DECEMBER 2016

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW DECEMBER 2016

Martijn Grooten & Ionuţ Răileanu

Over the years, cybercriminals have perfected the way they spread malware through email. They craft their emails to look like messages that people are likely to receive in everyday life, such as receipts or delivery notifications, and use attachments in file formats that people are used to receiving – quite often *Word* or *Excel* files in which the malware-downloading component requires activation by a gullible user. (It has long been known that end-users are the weakest link in just about every system.)

There are many things that individuals and organizations can reasonably be expected to do to make malware infections less likely, but blocking all *Office* documents attached to emails is not one of them. And thus there is no way to *a priori* block these emails and their malicious payload.

But how bad are things, really? After all, while there are millions of emails like this being sent every day, almost every mailbox is protected by an email security solution, or spam filter.

In this report, we share some good news: spam filters block the overwhelming majority of these malware-containing emails, at a rate even higher than that at which they block ‘ordinary’ spam. And while one should never be complacent about threats, this does explain why, despite all the dangers out there, for most people the Internet in general, and email in particular, continues to work.

We make these statements based on the performance of 16 full email security (or anti-spam) solutions, from both large and small vendors (and one open-source provider), in the 46th comparative VBSpam test. All of the products in the test reached the benchmark required for VBSpam certification, and six of them performed well enough to earn the VBSpam+ accolade. We also tested five DNS-based blocklists, as well as two combined lists.

To make this report more readable, we have moved the technical information about the test, as well as the methodology, to an appendix. Regular readers of these reports will also have noticed that they are now published quarterly.

SPAM WITH AND WITHOUT MALWARE

The conclusion drawn from this test remains the same as that drawn from a dozen previous tests: most spam is blocked. In fact, of the more than 117,000 spam emails used in this test, 97.7% were blocked by all full email security solutions, with most of the remaining spam emails missed by just one or two products. Only 18 emails (less than 0.02%) were missed by more than half of the full solutions.

Unsurprisingly, the most difficult to block spam emails are the ones that verge on the legal: legitimate companies using illegitimate means and sloppy sender practices to get their message seen. However, the three ‘winners’ – from the spammers’ point of view – in this test were actual scams: two emails that urged the recipient to contact the sender, and a third that contained what appeared to be a phishing link, but was inactive by the time we accessed it.

Much as scams are bad, and can be costly for the victim, far worse are emails that have malware attached. Among the spam emails in this test, we found 8,477 that contained malicious attachments. Following requests from both participating vendors and readers, we decided to report the performance of products on this corpus as a separate metric.

Malware was seen in spam throughout the duration of the test, but we identified a few dozen individual campaigns. Most of the attachments were either zip files with the payload hidden inside or *Word* documents where the payload would be downloaded through the execution of macros; one campaign used RAR archives as attachments.

It is beyond the scope of this report to analyse the attachments, but it is rare for them to contain the final payload; rather, attachments are downloaders that have the

ISSN 1749-7027

sole purpose of downloading the payload onto the victim's machine. The payload that is eventually downloaded may depend on a number of parameters, such as the victim's location, but it is fair to say that many of the people who opened the attachments we saw would have become infected with ransomware, most likely Locky.

The story of ransomware and how much damage it does has been told often enough, but we have more good news to report: in this test, all but one of the participating full solutions blocked at least 199 out of every 200 emails that contained a malicious attachment, with nine out of 16 products blocking all of them.

Moreover, none of these emails were missed by more than two products, and no campaign stood out as being significantly difficult to block, thus showing that cybercriminals haven't found a secret way past the spam filter.

Still, while this is certainly good news, there is an important caveat: we looked at the ability of products to block these emails *as spam*. What we showed was that, on average, more than 99.8% of these emails would not end up in users' *inboxes*.

But email that doesn't make it to the inbox is often still accessible to users. Given the cost of false positives, this is a feature of spam filters rather than a bug, but it does mean that there is still the possibility of a user being infected, even if the spam filter blocked the email. This is why many spam filters tread extra carefully when it comes to malicious attachments: they remove the attachments from the emails, or block access to the emails altogether. In this test, we did not assess products' ability to detect the malware.

It is possible that many malicious spam emails were only recognized as spam. After all, the two IP-blacklists we tested stopped the overwhelming majority of them, despite not having access to the attachments. In future tests, we aim to look at products' ability to detect malicious attachments as such.

RESULTS

In this test, *OnlyMyEmail* stood out for missing just three spam emails in the spam corpus, while *ESET*, *Bitdefender* and *Fortinet* all blocked at least 99.98% of spam as well. These four products did not block any legitimate emails either, earning them VBSpam+ awards, along with *Libra Esva* and *Vade Retro MailCube*. 'Clean sheets' – where the product didn't block any legitimate emails or any emails from the newsletter feed – were achieved by *ESET* and *Libra Esva*.

New in this test is a domain-blacklist that is part of *IBM*'s *X-Force* suite. We found the product to block well over half of the spam emails in our test set, purely by looking at the domains visible inside them. We also included in the test a combination of both *IBM X-Force* lists.

Axway MailGate 5.5.1

vb VERIFIED SPAM virusbtn.com

SC rate: 99.71%
FP rate: 0.04%
Final score: 99.43
Project Honey Pot SC rate: 99.72%
Abusix SC rate: 99.44%
Newsletters FP rate: 2.6%
Malware SC rate: 99.72%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6

vb VERIFIED SPAM + virusbtn.com

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.3%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Egedian Mail Security

vb VERIFIED SPAM virusbtn.com

SC rate: 99.19%
FP rate: 0.00%
Final score: 99.16
Project Honey Pot SC rate: 99.18%
Abusix SC rate: 99.38%
Newsletters FP rate: 0.6%
Malware SC rate: 98.86%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

vb VERIFIED SPAM + virusbtn.com

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

vb VERIFIED SPAM + virusbtn.com

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.94
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.79%
Newsletters FP rate: 1.2%
Malware SC rate: 99.96%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

GFI MailEssentials

vb VERIFIED SPAM virusbtn.com

SC rate: 99.59%
FP rate: 0.05%
Final score: 99.18
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 98.50%
Newsletters FP rate: 4.3%
Malware SC rate: 99.93%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟡; 98%: 🟡

IBM Lotus Protector for Mail Security

vb VERIFIED SPAM virusbtn.com

SC rate: 99.95%
FP rate: 0.01%
Final score: 99.88
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.3%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Kaspersky Linux Mail Security 8.0

vb VERIFIED SPAM virusbtn.com

SC rate: 99.74%
FP rate: 0.04%
Final score: 99.56
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.40%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Kaspersky Secure Mail Gateway

vb VERIFIED SPAM virusbtn.com

SC rate: 99.72%
FP rate: 0.04%
Final score: 99.54
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.36%
Newsletters FP rate: 0.0%
Malware SC rate: 99.99%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Libra Esva 3.7.0.1

vb VERIFIED SPAM + virusbtn.com

SC rate: 99.89%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.74%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

OnlyMyEmail's Corporate MX-Defender

vb VERIFIED SPAM + virusbtn.com

SC rate: 99.997%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.98%
Newsletters FP rate: 2.3%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟡

Scrollout F1

vb VERIFIED SPAM virusbtn.com

SC rate: 99.80%
FP rate: 0.07%
Final score: 99.36
Project Honey Pot SC rate: 99.82%
Abusix SC rate: 99.47%
Newsletters FP rate: 2.3%
Malware SC rate: 99.69%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

Sophos Email Appliance

SC rate: 99.49%
FP rate: 0.05%
Final score: 99.25
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.44%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb VERIFIED SPAM virusbtn.com

SpamTitan 6.00

SC rate: 99.80%
FP rate: 0.01%
Final score: 99.75
Project Honey Pot SC rate: 99.80%
Abusix SC rate: 99.83%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟡; 98%: 🟡

vb VERIFIED SPAM virusbtn.com

Vade Retro MailCube

SC rate: 99.55%
FP rate: 0.00%
Final score: 99.50
Project Honey Pot SC rate: 99.52%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.2%
Malware SC rate: 99.55%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb VERIFIED SPAM + virusbtn.com

ZEROSPAM

SC rate: 99.87%
FP rate: 0.09%
Final score: 99.33
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 100.00%
Newsletters FP rate: 2.0%
Malware SC rate: 100.00%
Speed: 10%: 🟢; 50%: 🟢; 95%: 🟢; 98%: 🟢

vb VERIFIED SPAM virusbtn.com

IBM X-Force API

SC rate: 94.29%
FP rate: 0.00%
Final score: 94.29
Project Honey Pot SC rate: 94.52%
Abusix SC rate: 89.47%
Newsletters FP rate: 0.0%
Malware SC rate: 96.90%

IBM X-Force API - combined

SC rate: 96.78%
FP rate: 0.01%
Final score: 96.72
Project Honey Pot SC rate: 97.10%
Abusix SC rate: 90.12%
Newsletters FP rate: 0.0%
Malware SC rate: 96.90%

IBM X-Force API - URLs

SC rate: 53.65%
FP rate: 0.01%
Final score: 53.59
Project Honey Pot SC rate: 55.95%
Abusix SC rate: 5.15%
Newsletters FP rate: 0.0%
Malware SC rate: 0.02%

Spamhaus DBL

SC rate: 15.80%
FP rate: 0.00%
Final score: 15.80
Project Honey Pot SC rate: 16.47%
Abusix SC rate: 1.71%
Newsletters FP rate: 0.0%
Malware SC rate: 0.46%

Spamhaus ZEN

SC rate: 93.60%
FP rate: 0.00%
Final score: 93.60
Project Honey Pot SC rate: 93.43%
Abusix SC rate: 97.22%
Newsletters FP rate: 0.0%
Malware SC rate: 98.87%

Spamhaus ZEN+DBL

SC rate: 95.22%
FP rate: 0.00%
Final score: 95.22
Project Honey Pot SC rate: 95.12%
Abusix SC rate: 97.29%
Newsletters FP rate: 0.0%
Malware SC rate: 98.88%

URIBL (MX Tools)

SC rate: 43.52%
FP rate: 0.50%
Final score: 40.21
Project Honey Pot SC rate: 45.26%
Abusix SC rate: 6.92%
Newsletters FP rate: 24.8%
Malware SC rate: 0.52%

CONCLUSION

After a decline at the beginning of the decade, malicious spam has once again become a very big problem and one that deserves special attention in a report like this one.

The next test report – to be published in March 2017 – will continue to look at this aspect of spam. Those interested in submitting a product should contact martijn.grooten@virusbulletin.com.

APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

The full VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/.

The test ran for 19 days, from 12am on 19 November to 12am on 7 December 2016. The test period was extended by three days, following unexpected maintenance performed by our Internet provider, which caused some downtime on 24 and 25 November.

The test corpus consisted of 126,167 emails. 117,303 of these were spam, 111,987 of which were provided by *Project Honey Pot*, with the remaining 5,316 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 8,517 legitimate emails (‘ham’) and 347 newsletters.

Moreover, 8,477 emails from the spam corpus were found to contain malicious attachments; though we report separate performance metrics on this corpus, it should be noted that these are also part of the full 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[1]. Consequently, products were able to filter email in an environment that very closely resembled one in which they would be deployed in the real world.

Those products running in our lab were all run 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)

> **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.

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

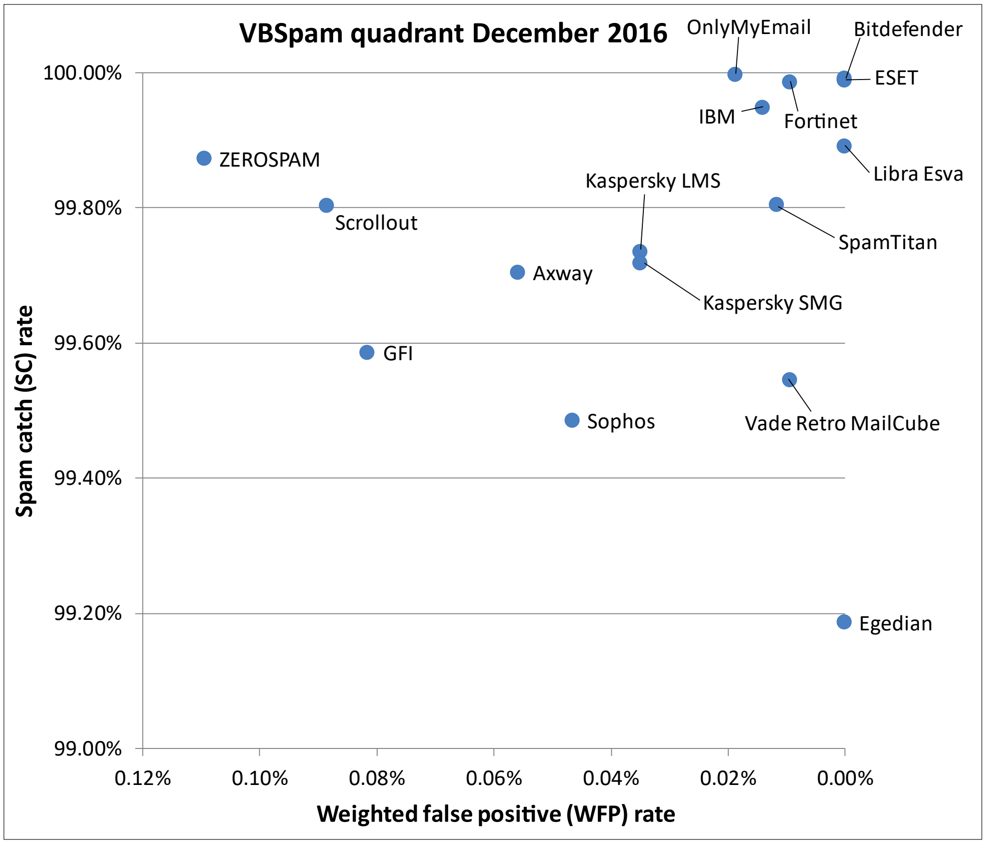
Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives, no more than 2.5% false positives among the newsletters and 'delivery speed colours' of green at 10 and 50 per cent and green or yellow at 95 and 98 per cent earn a VBSpam+ award.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

© 2016 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Email: editorial@virusbulletin.com
Web: https://www.virusbulletin.com/

Product	Final score
ESET	99.99
Bitdefender	99.98
FortiMail	99.94
OnlyMyEmail	99.90
Libra Esva	99.89
IBM	99.88
SpamTitan	99.75
Kaspersky LMS	99.56
Kaspersky SMG	99.54
MailCube	99.50
Axway	99.43
Scrollout	99.36
ZEROSPAM	99.33
Sophos	99.25
GFI MailEssentials	99.18
Egedian	99.16

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



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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	8514	3	0.04%	346	116957	99.71%	SPAM Verified	99.43
Bitdefender	8517	0	0.00%	13	117290	99.99%	SPAM+ Verified	99.98
Egedian	8517	0	0.00%	954	116349	99.19%	SPAM Verified	99.16
ESET	8517	0	0.00%	9	117294	99.99%	SPAM+ Verified	99.99
FortiMail	8517	0	0.00%	17	117286	99.99%	SPAM+ Verified	99.94
GFI MailEssentials	8453	4	0.05%	485	116818	99.59%	SPAM Verified	99.18
IBM	8516	1	0.01%	61	117242	99.95%	SPAM Verified	99.88
Kaspersky LMS	8514	3	0.04%	310	116993	99.74%	SPAM Verified	99.56
Kaspersky SMG	8514	3	0.04%	331	116972	99.72%	SPAM Verified	99.54
Libra Esva	8517	0	0.00%	128	117175	99.89%	SPAM+ Verified	99.89
OnlyMyEmail	8517	0	0.00%	3	117300	99.997%	SPAM+ Verified	99.90
Scrollout	8511	6	0.07%	230	117073	99.80%	SPAM Verified	99.36
Sophos	8513	4	0.05%	603	116700	99.49%	SPAM Verified	99.25
SpamTitan	8516	1	0.01%	229	117074	99.80%	SPAM Verified	99.75
Vade Retro MailCube	8517	0	0.00%	533	116770	99.55%	SPAM+ Verified	99.50
ZEROSPAM	8509	8	0.09%	149	117154	99.87%	SPAM Verified	99.33
IBM X-Force API*	8517	0	0.00%	6700	110603	94.29%	N/A	94.29
IBM X-Force API - combined*	8516	1	0.01%	3775	113528	96.78%	N/A	96.72
IBM X-Force API - URLs*	8516	1	0.01%	54372	62931	53.65%	N/A	53.59
Spamhaus DBL*	8517	0	0.00%	98769	18534	15.80%	N/A	15.80
Spamhaus ZEN*	8517	0	0.00%	7509	109794	93.60%	N/A	93.60
Spamhaus ZEN+DBL*	8517	0	0.00%	5611	111692	95.22%	N/A	95.22
URIBL*	8474	43	0.50%	66248	51055	43.52%	N/A	40.21

**The Spamhaus products, IBM X-Force and URIBL 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		Project Honey Pot		Abusix		Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	10%	50%	95%	98%
Axway	9	2.6%	24	99.72%	316	99.72%	30	99.44%	🟢	🟢	🟢	🟢
Bitdefender	1	0.3%	0	100.00%	9	99.99%	4	99.92%	🟢	🟢	🟢	🟢
Egedian	2	0.6%	97	98.86%	921	99.18%	33	99.38%	🟢	🟢	🟢	🟢
ESET	0	0.0%	0	100.00%	8	99.99%	1	99.98%	🟢	🟢	🟢	🟢
FortiMail	4	1.2%	3	99.96%	6	99.99%	11	99.79%	🟢	🟢	🟢	🟢
GFI MailEssentials	15	4.3%	6	99.93%	405	99.64%	80	98.50%	🟢	🟢	🟡	🟡
IBM	1	0.3%	0	100.00%	58	99.95%	3	99.94%	🟢	🟢	🟢	🟢
Kaspersky LMS	0	0.0%	0	100.00%	278	99.75%	32	99.40%	🟢	🟢	🟢	🟢
Kaspersky SMG	0	0.0%	1	99.99%	297	99.73%	34	99.36%	🟢	🟢	🟢	🟢
Libra Esva	0	0.0%	0	100.00%	114	99.90%	14	99.74%	🟢	🟢	🟢	🟢
OnlyMyEmail	8	2.3%	0	100.00%	2	100.00%	1	99.98%	🟢	🟢	🟢	🟡
Scrollout	8	2.3%	26	99.69%	202	99.82%	28	99.47%	🟢	🟢	🟢	🟢
Sophos	0	0.0%	0	100.00%	573	99.49%	30	99.44%	🟢	🟢	🟢	🟢
SpamTitan	0	0.0%	0	100.00%	220	99.80%	9	99.83%	🟢	🟢	🟡	🟡
MailCube	4	1.2%	38	99.55%	532	99.52%	1	99.98%	🟢	🟢	🟢	🟢
ZEROSPAM	7	2.0%	0	100.00%	149	99.87%	0	100.00%	🟢	🟢	🟢	🟢
IBM X-Force API[*]	0	0.0%	263	96.90%	6140	94.52%	560	89.47%	N/A	N/A	N/A	N/A
IBM X-Force API - combined[*]	0	0.0%	263	96.90%	3250	97.10%	525	90.12%	N/A	N/A	N/A	N/A
IBM X-Force API - URLs[*]	0	0.0%	8475	0.02%	49330	55.95%	5042	5.15%	N/A	N/A	N/A	N/A
Spamhaus DBL[*]	0	0.0%	8438	0.46%	93544	16.47%	5225	1.71%	N/A	N/A	N/A	N/A
Spamhaus ZEN[*]	0	0.0%	96	98.87%	7361	93.43%	148	97.22%	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL[*]	0	0.0%	95	98.88%	5467	95.12%	144	97.29%	N/A	N/A	N/A	N/A
URIBL[*]	86	24.8%	8433	0.52%	61300	45.26%	4948	6.92%	N/A	N/A	N/A	N/A

[*] *The Spamhaus products, IBM X-Force and URIBL 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.*

🟢 *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.)

Hosted solutions	**Anti-malware**	**IPv6**	**DKIM**	**SPF**	**DMARC**	**Multiple MX-records**	**Multiple locations**
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Retro MailCube	DrWeb; proprietary	√	√	√		√	√
ZEROSPAM	ClamAV			√		√	√

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

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

Local solutions	**Anti-malware**	**IPv6**	**DKIM**	**SPF**	**DMARC**	**Interface**			
						CLI	**GUI**	**Web GUI**	**API**
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender, ClamAV	√				√		√	√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√		√		√	
Kaspersky SMG	Kaspersky Lab	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Scrollout	ClamAV			√		√		√	√
Sophos	Sophos		√	√				√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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