SEPTEMBER 2020

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 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, the results for which are included in this report.

The results detailed in the VBSpam test reports generally indicate that email security products do a good job of blocking the majority of spam emails. However, in this report we will focus on those emails that, through attachments or URLs, lead directly to a malicious action, and highlight the particular emails that managed to evade most of the security products filters in our test. Since the emails used in the test cover the threats that exist at the moment when it is run, we are able to determine how the security solutions are performing against up-to-date spam campaigns.

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.

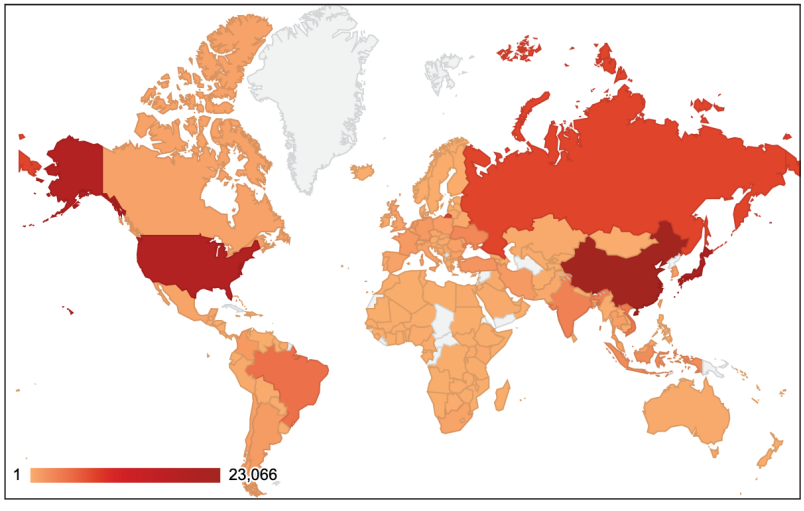
CHALLENGING EMAILS

The spam campaign that the products in this test found the most challenging to block was one that sent stock exchange-related emails. The emails didn't contain any attachments or URLs and were sent from free email service accounts (mail[.]ru, gmx[.]net and gmx[.]com). The campaign was active on 17 August from 12:13 to 12:48 GMT and then again for a short time the next day, 18 August, around 12:50 GMT.

Axway was the only product that managed to block all the emails from this campaign.

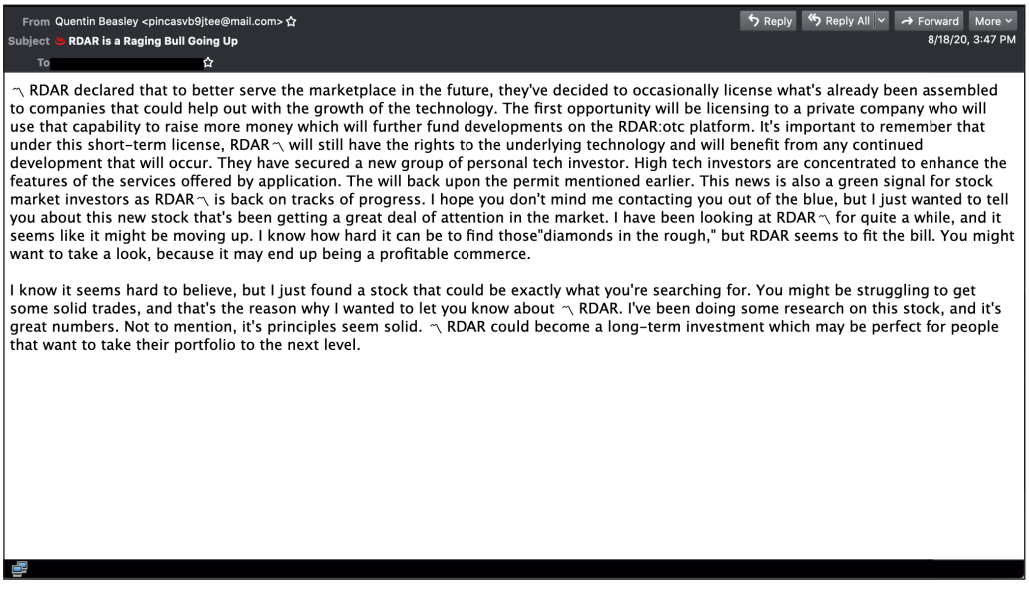
#	Sender's IP country	Percentage of spam
1	China	18.50%
2	Japan	16.30%
3	United States	14.83%
4	Russian Federation	6.19%
5	Brazil	3.70%
6	Vietnam	3.01%
7	India	2.63%
8	Ukraine	2.24%
9	Indonesia	1.90%
10	Turkey	1.39%

Top 10 countries from which spam was sent.

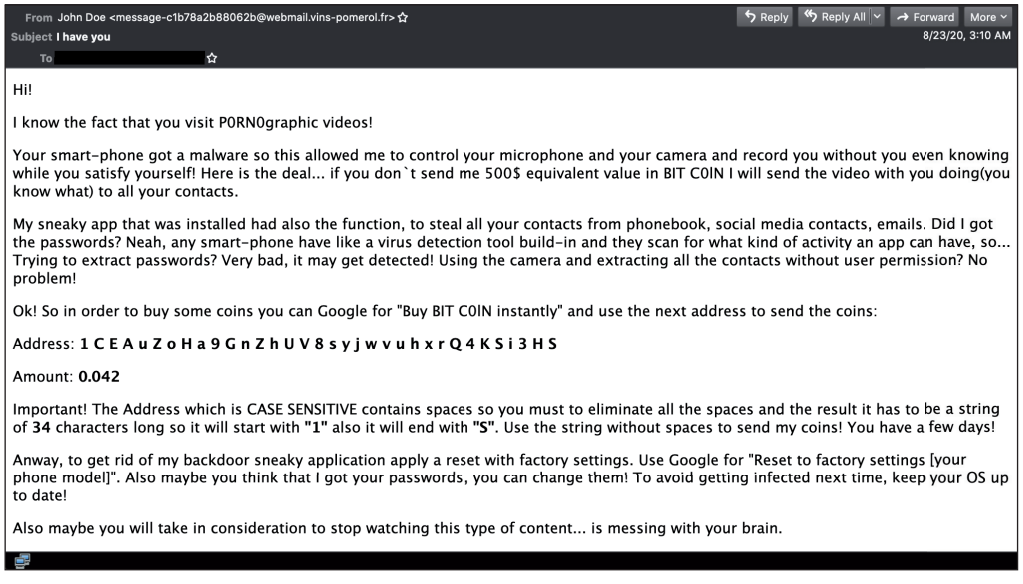


Geographical distribution of spam based on sender IP address.

ISSN 1749-7027



Sample from the RDAR spam campaign.



Example of an extortion spam.

We continue to see extortion emails in the spam feeds, but it looks like, despite all the evasive techniques used to bypass the filters of the security products, this kind of spam is reaching inboxes less. However, we mention here a sample that was missed by most of the products in the test (the products that blocked it were: *Axway, IBM, Libraesva, ZEROSPAM*, and the partial solutions *Abusix Mail Intelligence*, *IBM X-Force IP* and *IBM X-Force Combined*).

MALWARE AND PHISHING

In the following sections we present some of malware and phishing emails that proved the most challenging for the products we saw in the test.[2]

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

1. Password-protected archives containing malicious '.doc' files

Subjects:

- `Re: (no subject)`
- `Re: Alarm`

Attachments:

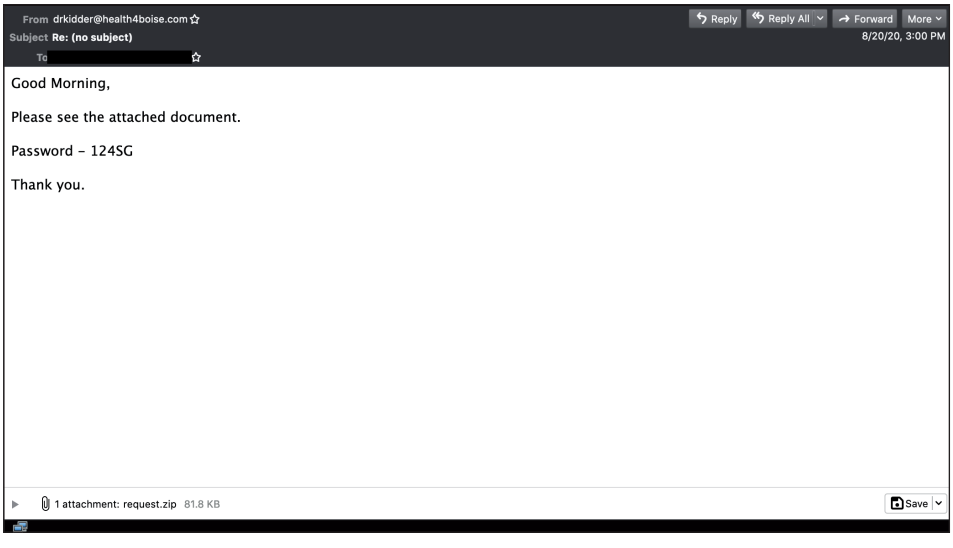
- `request.zip: 329e45d95f39e6e68f7659bf4947649f971489c3257bfb2b136f59323d862fed`, which contained `report,08.20.doc: 979f10f83dcf1e9a9aad6e30f42ac6d84d9c329e0f08b3232ca04366aae23072`
- `Request.zip: 0062169d2871199582141e20b6eb0d371f4d0bc304bd6d1347ebe5cae4b06820`, which contained `report,08.20.doc: 6d93346bea6220274108bfe72decb671687c80d53c434e74fe03c106379fb81c`

MAIL FROM:

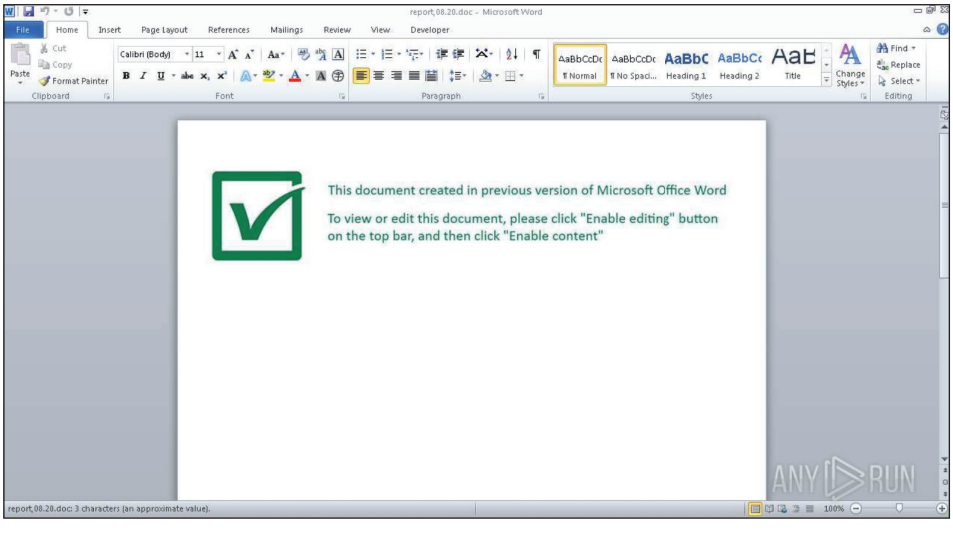
- `drkidder@health4boise.com`
- `megan@hot-deals-online.com`

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

- 20 August 12:04 GMT; two products: *Libraesva* and *ZEROSPAM*.



A capture of the email.



The attached .doc file, captured when opening the archive in the app.any.run sandbox.

- 20 August 13:02 GMT; four products: *IBM*, *Fortinet*, *Libraesva* and *ZEROSPAM*)

Malware features:

- Because the attached archive is password protected it is a challenge for anti-spam solutions to block the emails at first sight.
- It has been reported[3] that this campaign was pushing IcedID to English-speaking recipients.

2. Fattura n.XXXXX del 05/17/2020

Subjects:

- `Fattura n.[0-9]{5} del 05/17/2020`

Attachments:

- `fattura_174.xls: 768fb3244d426ccdd043fc5f72276f69494b50d20f49477f039c9911d878a3cb`
- `fattura_4423.xlsm: f1cf9543cc45d69177dac3b26015955c0d6c34295fd688df501eea9a11b85e92`
- `fattura_1194.xls: caac5b35adcf5efeacec8f82357f7e25d0f7cb0f73c4354ddccfff52f881ee7b`
- `fattura_489.xls: 5e145ca74870d3db2317eb6fc46371ef388054dfffc8d138b06da1ac6c6e9fe7`
- `Fattura_960.xls: 5f5c86843bea1ebfa1cd7de5140b78f6023785d98d05a27f45b91ef200adc21b`

MAIL FROM:

- `noreply@ticketnet.cloud`
- `noreply@implantology.club`
- `noreply@realtycashcow.club`
- `noreply@hotsales.cf`

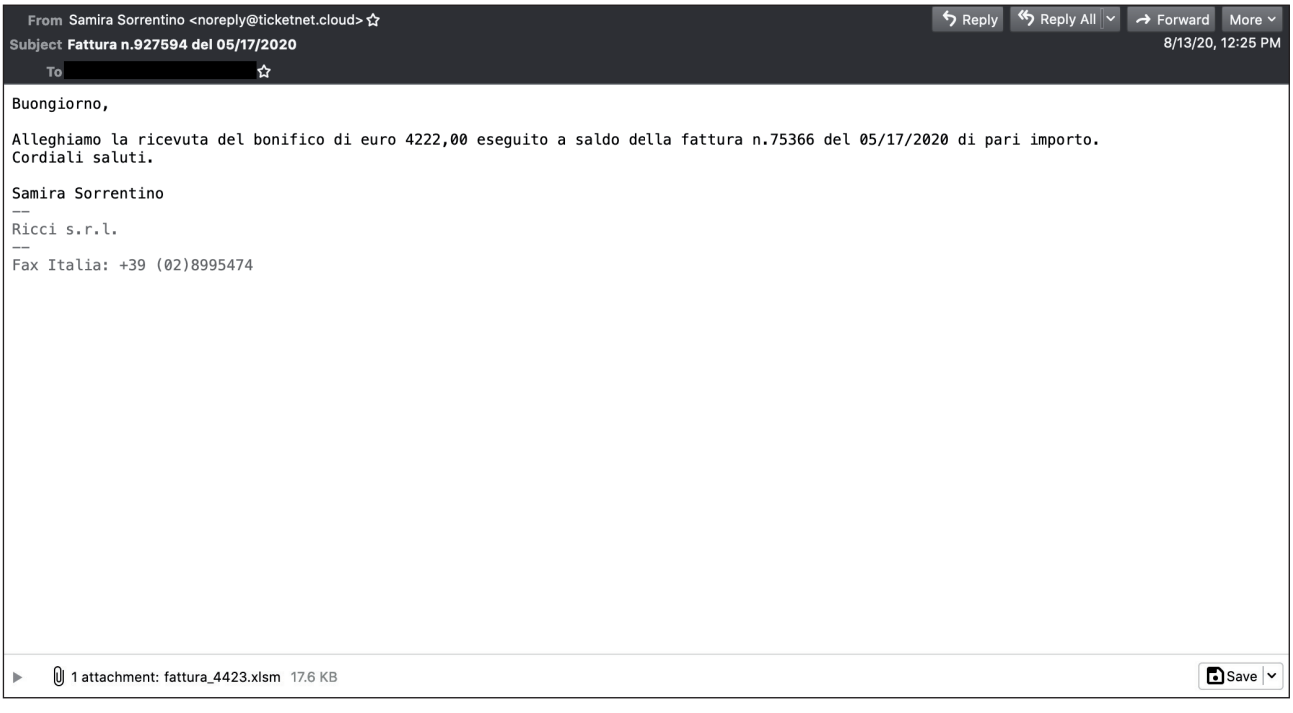
Dates of occurrence and number of products that correctly blocked it:

- There were 20 emails in approximately 15 minutes (09:25:20 to 09:38:45 on 13 August). Only those with the `noreply@ticketnet.cloud` MAIL FROM seem to have bypassed the filters of all the solutions in the test, with the exception of *Fortinet*, *IBM* and *Libraesva*.

Malware features:

- A geographically targeted spam campaign, active for a few minutes, containing password-protected '.xls' files.
- Based on our research, it looks like this is a Gootkit campaign.

[3] https://twitter.com/malware_traffic/status/1296480451301912577.



A capture of the malware campaign in Italian.

3. Emotet

Subjects:

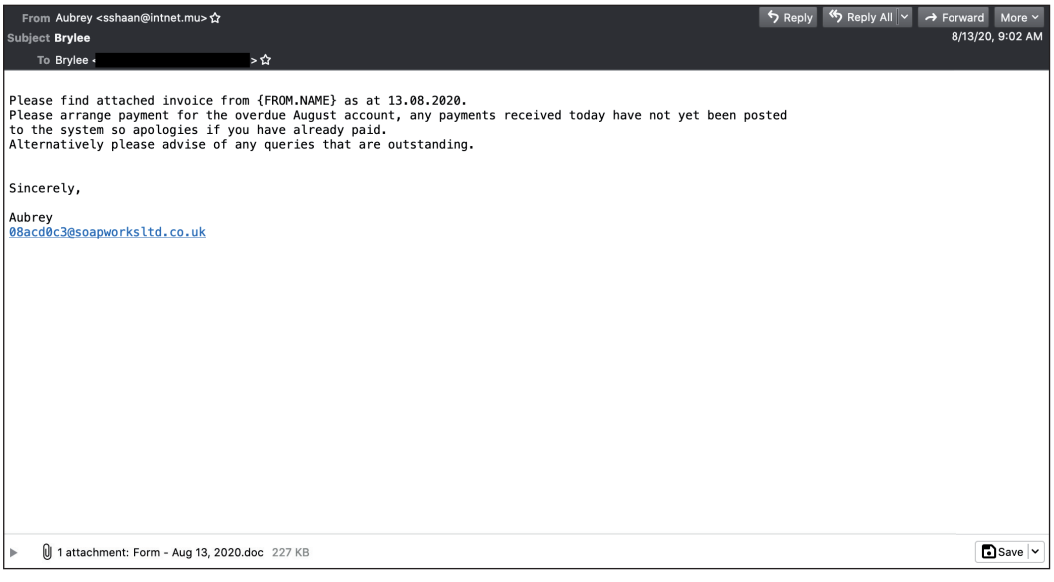
- `Eintragung`
- First names (e.g. `Brylee`, `Magdalena`, `Meike`, `Bianca`)

Attachments:

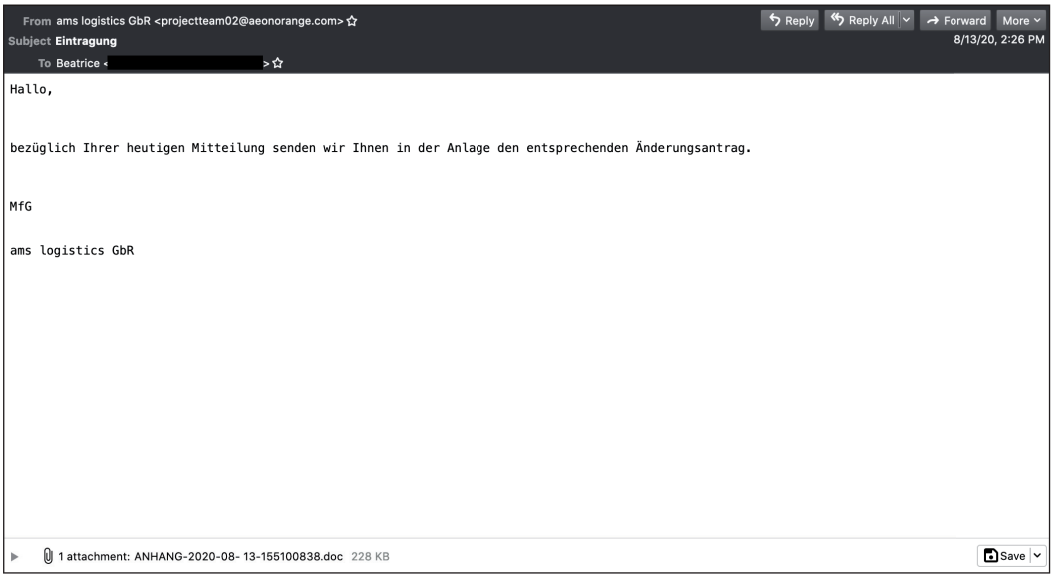
- `ANHANG-2020-08- 13-155100838.doc: c30a4592cd8e7e2a97b2ee19d0061553ccbd7cd1b7e2af8bca2dd6913a1bccb5`
- `Form - Aug 13, 2020.doc: ba510b5a0f97430a09efbd12acbb4c1be869e71e678adf5fa0b5498fb477068e`
- `PO# 08152020Ex.doc: 72af635d51194d2ab428924c2c7f51aa4a9d040e93566ed7302ed43f5fa16eed`
- `Electronic form.doc: 62f25d164ef59be5ad282fad344656d63ae755643c7be3b729899b31c97b0925`

MAIL FROM:

- `projectteam02@aeonorange.com`



The most common version seen in the test of spam containing Emotet.



A different version of the Emotet spam from the test.

- sshaan@intnet.mu
- ksj@yses.kr
- cheryllong@iuncapped.co.za

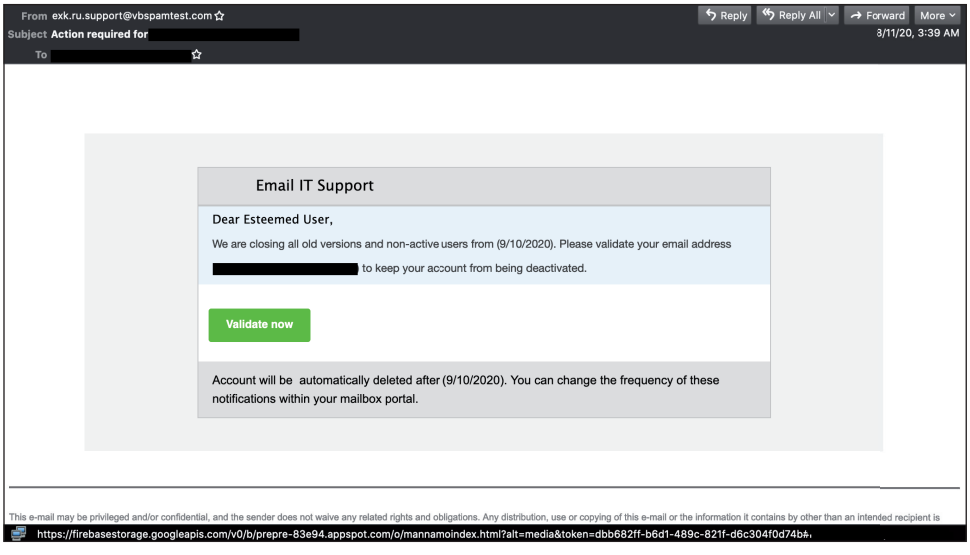
Dates of occurrence and number of products that correctly blocked it:

- We saw Emotet spam emails on every day of the test apart from at weekends.
- The only products that didn't miss any of the emails from this campaign were *IBM*, *Libraesva* and *Spamhaus DQS*.

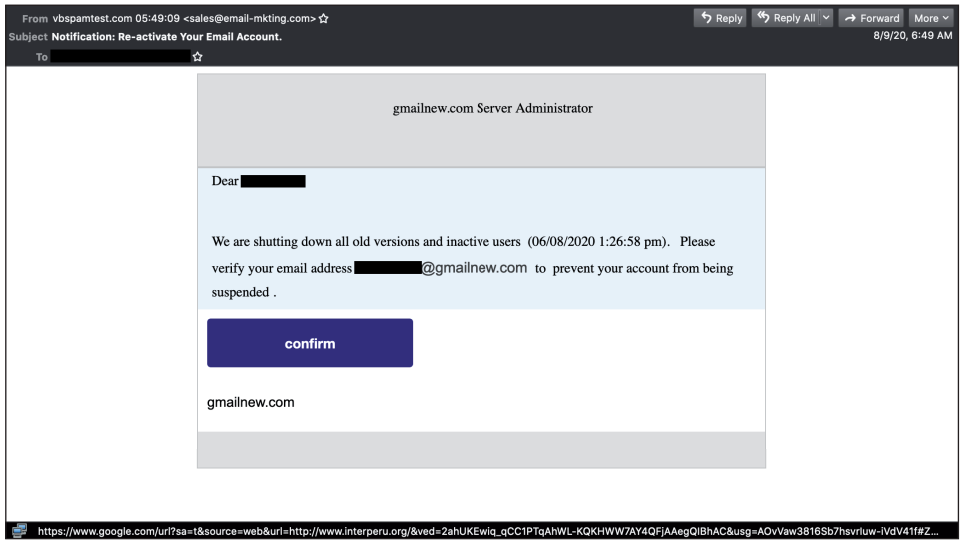
4. Phishing that uses public legitimate Google services as a proxy

Subjects:

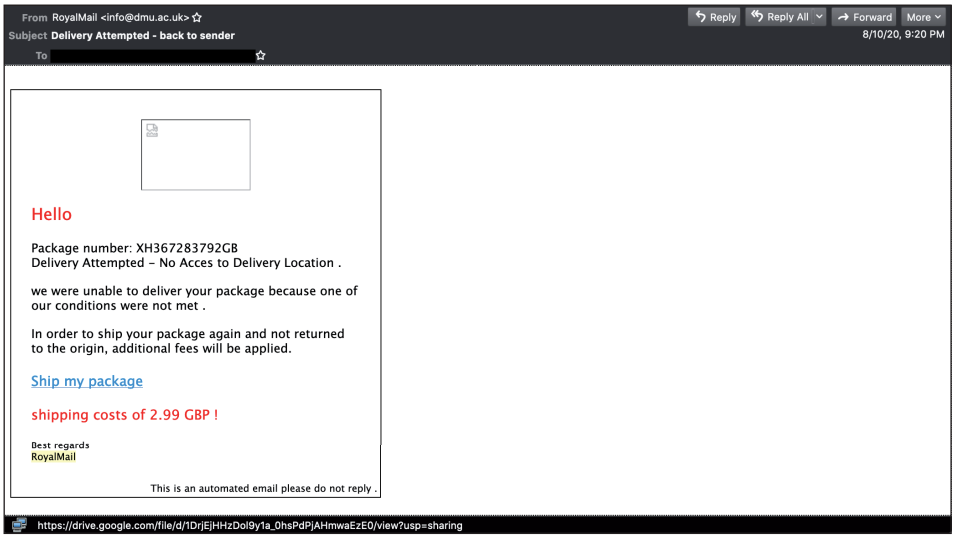
- Action required for *recipient email address*
- Notification: Re-activate Your Email Account.
- Delivery Attempted - back to sender
- Delayed invoice detailsfororder452062



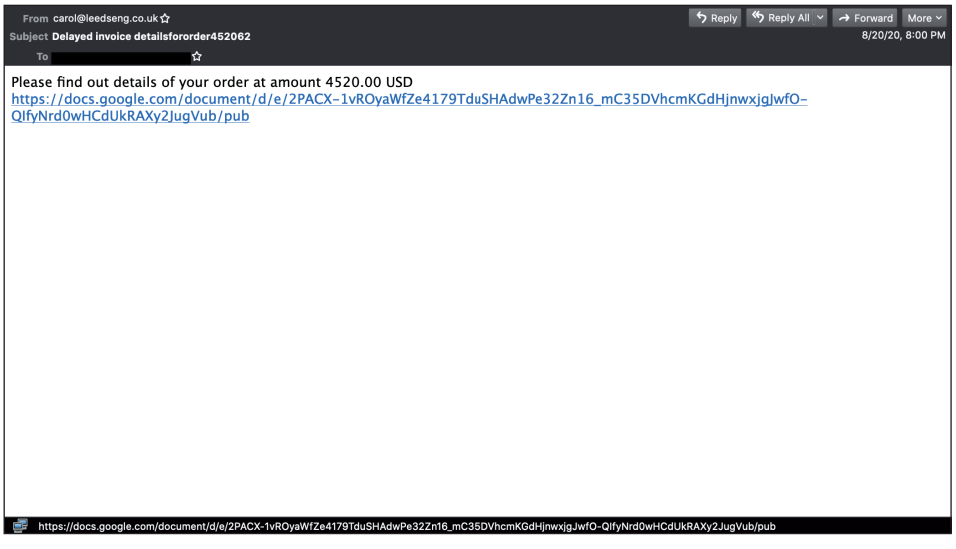
This phishing email was missed by the most products.



Phishing email redirecting the landing page through Google browser.



Phishing email making use of the Google Drive service.



Another example of a phishing email making use of the Google Drive service.

MAIL FROM:

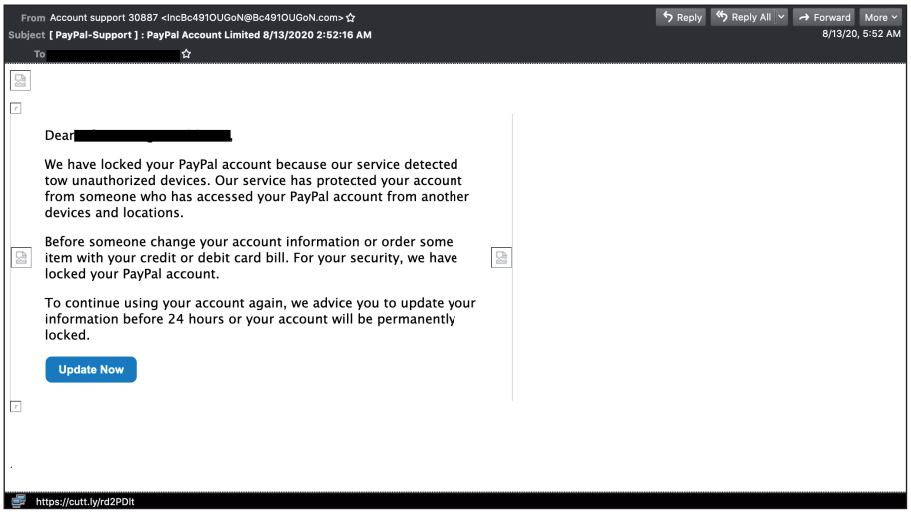
- `support@recipient_email_address_domain`
- `sales@email-mkting.com`
- `info@dmu.ac.uk`
- `carol@leedseng.co.uk`

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

- 11 August; three products: *Axway*, *IBM* and *Libraesva*.
- 9 August; four products: *Axway*, *Bitdefender*, *Libraesva* and *ZEROSPAM*.
- 10 August; two products: *Libraesva* and *ZEROSPAM*.
- 20 August; four products: *Fortinet*, *IBM*, *Libraesva* and *ZEROSPAM*.

Malware features:

- We couldn't track the malicious behaviour further, since the URLs were either no longer accessible or



Capture of the PayPal phishing email.

had been blocked by *Google* for violating the service's terms and conditions.

- These phishing emails were the most challenging for the products in our test.

5. PayPal phishing with shortened URL

Subjects:

- `[ PayPal-Support ] : PayPal Account Limited 8/13/2020 2:52:16 AM`

Malicious URL:

- `hxxps://cutt[.]ly/rd2PDlt`

MAIL FROM:

- `japos7@juno.com`

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

- 13 August; four products: *Bitdefender*, *Libraesva*, *Spamhaus DQS* and *ZEROSPAM*.

Malware features:

- We couldn't track the malicious behaviour further, since the URL is no longer accessible.

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. Of the participating full solutions, two achieved a VBSpam award: *Libraesva* and *ZEROSPAM*, while four performed well enough to achieve a VBSpam+ award: *Axway*, *Bitdefender*, *Fortinet* and *IBM Lotus Protector*. The *Spamhaus DQS* custom configured solution also achieved a VBSpam award.

Axway MailGate 5.6

SC rate: 99.71%
FP rate: 0.00%
Final score: 99.68
Malware catch rate: 91.79%
Phishing catch rate: 96.88%
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.64%
Newsletters FP rate: 0.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.88%
FP rate: 0.00%
Final score: 99.88
Malware catch rate: 96.54%
Phishing catch rate: 97.64%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.84%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.71%
FP rate: 0.00%
Final score: 99.71
Malware catch rate: 94.71%
Phishing catch rate: 93.01%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.61%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.78%
FP rate: 0.00%
Final score: 99.78
Malware catch rate: 97.62%
Phishing catch rate: 97.54%
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.72%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libraesva ESG v.4.7

SC rate: 99.94%
FP rate: 0.02%
Final score: 99.84
Malware catch rate: 99.89%
Phishing catch rate: 99.43%
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.93%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service

SC rate: 98.72%
FP rate: 0.00%
Final score: 98.72
Malware catch rate: 96.87%
Phishing catch rate: 83.85%
Project Honey Pot SC rate: 99.58%
Abusix SC rate: 98.42%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.69%
FP rate: 0.06%
Final score: 99.35
Malware catch rate: 92.87%
Phishing catch rate: 99.34%
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.59%
Newsletters FP rate: 0.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Abusix Mail Intelligence

SC rate: 99.25%
FP rate: 0.06%
Final score: 98.94
Malware catch rate: 71.17%
Phishing catch rate: 94.90%
Project Honey Pot SC rate: 98.61%
Abusix SC rate: 99.47%
Newsletters FP rate: 0.0%

IBM X-Force Combined

SC rate: 96.05%
FP rate: 0.00%
Final score: 96.05
Malware catch rate: 75.70%
Phishing catch rate: 82.34%
Project Honey Pot SC rate: 99.13%
Abusix SC rate: 95.00%
Newsletters FP rate: 0.0%

IBM X-Force IP

SC rate: 93.54%
FP rate: 0.00%
Final score: 93.54
Malware catch rate: 66.85%
Phishing catch rate: 78.00%
Project Honey Pot SC rate: 98.61%
Abusix SC rate: 91.80%
Newsletters FP rate: 0.0%

IBM X-Force URL

SC rate: 67.06%
FP rate: 0.00%
Final score: 67.06
Malware catch rate: 18.36%
Phishing catch rate: 24.36%
Project Honey Pot SC rate: 92.81%
Abusix SC rate: 58.26%
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 8 August to 12am on 24 August 2020.

The test corpus consisted of 129,515 emails. 124,691 of these were spam, 31,775 of which were provided by *Project Honey Pot*, with the remaining 92,916 spam emails provided by *Abusix*. There were 4,686 legitimate emails ('ham') and 138 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

144 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[4]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 926 emails from the spam corpus were found to contain a malicious attachment while 1,059 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[5].

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)

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/

[4] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Axway	4686	0	0.00%	366	124209.8	99.71%	99.68	SPAM + Verified
Bitdefender	4686	0	0.00%	152	124423.8	99.88%	99.88	SPAM + Verified
FortiMail	4686	0	0.00%	362.6	124213.2	99.71%	99.71	SPAM + Verified
IBM	4686	0	0.00%	278.8	124297	99.78%	99.78	SPAM + Verified
Libraesva	4685	1	0.02%	70.4	124505.4	99.94%	99.84	SPAM Verified
Spamhaus DQS	4686	0	0.00%	1600.4	122975.4	98.72%	98.72	SPAM Verified
ZEROSPAM	4683	3	0.06%	388.2	124178.6	99.69%	99.35	SPAM Verified
Abusix Mail Intelligence*	4683	3	0.06%	929.2	123646.6	99.25%	98.94	N/A
IBM X-Force Combined*	4686	0	0.00%	4922.2	119653.6	96.05%	96.05	N/A
IBM X-Force IP*	4686	0	0.00%	8051	116524.8	93.54%	93.54	N/A
IBM BL - URL*	4686	0	0.00%	41029.2	83546.6	67.06%	67.06	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	1	0.72%	76	91.79%	33	96.88%	32	99.90%	334	99.64%	1.16
Bitdefender	0	0.00%	32	96.54%	25	97.64%	2	99.99%	150	99.84%	0.26
FortiMail	0	0.00%	49	94.71%	74	93.01%	3.2	99.99%	359.4	99.61%	0.58
IBM	0	0.00%	22	97.62%	26	97.54%	14.4	99.95%	264.4	99.72%	0.66
Libraesva	0	0.00%	1	99.89%	6	99.43%	3	99.99%	67.4	99.93%	0.59
Spamhaus DQS	0	0.00%	29	96.87%	171	83.85%	134	99.58%	1466.4	98.42%	1.96
ZEROSPAM	1	0.72%	66	92.87%	7	99.34%	7	99.98%	381.2	99.59%	0.93
Abusix Mail Intelligence*	0	0.00%	267	71.17%	54	94.90%	440.6	98.61%	488.6	99.47%	1.03
IBM X-Force Combined*	0	0.00%	225	75.70%	187	82.34%	276.8	99.13%	4645.4	95.00%	3.68
IBM X-Force IP*	0	0.00%	307	66.85%	233	78.00%	441.4	98.61%	7609.6	91.80%	4.26
IBM BL - URL*	0	0.00%	756	18.36%	801	24.36%	2284.6	92.81%	38744.6	58.26%	11.06

**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%**
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	99.88
Libraesva	99.84
IBM	99.78
FortiMail	99.71
Axway	99.68
ZEROSPAM	99.35
Spamhaus DQS	98.72

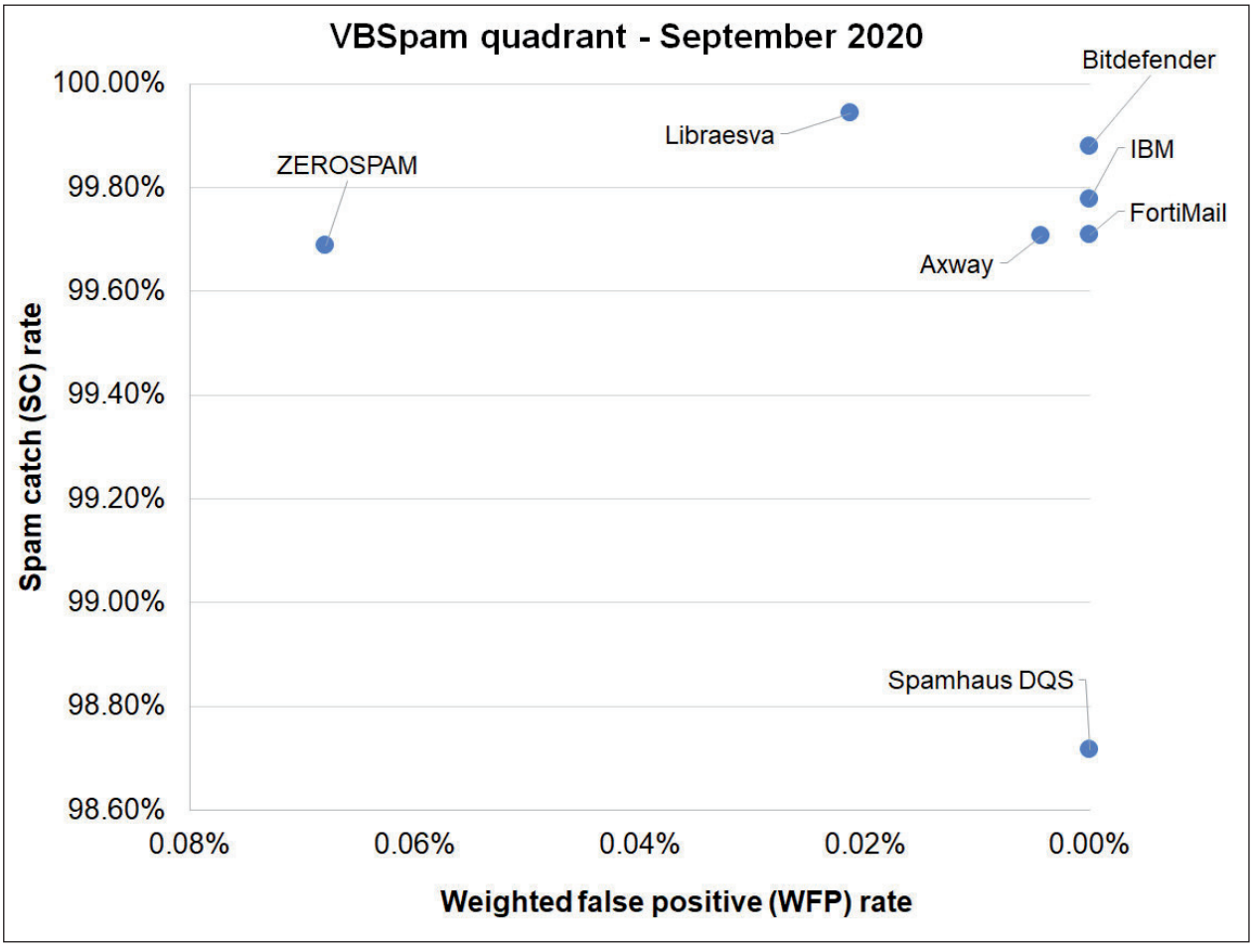
(Please refer to the text for full product names and details.)

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.)