MAY 2014

virus BULLETIN

Covering the global threat landscape

MAY 2014 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

This month marks five years since six brave anti-spam products took part in the very first VBSpam test.

Spam levels peaked in late 2008 – which was when we started developing the VBSpam test framework. I have often joked that it was VBSpam that stopped spam levels from growing further, but that is of course nonsense: a few prominent botnet takedowns halted the growth and initiated a decline from which spam never fully recovered – even if levels have recently reached a three-year high[1].

Still, we hope that the last 30 VBSpam tests have contributed somewhat to the global effort to contain the problem of spam – something that we, as a community, have become rather good at. The VBSpam tests have shown potential customers which products are best at blocking spam, and for developers, they have highlighted where their products' weaknesses lie.

But these reports represent far more than bi-monthly rankings of anti-spam solutions. They provide the security community with information on trends in spam, such as the move towards spam sent from *Linux* servers – spam which we showed is harder to block[2]. We showed that spam that passes SPF is also harder to block[3], and that newsletters with a confirmed opt-in subscription mechanism were less likely to be blocked[4].

For this reason, I am excited by the fact that, as of 1 July 2014, all past and future VBSpam reports will be available to all, free of charge[5] – anyone who in one way or another is helping the fight against spam, or who is interested in it, will be able to read the test reports, and perhaps even give useful feedback.

We hope this will mean that the reports become even more widely read, and we look forward to welcoming new readers. What new readers will learn is that there are many solutions, for all kinds of businesses, that do a rather good job of fighting spam, and which typically have few, if any, false positives.

For the first time since November 2012, all of the full solutions participating in this test (there were 15 of them) achieved a VBSpam award. Six of them didn't block a single legitimate email and, by combining this with a high spam catch rate and a low newsletter-blocking rate, they earned a VBSpam+ award.

THE TEST SET-UP

The VBSpam test methodology can be found at http://www.virusbtn.com/vbspam/methodology/. As usual, emails were sent to the products in parallel and in real time, and products were given the option to block email pre-DATA (that is, based on the SMTP envelope and before the actual email was sent). Three products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. 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

[1] http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark/.
[2] https://www.virusbtn.com/virusbulletin/archive/2013/05/vb201305-vbspam-comparative.
[3] https://www.virusbtn.com/virusbulletin/archive/2013/01/vb201301-vbspam-comparative.
[4] https://www.virusbtn.com/virusbulletin/archive/2011/09/vb201109-vbspam-comparative.
[5] https://www.virusbtn.com/virusbulletin/archive/2014/04/vb201404-shape-of-things.

ISSN 1749-7027

we receive is representative of that received by a smaller organization.

To compare the products, we calculate a 'final score', which 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)

Products earn VBSpam certification if the value of the final score is at least 98:

SC - (5 x WFP) ≥ 98

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives and no more than 2.5% false positives among the newsletters earn a VBSpam+ award.

THE EMAIL CORPUS

In recent months, we have experienced a number of issues caused by the lack of scalability of our VBSpam test network. While it is true that in many organizations, spam filters are required to filter many times the number of emails we process in our tests, in our environment, one copy of each email is sent to each participating filter. Moreover, we keep a full audit trail for each email: this allows participants to check that the apparent misclassification of an email hasn't been caused by a glitch on our side.

Having unexpectedly been forced to make some network changes, we spent several days working on improving the VBSpam framework and making it both able to handle more emails and more robust.

This worked. Almost. A mechanism that was intended to pause the sending of emails for a short while should the framework come under a lot of pressure worked a little too well and led to an eight-hour period (overnight from 28 to 29 April) during which no emails were sent. Other than that, there were no significant issues during the 16-day period over which the test ran.

The test period started at 12am on Saturday 26 April and ended at 12am on Monday 12 May 2014.

The test corpus consisted of 143,245 emails – almost 50% more than in the last test. 131,030 of these emails were spam, 66,884 of which were provided by *Project Honey Pot*, with the remaining 64,146 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 11,873 legitimate emails ('ham') and 342 newsletters.

Figure 1 shows the catch rate of all full solutions throughout the test. To avoid the average being skewed by poorly performing products, the highest and lowest catch rates have been excluded for each hour.

As the graph shows, spam catch rates were very high and the average catch rate has barely changed between the last test and this one. This is good news, especially given the increase in size of the *Abusix* corpus, which some products have had difficulties with in the past.

Interestingly, the average false positive rate more than halved compared to the last test – although this decline was mainly caused by three products that had relatively high false positive rates in the previous tests.

'Newsletters' – a corpus which includes both direct-marketing emails and purely informative newsletters, but always ones that have explicitly been subscribed to – remained harder to detect than ordinary ham, with an average block rate of over 4%. This number wasn't simply caused by a number of senders with poor sending practices: the most 'difficult' newsletter, a marketing email from a Japanese firm, was still only blocked by five products.

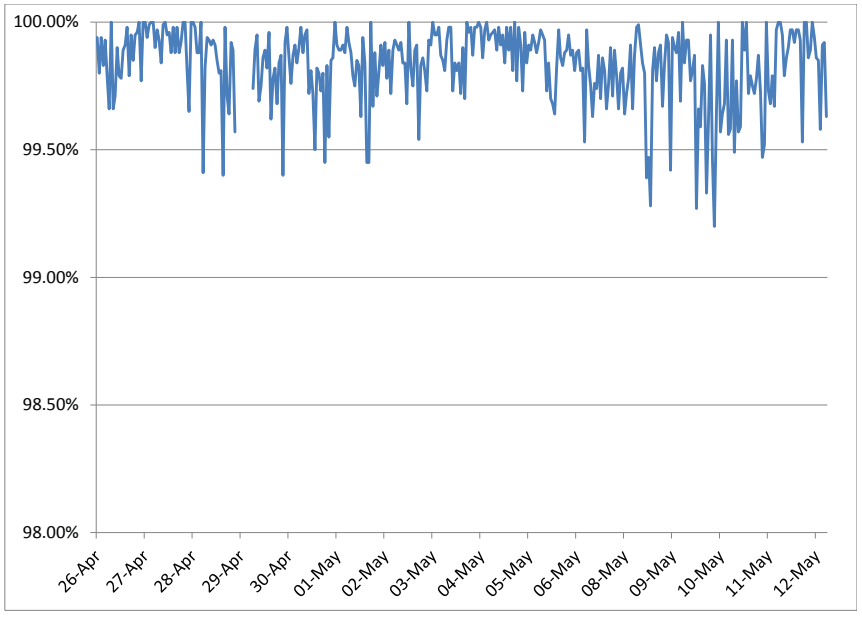


Figure 1: Spam catch rate of all complete solutions throughout the test period.

As for difficult spam: two emails stood out as particularly difficult to filter – both were blocked by only a third of the participating full solutions.

One was an email in German, congratulating the recipient on winning €1,250,000 in an email lottery. Of course, payment of a fee was required in order to claim the money, which is how the scam works. With the content embedded as an image, it is perhaps not surprising that products found it hard to block the email.

Figure 2: German lotto scam.

The same holds for the other difficult email, which offered databases of email addresses for sale and which, on the face of it, may look reasonably legitimate. Selling such databases is considered rather a bad idea and is probably illegal in many countries. The fact that the email was sent to a spam trap makes one wonder about the quality of the databases in any case.

Hi,

Would you be interested in acquiring contact database with complete Business Email and phone Numbers of your most potential prospects to boost your sales efforts?

Accounts Software Users:

Accounting Director	Finance Director
Accounting Manager	Finance Manager
Audit and Compliance Director	Information Technology Audit Manager
Budget Manager	Regulators
Chief Accounting Officer	Senior Strategic Planner
Chief Financial Officer	State and Private Pension Fund Managers
Director of Financial Operations	And many more...

Ã¼ Complete list with Email address in an Excel Sheet for unlimited usage.
Ã¼ Do an email blast endorsing your product/services and providing your contact information.
Ã¼ Email appending, multiple contacts appending, Data appending which will append or add the missing information to your existing database

Figure 3: Email databases spam.

DMARC

In January, we looked at which products supported the DMARC protocol[6]. We found that very few products supported it, but we also noted that DMARC was started as a private project among some larger senders: it is thus not surprising that adoption of the protocol among participating spam filters – which tend to cater for small and medium-sized organizations – is a little slower.

DMARC made the news recently when first *Yahoo!*[7] and then *AOL*[8] set strict DMARC policies, thus significantly reducing the delivery rates of spam that forges the companies' addresses, but also causing not insignificant collateral damage for email discussion lists.

We follow these developments with interest, in particular because we use such lists as a source for our ham stream. It is possible that other senders will follow suit and adopt strict DMARC policies, thus ultimately forcing discussion lists to rewrite the From: address. It is also possible that the collateral damage will cause receiving mail servers to stop adhering to senders' strict DMARC policies.

What these developments show is that the fight against spam is far more complex than a simple cat-and-mouse game between spam senders and spam fighters.

RESULTS

In the text that follows, unless otherwise specified, 'ham' or 'legitimate email' refers to email in the ham corpus – which excludes the newsletters – and a 'false positive' is a message in that corpus that has been erroneously marked by a product as spam.

Because the size of the newsletter corpus is significantly smaller than that of the ham corpus, a missed newsletter has a much greater effect on the newsletter false positive rate than a missed legitimate email has on the false positive rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of less than 0.01%, while one missed email in the newsletter corpus results in an FP rate of almost 0.3%).

It should also be noted that, because of the recent change to the formula used to calculate the final score, these scores are not comparable with those achieved in reports prior to the March 2014 report.

[6] https://www.virusbtn.com/virusbulletin/archive/2014/01/vb201401-vbspam-comparative.
[7] https://www.virusbtn.com/blog/2014/04_15.xml.
[8] https://www.virusbtn.com/blog/2014/04_23.xml.

Axway MailGate 5.3.1

SC rate: 99.20%
FP rate: 0.03%
Final score: 98.85
Project Honey Pot SC rate: 99.20%
Abusix SC rate: 99.19%
Newsletters FP rate: 7.9%

Axway MailGate has had some issues with false positives in the last couple of tests, so I was rather pleased to see that the product missed only three legitimate emails on this occasion – in three different languages. Against that stood a slight drop in the spam catch rate, although in fairness to *Axway*'s developers, they may have been a bit unlucky as about half of the spam missed by the product was part of a single campaign.

The product erroneously blocked an international selection of newsletters, but with a final score of 98.85, I am pleased to say that the virtual appliance regained its VBSpam certified status.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.6%

One of the six brave products mentioned in the introduction that entered the very first VBSpam test five years ago, was *Bitdefender*'s anti-spam solution, and the product hasn't missed a single test since. What is more, the product has never failed to earn a VBSpam award, and in January 2013 it started a run of VBSpam+ awards.

This test was no different: yet again, the product had no false positives, while the spam catch rate increased even further to a rather stunning 99.98% – just 28 spam emails slipped through *Bitdefender*'s grasp. The product thus earns its ninth successive VBSpam+ award (its 31st VBSpam award).

Egedian Mail Security

SC rate: 99.74%
FP rate: 0.06%
Final score: 99.37
Project Honey Pot SC rate: 99.55%
Abusix SC rate: 99.94%
Newsletters FP rate: 2.6%

It is always exciting when a new vendor decides to submit its solution to our test bench. *Profil Technology* is a company from the Parisian suburb of Montrouge, which sells a number of different products for the French and international market, including the email security solution *Egedian Mail Security*.

The product is based on a number of third-party technologies, such as *Copperfasten* for the spam filter and *Bitdefender* for the anti-malware element. Installation and set-up of the product on a virtual host was easy and it didn't take long for the product to become fully adjusted to our environment.

I am used to it taking a few tests for new participants to fully adjust to the test conditions, especially when it comes to false positives. I was thus delighted to see *Egedian* miss only seven legitimate emails and nine newsletters.

At the same time, the product's catch rate was 99.74% – higher than that of several other participants. Among the spam that was missed, about a third was written in Japanese. A more than decent debut, and with a final score of 99.37, *Egedian Mail Security* earns its first VBSpam award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.63%
FP rate: 0.03%
Final score: 99.48
Project Honey Pot SC rate: 99.37%
Abusix SC rate: 99.91%
Newsletters FP rate: 0.9%

ESET missed fewer than one in 270 spam messages – a pretty good performance and a nice increase in catch rate compared to the last test. Among those emails that were missed were some apparent phishing emails – a reminder to end-users that they shouldn't trust their spam filter never to let anything bad slip through, and perhaps also a hint as to the importance of a multiple-layered defence strategy.

False positives were few, if not non-existent (although the three missed emails were all sent from the same source). As a consequence, the product just missed out on a VBSpam+ award, but the product's 11th VBSpam award should keep its developers motivated towards aiming for that VBSpam+ next time.

Fortinet FortiMail

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.87
Project Honey Pot SC rate: 99.83%

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	11870	3	0.03%	1052	129978	99.20%	98.85
Bitdefender	11873	0	0.00%	28	131002	99.98%	99.96
Egedian	11866	7	0.06%	342	130688	99.74%	99.37
ESET	11870	3	0.03%	480	130550	99.63%	99.48
FortiMail	11873	0	0.00%	123	130907	99.91%	99.87
GFI	11870	3	0.03%	533	130497	99.59%	99.46
IBM	11866	7	0.04%	214	130816	99.84%	99.55
Kaspersky LMS	11873	0	0.00%	262	130768	99.80%	99.79
Libra Esva	11873	0	0.00%	83	130947	99.94%	99.92
Netmail Secure	11870	3	0.03%	379	130651	99.71%	99.58
OnlyMyEmail	11873	0	0.00%	5	131025	99.996%	99.98
Scrollout	11863	10	0.08%	123	130907	99.91%	98.91
Sophos	11869	4	0.03%	371	130659	99.72%	99.54
SpamTitan	11873	0	0.00%	251	130779	99.81%	99.80
ZEROSPAM	11866	7	0.03%	100	130930	99.92%	99.27
Spamhaus DBL*	11872	1	0.01%	94900	36130	27.57%	27.52
Spamhaus ZEN*	11873	0	0.00%	12231	118799	90.67%	90.67

*Spamhaus is a partial solution and its performance is not to be compared with that of other products.

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

Abusix SC rate: 99.99%
Newsletters FP rate: 1.2%

Fortinet's *FortiMail* appliance missed only the very first few VBSpam tests, and looking at its past results, it is no wonder its developers were confident enough to submit it so early on – it has proved to be one of the better performing products in each test.

This test is no different. In fact, with no false positives and a high catch rate, *Fortinet* achieves not just its 30th VBSpam award, but its third VBSpam+ award.

GFI MailEssentials

SC rate: 99.59%
FP rate: 0.03%
Final score: 99.46
Project Honey Pot SC rate: 99.36%
Abusix SC rate: 99.83%
Newsletters FP rate: 0.3%

GFI's *MailEssentials* missed three legitimate emails – an increase from the last test (in which it only missed one), but as they all three came from the same source, it may have been a single mistake that caused them. In any case, false positives are a minor problem for *GFI*, which also blocked only a single newsletter.

The same is true for missed spam, which only happened around once in every 250 emails – a figure comparable to the product's performance in the previous test. We are pleased to be sending news of yet another VBSpam award to the company's headquarters in Malta.

IBM Lotus Protector for Mail Security

SC rate: 99.84%
FP rate: 0.04%
Final score: 99.55
Project Honey Pot SC rate: 99.68%
Abusix SC rate: 99.998%
Newsletters FP rate: 2.6%

It is hard not to feel a little sorry for *IBM*, as four of the five false positives

	Newsletters		Project Honey Pot		Abusix		pre-DATA‡		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway	27	7.9%	535	99.20%	517	99.19%			3.36
Bitdefender	2	0.6%	17	99.97%	11	99.98%			0.1
Egedian	9	2.6%	302	99.55%	40	99.94%			0.33
ESET	3	0.9%	422	99.37%	58	99.91%			0.68
FortiMail	4	1.2%	114	99.83%	9	99.99%			0.28
GFI	1	0.3%	425	99.36%	108	99.83%			0.57
IBM	9	2.6%	213	99.68%	1	99.998%			0.29
Kaspersky LMS	1	0.3%	193	99.71%	69	99.89%			0.38
Libra Esva	2	0.6%	82	99.88%	1	99.998%	119693	91.35%	0.2
Netmail Secure	1	0.3%	341	99.49%	38	99.94%	119235	91.00%	0.48
OnlyMyEmail	2	0.6%	2	99.997%	3	99.995%			0.04
Scrollout	99	29.0%	88	99.87%	35	99.95%			0.23
Sophos	1	0.3%	288	99.57%	83	99.87%			0.4
SpamTitan	1	0.3%	240	99.64%	11	99.98%			0.3
ZEROSPAM	58	17.0%	95	99.86%	5	99.99%	127475	97.29%	0.21
Spamhaus DBL*	1	0.3%	39245	41.32%	55655	13.24%			8.13
Spamhaus ZEN*	0	0.0%	10546	84.23%	1685	97.37%			4.02

*Spamhaus is a partial solution and its performance is not to be compared with that of other products.

‡pre-DATA filtering was optional and was applied on the full corpus. All of ZEROSPAM's false positives occurred pre-DATA, all others occurred post-DATA.

†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.)

its *Lotus Protector* product picked up this month were caused by a setting that blocked emails with too many Received: headers. This is an entirely reasonable setting, but unfortunately, our ham corpus contained four emails with more than 20 such headers. That is an unusually large number, even if the emails were completely legitimate. In any case, after speaking with the product's developers, they have raised the product's threshold.

It was actually a rather good test for *IBM*, which saw its spam catch rate increase to 99.84% – interestingly, only one of the 214 missed spam emails were from the *Abusix* corpus. The product thus easily achieved yet another VBSpam award – and is not far off achieving its first VBSpam+ award.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.80%

FP rate: 0.00%

Final score: 99.79

Project Honey Pot SC rate: 99.71%

Abusix SC rate: 99.89%

Newsletters FP rate: 0.3%

Kaspersky Security 8 for Linux Mail Server is a mouthful – but among regular readers of these reports, it will be known as the spam filter from the Russian security giant that continues to perform so well. Once again this month, it didn't block any legitimate email – although it did block a single newsletter: an email from *Xerox* was wrongly copied to the spam folder.

The product's spam catch rate increased a little as well – among the 262 emails that were missed were a fairly large number of emails that were written in Japanese. With such impressive scores, *Kaspersky* is well deserving of its fifth VBSpam+ award.

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
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	Kaspersky; McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender	√				√		√	√
ESET	ESET Threatsense					√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Netmail Secure	Proprietary	√	√	√		√		√	
Scrollout	ClamAV			√		√		√	
Sophos	Sophos							√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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

Libra Esva 3.2

SC rate: 99.94%
FP rate: 0.00%
Final score: 99.92
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.998%
Pre-DATA SC rate: 91.35%
Newsletters FP rate: 0.6%

I had the pleasure of meeting some of *Libra Esva*'s developers at the recent Infosec exhibition in London. Their exhibition stand proudly displayed the product's VBSpam performance history. The developers have every right to be proud, given that the product has achieved VBSpam certification in all 24 tests that it has entered – and on no fewer than seven of those occasions it has earned a VBSpam+ award.

This test was no exception: yet again, the product combined a catch rate of over 99.9% with a lack of false positives. With just a single blocked newsletter, the Italian company gains yet another VBSpam+ to add to its growing collection.

Netmail Secure

SC rate: 99.71%
FP rate: 0.03%
Final score: 99.58
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.94%
Pre-DATA SC rate: 91.00%
Newsletters FP rate: 0.3%

Looking through the spam missed by the *Netmail Secure* virtual appliance was a good reminder that a lot of today's spam isn't a mere nuisance, simply trying to sell *Viagra* or weight-loss products: a lot of spam messages have a malicious payload. Hence blocking nine out of 10 emails doesn't suffice.

Complete solutions sorted by final score	
OnlyMyEmail	99.98
Bitdefender	99.96
Libra Esva	99.92
FortiMail	99.88
SpamTitan	99.80
Kaspersky LMS	99.79
Netmail Secure	99.58
IBM	99.56
Sophos	99.54
ESET	99.48
GFI	99.46
Egedian	99.37
ZEROSPAM	99.27
Scrollout	98.92
Axway	98.85

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

Thankfully, *Netmail*'s spam catch rate is far better than that: it blocks more than 997 out of every 1,000 spam emails, and the few missed emails that I did see really were the exception. In any case, it was an increase in catch rate compared to the last test. The number of false positives increased too, from one to three, but as they all came from the same source, this may be related. Clearly, *Netmail* is well deserving of its 20th VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.996%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 99.995%
Newsletters FP rate: 0.6%

Five spam emails were missed by *OnlyMyEmail*'s hosted anti-spam solution, which is more than the product has missed since July 2012. To put it differently: missing fewer than one in 26,000 spam emails is the *worst* the product has performed in a long while – which is rather an impressive claim.

On this occasion (and indeed on several others), *OnlyMyEmail* didn't erroneously block any legitimate emails, and it blocked only two newsletters. With the highest final score in this test, the VBSpam+ award for *OnlyMyEmail* shines brightly.

Scrollout F1

SC rate: 99.91%
FP rate: 0.08%
Final score: 98.91
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.95%
Newsletters FP rate: 29.0%

Scrollout F1, the free ('as in beer and as in speech') virtual solution, has historically had a relatively large number of false positives, so I was rather pleased to see this number drop to ten. Although the false positive rate was still higher than that of any other product (and the 29% newsletter FP rate remains a slight concern), it was good to see signs of some improvement.

Happily, the improvement in false positive rate didn't come at the cost of a reduced catch rate, which at 99.91% remains high. As a result, with a decent final score, *Scrollout* obtains another VBSpam award.

Sophos Email Appliance

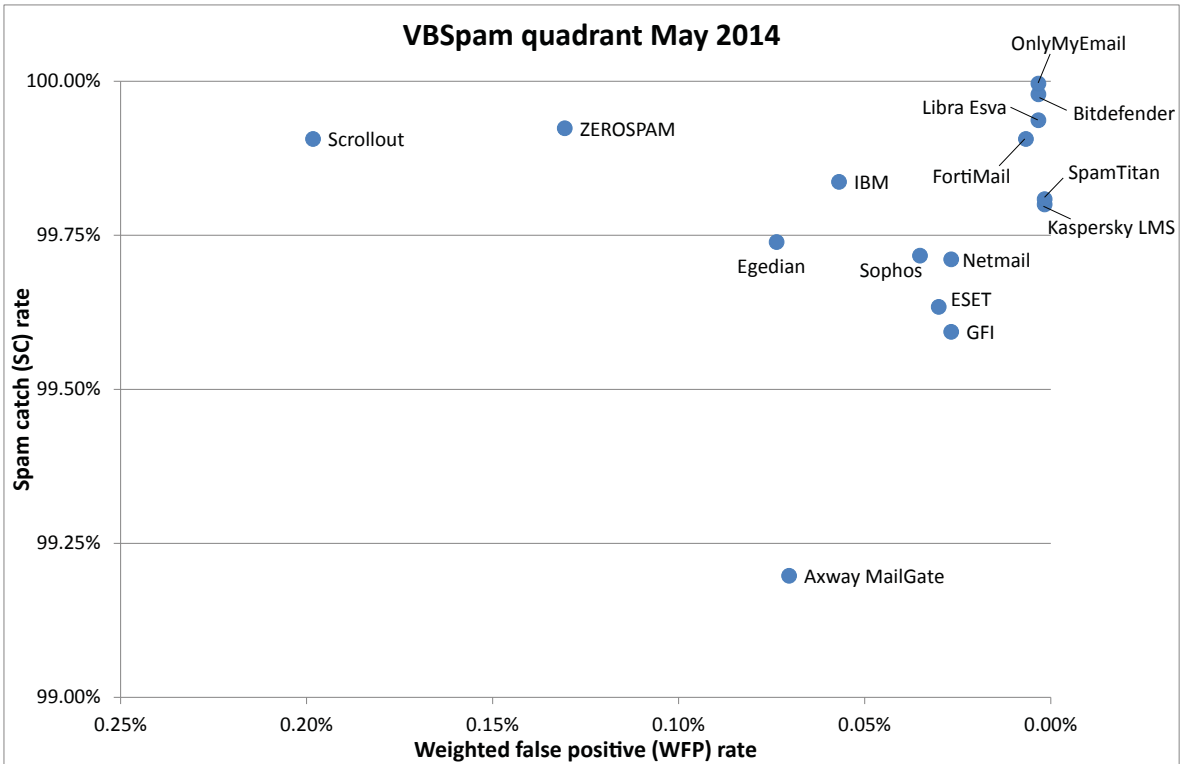
SC rate: 99.72%
FP rate: 0.03%
Final score: 99.54
Project Honey Pot SC rate: 99.57%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.3%

Having hit a bit of a glitch in the last test, *Sophos*'s false positive rate bounced back this month, and the product missed only four legitimate emails, and only one newsletter (an area in which the product has always scored well).

The product's spam catch rate was also a little better and I noticed a lot of emails in foreign character sets among those that were missed. All in all, it was a good test for *Sophos*'s hardware appliance, which earns its 26th VBSpam award.

SpamTitan 6.00

SC rate: 99.81%
FP rate: 0.00%
Final score: 99.80
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%



(Please refer to text for full product names.)

SpamTitan's virtual appliance missed just a single newsletter in this test, which I was pleased to see as, although it's the least important of the three main feeds, it was a relatively high newsletter FP rate that caused the product to miss out on a VBSpam+ award in the last test.

Thankfully, performance on the other feeds remained good as well, with yet again no false positives and a spam catch rate that was only marginally lower than in the last test. The Irish product is thus well deserving of its fourth VBSpam+ award.

ZEROSPAM

SC rate: 99.92%
FP rate: 0.03%
Final score: 99.27
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.99%
Pre-DATA SC rate: 97.29%
Newsletters FP rate: 17.0%

ZEROSPAM is one of the few products in the test that is set up so that we can measure its 'pre-DATA' catch rate: the percentage of spam blocked based on the email's sending IP address and domain. At well over 97%, this was rather high, which should help keep *ZEROSPAM*'s servers in Canada nice and clean. In this test, it also meant that the four false positives were blocked pre-DATA, which would probably have meant that the senders would have been sent a bounce message, which would at least inform them that their message had not reached the recipient.

'Post-DATA' filtering increased the product's total catch rate to a very decent 99.92% – although the good news was tempered by the fact that no fewer than 58 newsletters were erroneously blocked. This lowered the final score quite a bit, but ultimately it didn't stop *ZEROSPAM* from achieving yet another VBSpam award.

Spamhaus DBL

SC rate: 27.57%
FP rate: 0.01%
Final score: 27.52
Project Honey Pot SC rate: 41.32%
Abusix SC rate: 13.24%
Newsletters FP rate: 0.3%

Spamhaus ZEN

SC rate: 90.67%
FP rate: 0.00%
Final score: 90.67
Project Honey Pot SC rate: 84.23%
Abusix SC rate: 97.37%
Newsletters FP rate: 0.0%

Spamhaus will be a familiar name to regular readers of these reports, or to anyone dealing with spam in one way or another: the maintainers of the various blacklists (many of whom are volunteers) are at the forefront of the fight against spam. It was at their request that we have separated the scores for *Spamhaus DBL* and *Spamhaus ZEN*.

Spamhaus DBL is a blacklist of domains used in spam. Domains found in each email header and body are checked against the list. As previously mentioned in these reports, domain block rates do tend to vary, and the almost 27.6% of emails that were found to contain at least one blacklisted domain probably says at least as much about the kind of domains spammers have been using recently as it does about the quality of the *DBL*.

In this case, one legitimate email contained a blacklisted domain: the popular bit.ly URL shortener, commonly used by spammers and legitimate senders alike. One can imagine making an exception for this domain in the integration of the *DBL* into one's own anti-spam solution.

Spamhaus ZEN is a combination of three popular IP-based blacklists. The just over 90% of emails blocked by this combined list were blocked purely based on the sending IP address. Considering that there weren't any false positives for this list – not even among newsletters – one can understand why many a system administrator puts this blacklist in front of, or integrates it into, their anti-spam solution.

CONCLUSION

It is pleasing to write a report in which every full solution has at least something to celebrate. Of course, this is also good news for the billions of users who have so many good spam filters to choose from.

Still, as mentioned before, the fight against spam isn't over, and the debate around DMARC shows the kind of challenges the email and anti-spam community faces today. We will continue to follow this debate with interest and do what we can to measure the effect of what is happening.

The next VBSpam test will run in June 2014, with the results scheduled for publication in July. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

VIRUS BULLETIN

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineer: Scott James

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Perl Developer: Tom Gracey

Consultant Technical Editors:

Dr Morton Swimmer, *Trend Micro, Germany*

Ian Whalley, *Google, USA*

SUBSCRIPTION RATES

Subscription price for Virus Bulletin magazine (including comparative reviews) for 1 year (12 issues):

- Single user: $175
- Corporate (turnover < $10 million): $500
- Corporate (turnover < $100 million): $1,000
- Corporate (turnover > $100 million): $2,000
- *Bona fide* charities and educational institutions: $175
- Public libraries and government organizations: $500

Corporate rates include a licence for intranet publication.

Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):

- Comparative subscription: $100

See http://www.virusbtn.com/virusbulletin/subscriptions/ for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: http://www.virusbtn.com/