SEPTEMBER 2024

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 2024

Ionuţ Răileanu & Adrian Luca

In the Q3 2024 VBSpam test – which forms part of *Virus Bulletin*'s continuously running security product test suite – we measured the performance of a number of email security solutions against various streams of wanted, unwanted and malicious emails. One third of the solutions we tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished). The solutions tested publicly were ten full email security solutions and one open-source solution.

Starting with this test, the public quarterly VBSpam tests will operate under the umbrella of the AMTSO protocol.

The supervision provided by AMTSO[1] enhances the transparency of VBSpam reports, as well as introducing more formal guarantees of fair and objective testing.

As we have iterated on previous occasions, email continues to be one of the main vectors for spreading malware and phishing attacks. As such, a dedicated email security solution is a good investment. Our tests show that such solutions can protect against the majority of existing threats – but also that there is still some work to be done.

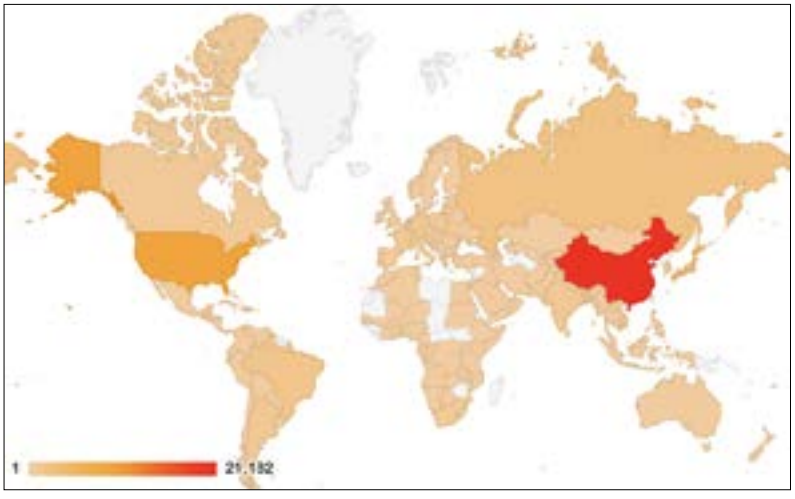
For some additional background to this report, the table and map below show the geographical distribution (based on sender IP address) of the spam emails seen in the test[2]. (*Note: these statistics are relevant only to the spam samples we received during the test period.*)

[1] https://www.amtso.org/.

[2] For 3,721 spam samples (6.28%) we couldn't find the data about geographical location based on IP address.

#	Sender's IP country	Percentage of spam
1	China	35.76%
2	United States	15.24%
3	Japan	6.16%
4	Russian Federation	3.79%
5	Brazil	2.68%
6	France	1.87%
7	India	1.81%
8	Argentina	1.71%
9	Republic of Korea	1.68%
10	Poland	1.55%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

AMTSO STANDARD COMPLIANCE

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the AMTSO website[3].

HIGHLIGHTS

Remcos malware

This was one of the malware samples that evaded detection of most of the tested solutions. It wasn't sent in bulk, and we detected it only once, on 5 August.

The malicious attachment had the following details:

Name: `"NEW ORDER SS25 DILMONI .xls"`

SHA256: `"696c5db492298e45c79d37eab78645ad3a59c855d140434d7719a60bd643b0f8"`

At the time of our analysis, through a number of redirects, opening the attachment would lead to the installation of Remcos malware:

```
xls downloader ->
hxxp[:]//tgt[.]ng/uAIHxP -> hxxp[:]//107[.]175[.]113[.]209/21/gbv/yesheisgreatthingstobeokmybabayiskinggretbaktotheentirethingstogetbackthisheisgreatthising_____sheisbeautygogirlbaby[.]doc rtf downloader 3aa674f28721c0eacaec64067ea370ad718f559e0fafae39898c7fabc6988fd4 ->
vbs downloader ->
hxxp[:]//servidorwindows[.]ddns[.]com.br/Files/ ->
Remcos
```

Non-English phishing

In recent reports we have continued to observe that many phishing threats are successfully blocked by the tested

[3] https://www.amtso.org/tests/virus-bulletin-vbspam-q3-2024/.

Email containing a malicious attachment that leads to Remcos malware.

Danish phishing sample.

German phishing sample.

security solutions. However, there are still some that slip through the net, and those that most often evade detection are phishing attempts in non-English languages.

Here we highlight two examples: one in Danish and one in German. At the time of our analysis, only the URL from the Danish phishing email was active. When users access this URL, they are redirected to the autopay[.]io website, while in the background a portable execution injection runs with the intent of stealing user credentials.

RESULTS

Of the participating full solutions, two achieved a VBSpam award: *SEPPmail.cloud Filter* and *Zoho Mail*, while eight – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *N-able Mail Assure*, *N-able SpamExperts*, *Net At Work NoSpamProxy*, *Sophos Email* and *SpamTitan* – were awarded a VBSpam+ certification.

(Note: since, for a number of products, catch rates and/or final scores were very close to, whilst remaining a fraction below, 100%, we quote all the spam-related scores with three decimal places.)

Bitdefender GravityZone Premium

SC rate: 99.985%
FP rate: 0.00%
Final score: 99.985
Malware catch rate: 99.920%
Phishing catch rate: 99.980%
Project Honey Pot SC rate: 99.991%
Abusix SC rate: 99.973%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender GravityZone Premium delivered an outstanding performance in the test, with a spam catch rate of 99.985% and no false positives. It demonstrated strong protection across all categories, achieving a 99.920% malware catch rate and a 99.980% phishing catch rate. Additionally, *Bitdefender* excelled in blocking all spam from the *Project Honey Pot* and *MXMailData* sources. With its reliable speed and zero false positives, the solution is awarded a well-deserved VBSpam+ certification.

Fortinet FortiMail

SC rate: 99.774%
FP rate: 0.00%
Final score: 99.774
Malware catch rate: 99.880%
Phishing catch rate: 99.760%
Project Honey Pot SC rate: 99.745%
Abusix SC rate: 99.837%
MXMailData SC rate: 99.650%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

FortiMail's robust performance in blocking threats without misclassifying any legitimate content earned it VBSpam+ certification with a final score of 99.774, demonstrating its all-round effectiveness as an email security solution.

Mimecast

SC rate: 99.514%
FP rate: 0.00%
Final score: 99.514
Malware catch rate: 100.000%
Phishing catch rate: 99.670%
Project Honey Pot SC rate: 99.196%
Abusix SC rate: 99.913%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Mimecast achieved a perfect 100% malware catch rate and an impressive phishing catch rate of 99.670%. With its reliable speed and zero false positives, the product earns VBSpam+ certification, continuing to demonstrate its effectiveness as a robust email security solution.

N-able Mail Assure

SC rate: 99.664%
FP rate: 0.00%
Final score: 99.664
Malware catch rate: 99.960%
Phishing catch rate: 99.910%
Project Honey Pot SC rate: 99.928%
Abusix SC rate: 99.212%
MXMailData SC rate: 99.970%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With malware and phishing catch rates higher than 99.90% and no false positives of any kind, *N-Able Mail Assure* continues to show a strong performance. A well deserved VBSpam+ certification is awarded to the product in this test.

N-able SpamExperts

SC rate: 99.664%
FP rate: 0.00%
Final score: 99.664
Malware catch rate: 99.960%
Phishing catch rate: 99.910%
Project Honey Pot SC rate: 99.928%
Abusix SC rate: 99.212%
MXMailData SC rate: 99.970%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With identical scores to its sister product, *N-Able Spam Experts* also continues to show a strong performance and also earns a well deserved VBSpam+ award.

Net At Work NoSpamProxy

SC rate: 99.963%
FP rate: 0.00%
Final score: 99.963
Malware catch rate: 99.960%
Phishing catch rate: 99.970%
Project Honey Pot SC rate: 99.960%
Abusix SC rate: 99.959%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With a 100% catch rate on the *MXMailData* corpus and only one missed malware sample, *Net At Work*'s email security solution earns VBSpam+ certification with an impressive final score of 99.963.

Rspamd

SC rate: 90.390%
FP rate: 0.77%
Final score: 86.480
Malware catch rate: 89.230%
Phishing catch rate: 93.230%
Project Honey Pot SC rate: 88.054%
Abusix SC rate: 96.404%
MXMailData SC rate: 75.770%
Newsletters FP rate: 2.8%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The open-source *Rspamd* found dealing with the malware samples a challenge. However, we continue to see good performances from the solution on the overall spam corpus, in this case blocking more than 90% of the samples.

SEPPmail.cloud Filter

SC rate: 99.969%
FP rate: 0.00%
Final score: 99.899
Malware catch rate: 100.000%
Phishing catch rate: 99.960%
Project Honey Pot SC rate: 99.945%
Abusix SC rate: 100.000%
MXMailData SC rate: 100.000%

Newsletters FP rate: 2.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SEPPmail.cloud Filter is one of only three solutions in the test that managed to successfully block all the malware samples. Despite narrowly missing out on VBSpam+ certification, a VBSpam award is well earned, with a final score placing it in the top half of the rankings.

Sophos Email

SC rate: 99.868%

FP rate: 0.00%

Final score: 99.868

Malware catch rate: 99.920%

Phishing catch rate: 100.000%

Project Honey Pot SC rate: 99.970%

Abusix SC rate: 99.791%

MXMailData SC rate: 99.410%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos Email is the only solution in this test that successfully blocked all the phishing emails. Adding to this a lack of false positives of any kind, the product earns a well deserved VBSpam+ certification.

SpamTitan

SC rate: 99.984%

FP rate: 0.00%

Final score: 99.984

Malware catch rate: 100.000%

Phishing catch rate: 99.980%

Project Honey Pot SC rate: 99.975%

Abusix SC rate: 99.995%

MXMailData SC rate: 100.000%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

No malware passed the filters of *SpamTitan* in this test. While scoring green in all the speed measurements and correctly classifying all the legitimate samples, the product is awarded VBSpam+ certification.

Zoho Mail

SC rate: 98.278%

FP rate: 0.00%

Final score: 98.278

Malware catch rate: 99.670%

Phishing catch rate: 99.460%

Project Honey Pot SC rate: 97.704%

Abusix SC rate: 98.918%

MXMailData SC rate: 99.630%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test *Zoho Mail* managed to correctly classify all the legitimate samples and blocked more than 99% of the malware and phishing emails. With a final score of 98.278 the product is awarded VBSpam certification.

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-ver30/.

The test ran for 16 days, from 12am on 3 August to 12am on 19 August 2024 (GMT).

The test corpus consisted of 60,690 emails. 59,229 of these were spam, 33,388 of which were provided by *Project Honey Pot*, 22,090 were provided by *Abusix* with the remaining 3,751 spam emails provided by *MXMailData*. There were 1,425 legitimate emails ('ham') and 36 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

27 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, 2,441 emails from the spam corpus were found to contain a malicious attachment while 13,068 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

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

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

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: Adrian Luca, Csaba Mészáros, Ionuț Răileanu
Operations Manager: Bálint Tanos
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
Bitdefender GravityZone Premium	1425	0	0.00%	9	59198.4	99.985%	99.985	
Fortinet FortiMail	1425	0	0.00%	134	59073.4	99.774%	99.774	
Mimecast	1425	0	0.00%	287.6	58919.8	99.514%	99.514	
N-able Mail Assure	1425	0	0.00%	199	59008.4	99.664%	99.664	
N-able SpamExperts	1425	0	0.00%	199	59008.4	99.664%	99.664	
Net At Work NoSpamProxy	1425	0	0.00%	22.2	59185.2	99.963%	99.963	
Rspamd	1414	11	0.77%	5690	53517.4	90.390%	86.480	
SEPPmail.cloud Filter	1425	0	0.00%	18.4	59189	99.969%	99.899	
Sophos Email	1425	0	0.00%	78.2	59129.2	99.868%	99.868	
SpamTitan	1425	0	0.00%	9.2	59198.2	99.984%	99.984	
Zoho Mail	1425	0	0.00%	1019.4	58188	98.278%	98.278	

	Newsletters		Malware		Phishing		Project Honey Pot		Abusix		MXMailData		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender GravityZone Premium	0	0.0%	2	99.920%	2	99.980%	3	99.991%	6	99.973%	0	100.000%	0.13
Fortinet FortiMail	0	0.0%	3	99.880%	31	99.760%	85	99.745%	36	99.837%	13	99.650%	0.57
Mimecast	0	0.0%	0	100.000%	43	99.670%	268.4	99.196%	19.2	99.913%	0	100.000%	0.94
N-able Mail Assure	0	0.0%	1	99.960%	12	99.910%	24	99.928%	174	99.212%	1	99.970%	2.28
N-able SpamExperts	0	0.0%	1	99.960%	12	99.910%	24	99.928%	174	99.212%	1	99.970%	2.28
Net At Work NoSpamProxy	0	0.0%	1	99.960%	4	99.970%	13.2	99.960%	9	99.959%	0	100.000%	0.2
Rspamd	1	2.8%	263	89.230%	885	93.230%	3987	88.054%	794	96.404%	909	75.770%	6.2
SEPPmail. cloud Filter	1	2.8%	0	100.000%	5	99.960%	18.4	99.945%	0	100.000%	0	100.000%	0.25
Sophos Email	0	0.0%	2	99.920%	0	100.000%	10	99.970%	46.2	99.791%	22	99.410%	1.16
SpamTitan	0	0.0%	0	100.000%	2	99.980%	8.2	99.975%	1	99.995%	0	100.000%	0.18
Zoho Mail	0	0.0%	8	99.670%	70	99.460%	766.4	97.704%	239	98.918%	14	99.630%	2.41

† *The standard deviation of a product is calculated using the set of its hourly spam catch rates.*

	Speed			
	10%	**50%**	**95%**	**98%**
Bitdefender GravityZone Premium	🟢	🟢	🟢	🟢
Fortinet FortiMail	🟢	🟢	🟢	🟢
Mimecast	🟢	🟢	🟢	🟢
N-able Mail Assure	🟢	🟢	🟢	🟢
N-able SpamExperts	🟢	🟢	🟢	🟢
Net At Work NoSpamProxy	🟢	🟢	🟢	🟢
Rspamd	🟢	🟢	🟢	🟢
SEPPmail.cloud Filter	🟢	🟢	🟢	🟢
Sophos Email	🟢	🟢	🟡	🟡
SpamTitan	🟢	🟢	🟢	🟢
Zoho Mail	🟢	🟢	🟢	🟢

🟢 *0–30 seconds;* 🟡 *30 seconds to two minutes;* 🟠 *two minutes to 10 minutes;* 🔴 *more than 10 minutes.*

Products ranked by final score	
Bitdefender GravityZone Premium	99.985
SpamTitan	99.984
Net At Work NoSpamProxy	99.963
SEPPmail.cloud Filter	99.899
Sophos Email	99.868
Fortinet FortiMail	99.774
N-able Mail Assure	99.664
N-able SpamExperts	99.664
Mimecast	99.514
Zoho Mail	98.278
Rspamd	86.480

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
Net At Work NoSpamProxy	32Guards & NoSpamProxy		√	√	√	√	√
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Sophos Email	Sophos	√	√	√	√	√	√
SpamTitan	SpamTitan	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Bitdefender GravityZone Premium	Bitdefender	√				√		√	√
Fortinet FortiMail	Fortinet	√	√	√	√	√		√	√
Rspamd	None					√