MARCH 2024

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2024

Ionuţ Răileanu & Adrian Luca

In the Q1 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tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished).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 nine full email security solutions, one custom configured solution[1] and one open-source solution.

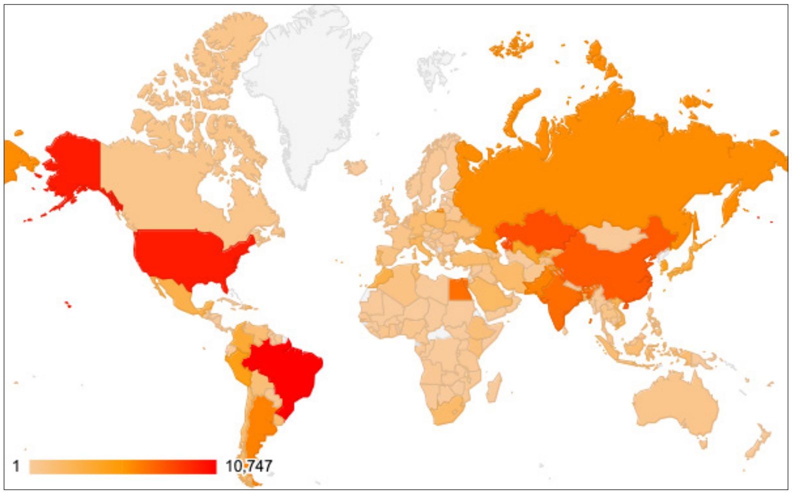
For quite some time now, the solutions we test have been able to block most of the spam samples they are presented with in the test. In fact, their spam catch rates have improved so much, and a number of products are so close to catching 100% of the samples, that we now quote all the spam-related scores with three decimal places. It seems that the email security solutions have it more or less figured out when it comes to blocking the spam.

However, as always the devil is in the details and the few samples missed by the products show that there is still some work to do. We highlight in this report the most commonly missed phishing and malware samples, the majority of which consist of non-English emails that form part of short and effective 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 during the test period.)*

#	Sender's IP country	Percentage of spam
1	Brazil	6.36%
2	United States	5.80%
3	Kazakhstan	4.75%
4	China	4.48%
5	India	4.09%
6	Egypt	4.06%
7	Pakistan	3.67%
8	Argentina	3.65%
9	Russian Federation	3.44%
10	Peru	2.74%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

[1] *Spamhaus Data Query Service* (*DQS*) + *SpamAssassin* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

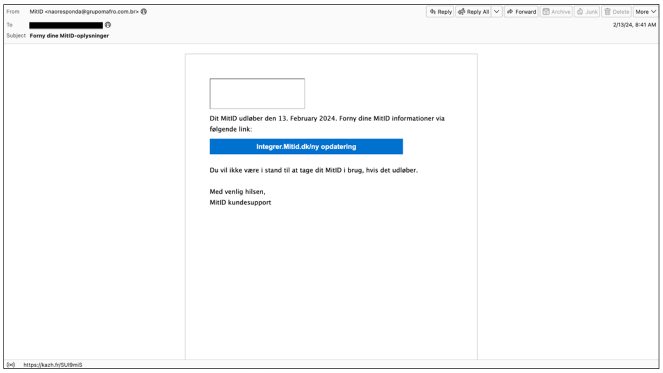
ISSN 1749-7027

HIGHLIGHTS

Non-English phishing emails

While it may seem repetitive to highlight, we continue to note that most of the phishing emails that evade the security solutions' filters are written in any language but English. These samples appear very rarely among the spam corpus, this fact contributing to the challenge of blocking them in a short period of time.

The following screenshots show some of these phishing emails in Danish, Dutch, Hebrew and Italian.



From MitID <naoresponda@grupomafro.com.br>
To [redacted]
Subject Forny dine MitID-oplysninger
2/13/24, 8:41 AM

Dit MitID udløber den 13. February 2024. Forny dine MitID informationer via følgende link:

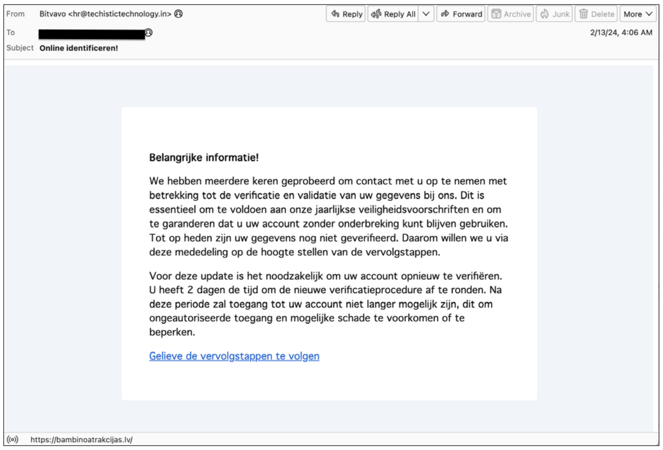
Integrer.Mitid.dk/ny opdatering

Du vil ikke være i stand til at tage dit MitID i brug, hvis det udløber.

Med venlig hilsen,
MitID kundesupport

https://kazh.fr/SUI9miS

Danish phishing sample.



From Bitvavo <hr@techistictechnology.in>
To [redacted]
Subject Online identificeren!
2/13/24, 4:06 AM

Belangrijke informatie!

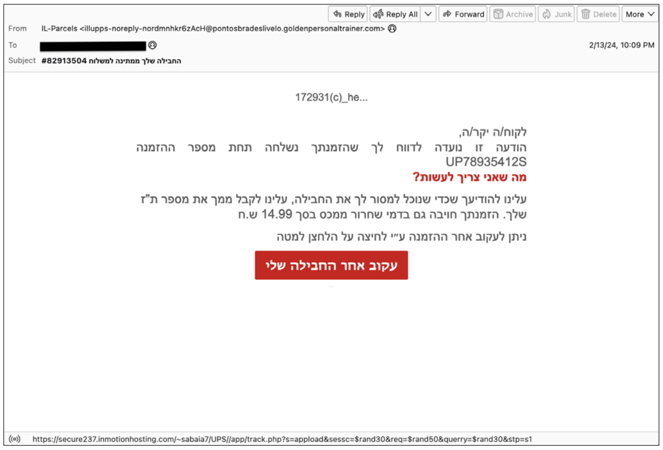
We hebben meerdere keren geprobeerd om contact met u op te nemen met betrekking tot de verificatie en validatie van uw gegevens bij ons. Dit is essentieel om te voldoen aan onze jaarlijkse veiligheidsvoorschriften en om te garanderen dat u uw account zonder onderbreking kunt blijven gebruiken. Tot op heden zijn uw gegevens nog niet geverifieerd. Daarom willen we u via deze mededeling op de hoogte stellen van de vervolgstappen.

Voor deze update is het noodzakelijk om uw account opnieuw te verifiëren. U heeft 2 dagen de tijd om de nieuwe verificatieprocedure af te ronden. Na deze periode zal toegang tot uw account niet langer mogelijk zijn, dit om ongeautoriseerde toegang en mogelijke schade te voorkomen of te beperken.

Gelieve de vervolgstappen te volgen

https://bambinoatrakcijas.lv/

Dutch phishing sample.



From IL-Parcels <illupps-noreply-nordmnhkr6zAcH@pontosbradeslivelo.goldenpersonaltrainer.com>
To [redacted]
Subject #82913504 החבילה שלך ממתינה למשלוח
2/13/24, 10:09 PM

172931(c)_he...

לקוח/ה יקר/ה,
הודעה זו נועדה לדווח לך שהזמנתך נשלחה תחת מספר ההזמנה
UP78935412S
מה שאני צריך לעשות?

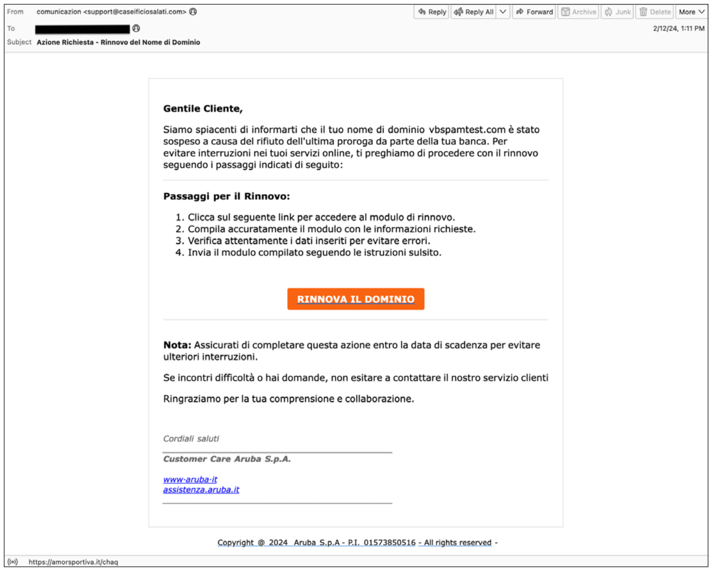
עלינו להודיעך שכדי שנוכל למסור לך את החבילה, עלינו לקבל ממך את מספר ת"ז
שלך. הזמנתך חויבה גם בדמי שחרור ממכס בסך 14.99 ש.ח

ניתן לעקוב אחר ההזמנה ע״י לחיצה על הלחצן למטה

עקוב אחר החבילה שלי

https://secure237.inmotionhosting.com/~sabaia7/UPS//app/track.php?s=appload&sessc=$rand30&req=$rand50&querry=$rand30&stp=s1

Hebrew phishing sample.



From comunicazion <support@caseificiosalati.com>

To [redacted]

2/12/24, 1:11 PM

Subject **Azione Richiesta - Rinnovo del Nome di Dominio**

Gentile Cliente,

Siamo spiacenti di informarti che il tuo nome di dominio vbspamtest.com è stato sospeso a causa del rifiuto dell'ultima proroga da parte della tua banca. Per evitare interruzioni nei tuoi servizi online, ti preghiamo di procedere con il rinnovo seguendo i passaggi indicati di seguito:

Passaggi per il Rinnovo:

1. Clicca sul seguente link per accedere al modulo di rinnovo.
2. Compila accuratamente il modulo con le informazioni richieste.
3. Verifica attentamente i dati inseriti per evitare errori.
4. Invia il modulo compilato seguendo le istruzioni sulsito.

Nota: Assicurati di completare questa azione entro la data di scadenza per evitare ulteriori interruzioni.

Se incontri difficoltà o hai domande, non esitare a contattare il nostro servizio clienti

Ringraziamo per la tua comprensione e collaborazione.

Cordiali saluti

Customer Care Aruba S.p.A.

www·aruba·it
assistenza.aruba.it

Copyright @ 2024 Aruba S.p.A - P.I. 01573850516 - All rights reserved -

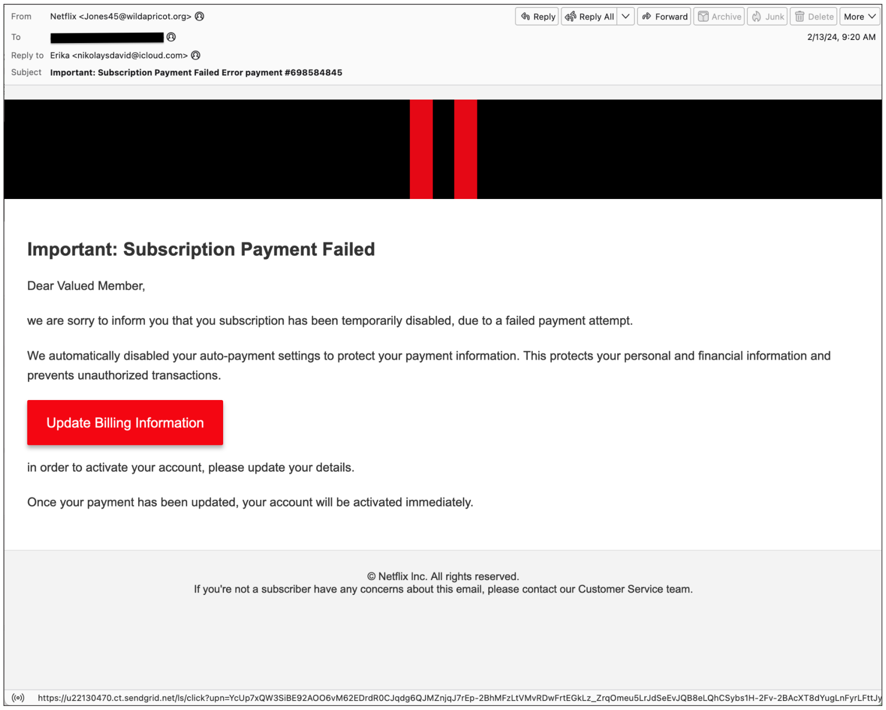
https://amorsportiva.it/chaq

Italian phishing sample.

English phishing sample

Despite the majority of English phishing samples being blocked by most of the VBSpam test participants, there are still some samples that pass through. When this happens it's usually because the attacker is using a legitimate service to send the email.

In this case we see a *Netflix* look-a-like email with a *Sendgrid* URL and an *iCloud* email address in the 'Reply-To' header.



From Netflix <Jones45@wildapricot.org>

To [redacted]

2/13/24, 9:20 AM

Reply to Erika <nikolaysdavid@icloud.com>

Subject **Important: Subscription Payment Failed Error payment #698584845**

Important: Subscription Payment Failed

Dear Valued Member,

we are sorry to inform you that you subscription has been temporarily disabled, due to a failed payment attempt.

We automatically disabled your auto-payment settings to protect your payment information. This protects your personal and financial information and prevents unauthorized transactions.

in order to activate your account, please update your details.

Once your payment has been updated, your account will be activated immediately.

© Netflix Inc. All rights reserved.
If you're not a subscriber have any concerns about this email, please contact our Customer Service team.

https://u22130470.ct.sendgrid.net/ls/click?upn=YcUp7xQW3SiBE92AOO6vM62EDrdR0CJqdg6QJMZnjqJ7rEp-2BhMFzLtVMvRDwFrtEGkLz_ZrqOmeu5LrJdSeEvJQB8eLQhCSybs1H-2Fv-2BAcXT8dYugLnFyrLFttJy

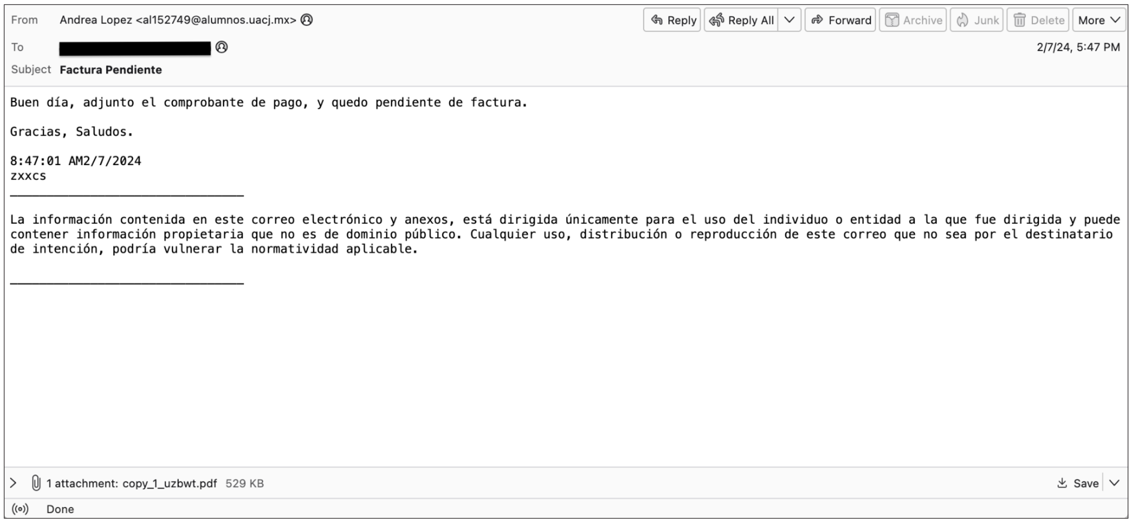
English phishing sample.

Malicious PDF

The most commonly missed malware sample contained a PDF attachment (`SHA 256: fcae77a2d05cf3327e9eb5bf397f2c98553675977afd2fb4c1e0bd018cffe4fe`) with a *Dropbox* URL that is reported[2] to download a malicious JavaScript file (`SHA 256: 2c94db3db031544534f93a25ba1e8fcfe986bf482f1757219ad42b4a03de75b3`).

XWorm malware

On 9 and 12 February we noticed two malware campaigns lasting for about an hour each time, with the subject '`Please confirm receipt`' and a zip attachment. The

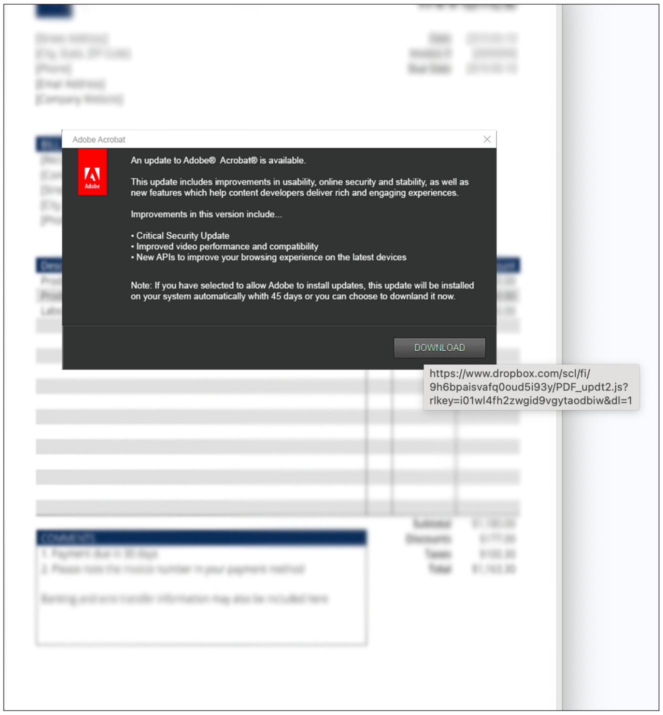


From Andrea Lopez <al152749@alumnos.uacj.mx>
To [redacted]
2/7/24, 5:47 PM
Subject **Factura Pendiente**

```
Buen día, adjunto el comprobante de pago, y quedo pendiente de factura.

Gracias, Saludos.

8:47:01 AM2/7/2024
zxxcs
________________________________

La información contenida en este correo electrónico y anexos, está dirigida únicamente para el uso del individuo o entidad a la que fue dirigida y puede
contener información propietaria que no es de dominio público. Cualquier uso, distribución o reproducción de este correo que no sea por el destinatario
de intención, podría vulnerar la normatividad aplicable.

________________________________
```

1 attachment: copy_1_uzbwt.pdf 529 KB

Email with a malicious PDF attachment.



An update to Adobe® Acrobat® is available.

This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

Improvements in this version include...

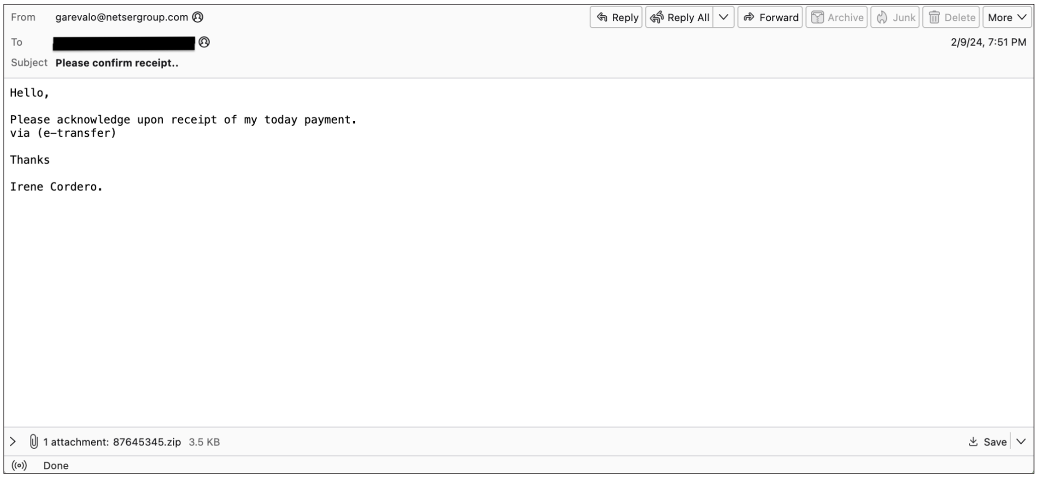
- Critical Security Update
- Improved video performance and compatibility
- New APIs to improve your browsing experience on the latest devices

Note: If you have selected to allow Adobe to install updates, this update will be installed on your system automatically whith 45 days or you can choose to downland it now.

https://www.dropbox.com/scl/fi/9h6bpaisvafq0oud5i93y/PDF_updt2.js?rlkey=i01wl4fh2zwgid9vgytaodbiw&dl=1

The PDF attachment.

[2] https://bazaar.abuse.ch/sample/fcae77a2d05cf3327e9eb5bf397f2c98553675977afd2fb4c1e0bd018cffe4fe/#intel



From garevalo@netsergroup.com
To [redacted]
Subject **Please confirm receipt..**
2/9/24, 7:51 PM

```
Hello,

Please acknowledge upon receipt of my today payment.
via (e-transfer)

Thanks

Irene Cordero.
```

1 attachment: 87645345.zip 3.5 KB

Done

Email sample that leads to XWorm malware.

zip[3] contained a vbs file (`SHA 256: 52a46b6e7500738156e1fd34a3327242db857b876a3dfbf54610e0a10d3406ed`) which, via PowerShell, downloaded and executed the XWorm payload.

We mention this campaign because it managed to bypass the filters of many of the participants.

RESULTS

The majority of the tested solutions managed to achieve high catch rates both on overall spam samples and on the malware sub-category, with values higher than 99%. In particular, we highlight the performance of *SEPPmail.cloud Filter*, which didn't miss any malware or phishing samples.

Of the participating full solutions, one achieved a VBSpam award – *SEPPmail.cloud Filter* – while eight – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *N-able Mail Assure*, *N-Able SpamExperts*, *Net At Work NoSpamProxy*, *SpamTitan* and *Zoho Mail* – were awarded a VBSpam+ certification, as was the custom configured solution *Spamhaus DQS*.

Bitdefender GravityZone Premium

vb March 2024 VERIFIED SPAM + virusbtn.com

SC rate: 99.988%

FP rate: 0.00%

Final score: 99.988

Malware catch rate: 100.000%

Phishing catch rate: 99.951%

Project Honey Pot SC rate: 100.000%

Abusix SC rate: 99.989%

MXMailData SC rate: 99.936%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Besides a well earned VBSpam+ award, we highlight the excellent performance of *Bitdefender*'s product in this test with no false negatives on the malware corpus and no false positives of any kind.

Fortinet FortiMail

vb March 2024 VERIFIED SPAM + virusbtn.com

SC rate: 99.994%

FP rate: 0.00%

Final score: 99.994

Malware catch rate: 100.000%

Phishing catch rate: 99.963%

Project Honey Pot SC rate: 99.928%

Abusix SC rate: 99.997%

MXMailData SC rate: 100.000%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet shows another a great performance in the test with the highest spam catch rate and no false positives. No malware sample bypassed the product's filters and another VBSpam+ award is added to its track record.

Mimecast

SC rate: 99.956%

FP rate: 0.00%

Final score: 99.956

[3] https://bazaar.abuse.ch/sample/52a46b6e7500738156e1fd34a3327242db857b876a3dfbf54610e0a10d3406ed/

Malware catch rate: 100.000%

Phishing catch rate: 99.988%

Project Honey Pot SC rate: 99.334%

Abusix SC rate: 99.988%

MXMailData SC rate: 100.000%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Mimecast achieved a perfect score on the malware corpus, and just one missed sample prevented it from scoring a 100% catch rate on the phishing corpus as well. With no false positives the product starts the 2024 VBSpam testing series with a VBSpam+ award.

N-able Mail Assure

SC rate: 99.925%

FP rate: 0.00%

Final score: 99.885

Malware catch rate: 98.695%

Phishing catch rate: 99.506%

Project Honey Pot SC rate: 99.625%

Abusix SC rate: 99.959%

MXMailData SC rate: 99.002%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

N-able Mail Assure continued its run of good performances in this test, earning another VBSpam+ award. In particular we highlight the lack of ham false positives and the higher than 99% phishing catch rate.

N-able SpamExperts

SC rate: 99.921%

FP rate: 0.00%

Final score: 99.881

Malware catch rate: 98.695%

Phishing catch rate: 99.506%

Project Honey Pot SC rate: 99.601%

Abusix SC rate: 99.956%

MXMailData SC rate: 99.002%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With almost identical scores to its sister product, *N-able SpamExperts* also easily earns VBSpam+ certification in this test.

Net At Work NoSpamProxy

SC rate: 99.986%

FP rate: 0.00%

Final score: 99.946

Malware catch rate: 99.959%

Phishing catch rate: 99.963%

Project Honey Pot SC rate: 99.988%

Abusix SC rate: 99.986%

MXMailData SC rate: 99.968%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Net At Work's email security solution continues to show a balanced performance. It achieved higher than 99.95% catch rates on both the malware corpus and the phishing corpus. With no ham false positives and an overall spam catch rate exceeding 99.95%, it earns VBSpam+ certification.

Rspamd

SC rate: 97.066%

FP rate: 0.24%

Final score: 95.874

Malware catch rate: 55.506%

Phishing catch rate: 79.825%

Project Honey Pot SC rate: 87.733%

Abusix SC rate: 98.329%

MXMailData SC rate: 58.229%

Newsletters FP rate: 0.0%

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 97% of the samples.

SEPPmail.cloud Filter

SC rate: 99.994%

FP rate: 0.04%

Final score: 99.755

Malware catch rate: 100.000%

Phishing catch rate: 100.000%

Project Honey Pot SC rate: 99.878%

Abusix SC rate: 100.000%

MXMailData SC rate: 100.000%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The Switzerland-based *SEPPmail.cloud Filter* scored the highest spam catch rate in this test and was the only solution to have blocked all of the malware and phishing samples. A relatively high false positive rate prevented the solution from achieving a VBSpam+ award, but VBSpam certification is easily earned with this impressive performance.

Spamhaus Data Query Service

SC rate: 99.763%

FP rate: 0.00%

Final score: 99.723

Malware catch rate: 98.328%

Phishing catch rate: 99.481%

Project Honey Pot SC rate: 99.916%

Abusix SC rate: 99.839%

MXMailData SC rate: 95.491%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus SpamAssassin Data Query Service (*DQS*) is a custom configured solution that integrates the *Spamhaus DQS* DNSBL service and the free open-source solution *SpamAssassin*. In this test no ham samples were blocked by this combined solution. With a final score of 99.723 the solution earns a VBSpam+ certification.

SpamTitan

SC rate: 99.983%

FP rate: 0.00%

Final score: 99.983

Malware catch rate: 99.511%

Phishing catch rate: 99.914%

Project Honey Pot SC rate: 100.000%

Abusix SC rate: 99.987%

MXMailData SC rate: 99.710%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamTitan joins the VBSpam test with an excellent performance, ranking in the top three based on final score. With a spam catch rate exceeding 99.95% and no ham false positives, it is awarded VBSpam+ certification.

Zoho Mail

SC rate: 99.535%

FP rate: 0.00%

Final score: 99.495

Malware catch rate: 99.551%

Phishing catch rate: 99.753%

Project Honey Pot SC rate: 98.145%

Abusix SC rate: 99.616%

MXMailData SC rate: 99.163%

Newsletters FP rate: 1.8%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail achieved higher than 99% catch rates not only on malware and phishing samples but also on the overall spam corpus, while correctly classifying all the ham samples. For this excellent performance the product earns 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-ver20.

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

The test corpus consisted of 171,511 emails. 168,951 of these were spam, 8,396 of which were provided by *Project Honey Pot*, 157,450 were provided by *Abusix*, with the remaining 3,105 spam emails provided by *MXMailData*. There were 2,505 legitimate emails ('ham') and 55 newsletters – a category that includes various kinds of commercial and non-commercial opt-in mailings.

37 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, 2,452 emails from the spam corpus were found to contain a malicious attachment while 8,094 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].

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

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

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

Head of Testing: Peter Karsai
Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu
Operations Manager: Bálint Tanos
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin

© 2024 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/

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.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender GravityZone Premium	2505	0	0.00%	20	168901.4	99.988%	99.988	SPAM+ Verified
FortiMail	2505	0	0.00%	10	168911.4	99.994%	99.994	SPAM+ Verified
Mimecast	2505	0	0.00%	75	168846.4	99.956%	99.956	SPAM+ Verified
N-able Mail Assure	2505	0	0.00%	127.4	168794	99.925%	99.885	SPAM+ Verified
N-able SpamExperts	2505	0	0.00%	133.4	168788	99.921%	99.881	SPAM+ Verified
Net At Work NoSpamProxy	2505	0	0.00%	24.2	168897.2	99.986%	99.946	SPAM+ Verified
Rspamd	2499	6	0.24%	4956	163965.4	97.066%	95.874	
SEPPmail.cloud Filter	2504	1	0.04%	10.2	168911.2	99.994%	99.755	SPAM Verified
Spamhaus DQS + SpamAssassin‡	2505	0	0.00%	400	168521.4	99.763%	99.723	SPAM+ Verified
SpamTitan	2505	0	0.00%	29.4	168892	99.983%	99.983	SPAM+ Verified
Zoho Mail	2505	0	0.00%	785.8	168135.6	99.535%	99.495	SPAM+ Verified

‡Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssasssin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

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

	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%	0	100.000%	4	99.951%	0	100.000%	18	99.989%	2	99.936%	0.16
FortiMail	0	0.0%	0	100.000%	3	99.963%	6	99.928%	4	99.997%	0	100.000%	0.24
Mimecast	0	0.0%	0	100.000%	1	99.988%	55.8	99.334%	19.2	99.988%	0	100.000%	0.77
N-able Mail Assure	1	1.8%	32	98.695%	40	99.506%	31.4	99.625%	65	99.959%	31	99.002%	1.02
N-able SpamExperts	1	1.8%	32	98.695%	40	99.506%	33.4	99.601%	69	99.956%	31	99.002%	1.11
Net At Work NoSpamProxy	1	1.8%	1	99.959%	3	99.963%	1	99.988%	22.2	99.986%	1	99.968%	0.27
Rspamd	0	0.0%	1091	55.506%	1633	79.825%	1027.6	87.733%	2631.4	98.329%	1297	58.229%	8.94
SEPPmail.cloud Filter	1	1.8%	0	100.000%	0	100.000%	10.2	99.878%	0	100.000%	0	100.000%	0.45
Spamhaus DQS + SpamAssassin[‡]	1	1.8%	41	98.328%	42	99.481%	7	99.916%	253	99.839%	140	95.491%	1.33
SpamTitan	0	0.0%	12	99.511%	7	99.914%	0	100.000%	20.4	99.987%	9	99.710%	0.22
Zoho Mail	1	1.8%	11	99.551%	20	99.753%	155.4	98.145%	604.4	99.616%	26	99.163%	3.72

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

[‡] *Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssasssin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.*

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

	Speed			
	10%	50%	95%	98%
Bitdefender GravityZone Premium	🟢	🟢	🟢	🟢
FortiMail	🟢	🟢	🟢	🟢
Mimecast	🟢	🟢	🟢	🟢
N-able Mail Assure	🟢	🟢	🟢	🟢
N-able SpamExperts	🟢	🟢	🟢	🟢
Net At Work NoSpamProxy	🟢	🟢	🟢	🟢
Rspamd	🟢	🟢	🟢	🟢
SEPPmail.cloud Filter	🟢	🟢	🟢	🟢
Spamhaus DQS + SpamAssassin[‡]	🟢	🟢	🟢	🟢
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	
FortiMail	99.994
Bitdefender GravityZone Premium	99.988
SpamTitan	99.983
Mimecast	99.956
Net At Work NoSpamProxy	99.946
N-able Mail Assure	99.885
N-able SpamExperts	99.881
SEPPmail.cloud Filter	99.755
Spamhaus DQS + SpamAssassin[‡]	99.723
Zoho Mail	99.495
Rspamd	95.874

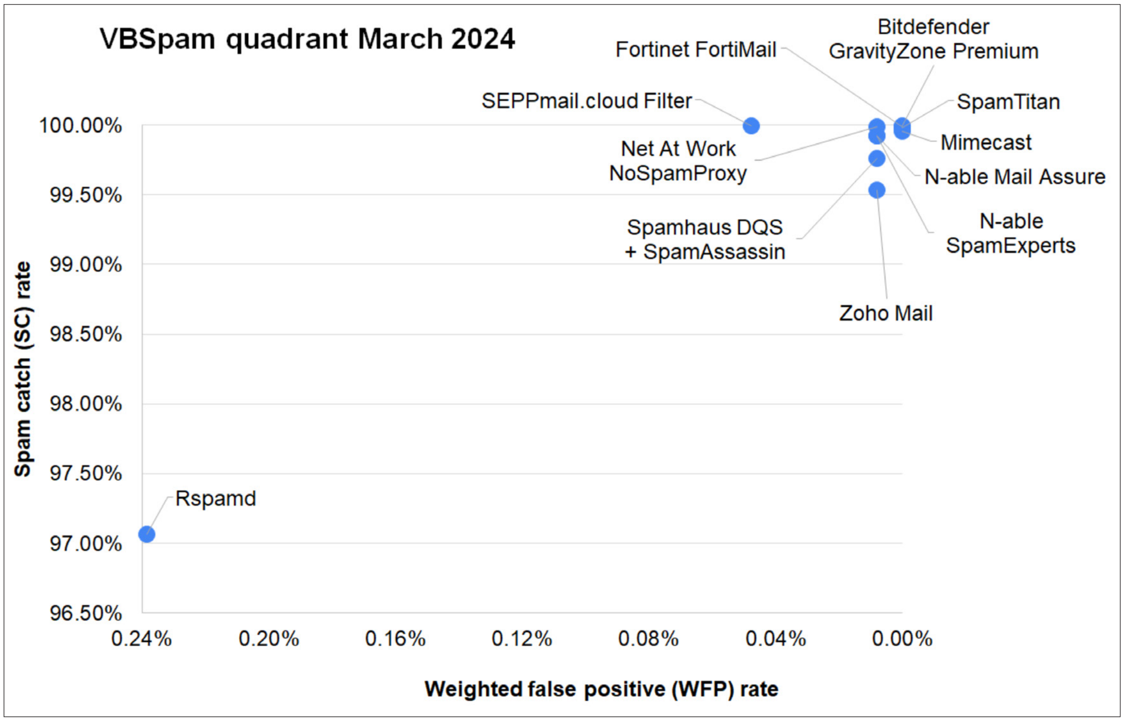
[‡] *Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssasssin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.*

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

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	√	√	√	√	√	√
SpamTitan	SpamTitan	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Bitdefender GravityZone Premium	Bitdefender	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
Rspamd	None					√			
Spamhaus DQS + SpamAssassin[‡]	Optional	√	√	√					√

[‡] Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssasssin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.



Please refer to the text for full product names.)