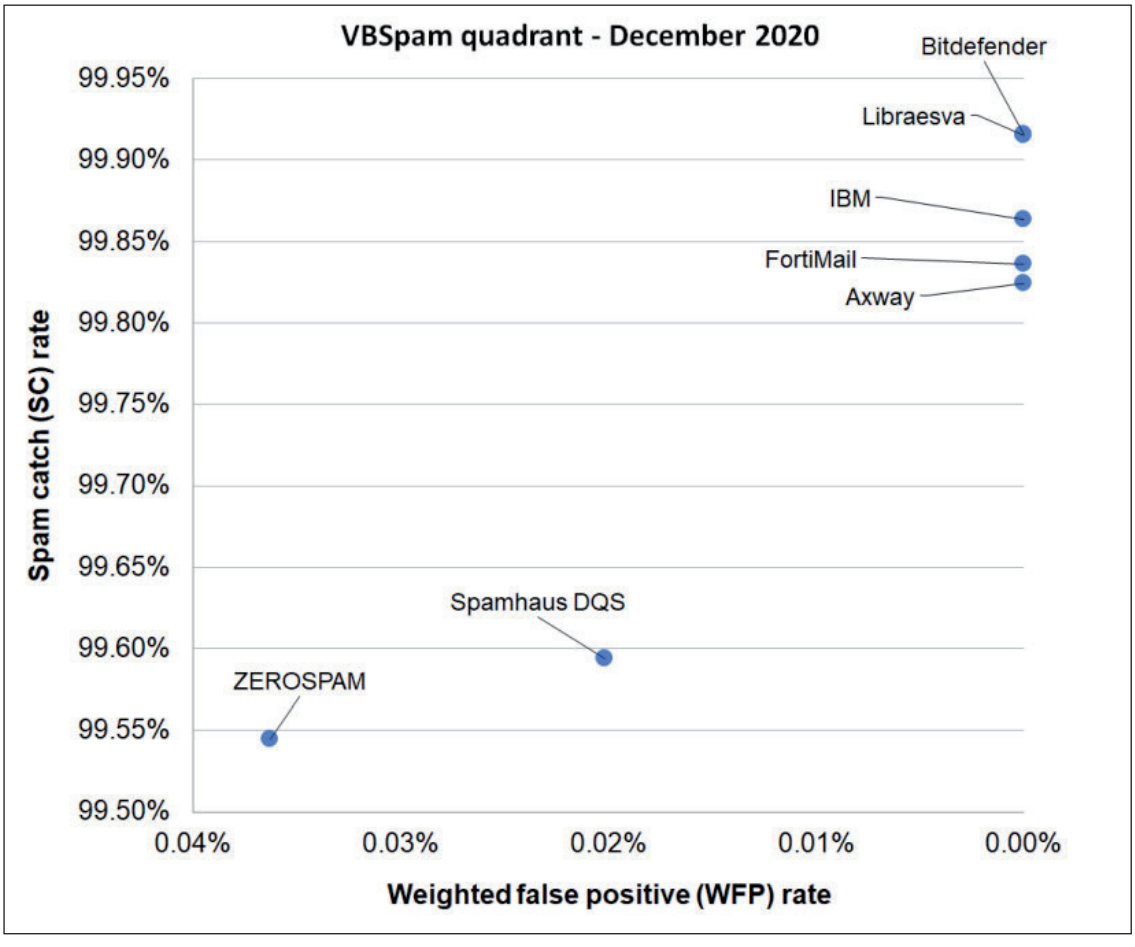
(Please refer to the text for full product names and details.)

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	√	√	√					√

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



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