JANUARY 2013

virus BULLETIN

Fighting malware and spam

JANUARY 2013 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

Security professionals have been debating for some time about whether desktop anti-virus makes a significant difference to a user's security – especially if the user follows good security practices. I've been following this debate – which was stirred up recently following the publication of a report[1] on the effectiveness of AV solutions, which presented some shocking results (and an equally shocking testing methodology) – with some interest.

Where spam filters are concerned, there is less debate: people do receive spam and, despite a decrease in global spam volumes, few would suggest that they can do without a spam filter. What's more, as our tests have repeatedly shown, most spam filters do a more than decent job of blocking most spam at the cost of a very small number of false positives (if any).

Of course, our test results are measured in a lab environment. On the one hand, this means that a small number of the products' features may not have been able to run, while on the other hand it means that products are not always tested against some of the more 'difficult' spam – such as targeted spam, as well as large numbers of emails in the grey area between ham and spam. Moreover, it is commonly said of spam that 'your mileage may vary' – that is, one person's (or organization's) spam can differ greatly from that of another.

This does not affect the relevance of the VBSpam tests, though. The tests are comparative, and the performance of each product can be judged against that of its competitors. However, readers should bear in mind that the measured performance of products in the VBSpam tests should always be considered in the context of these tests, and cannot immediately be translated into a real-life situation – though of course, where one product performs better than another in the test, it is also likely to do so in a real situation.

This is not to trivialize the performance of products in this test. No fewer than ten of the 21 complete solutions tested achieved a VBSpam+ award by blocking at least 99.5% of the spam from our test stream, while not blocking any of the 9,000+ legitimate emails. A further ten solutions achieved a standard VBSpam award.

THE TEST SET-UP

The VBSpam test methodology can be found at http://www.virusbtn.com/vbspam/methodology/. As usual, email was sent to the products in parallel and in real time, and products were given the option to block email pre-DATA. Five products chose to make use of this option.

As in previous tests, the products that needed to be installed on a server were installed on a *Dell PowerEdge R200*, with a 3.0GHz dual core processor and 4GB of RAM. The *Linux* products ran on *CentOS 6.3* (*Bitdefender*) or *Ubuntu 11* (*Kaspersky*); the *Windows Server* products ran on either the 2003 or the 2008 version, depending on which was recommended by the vendor.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the false positive (FP) rate. Products earn VBSpam certification if this value is at least 98 (note that this threshold has been raised as of this test – previously it was 97):

SC - (5 x FP) ≥ 98

Meanwhile, those products that combine a spam catch rate of 99.50% or higher with a lack of false positives earn a VBSpam+ award.

As always, we stress that there is no objective justification for using the weight of 5 in the calculation of the final

[1] http://www.imperva.com/download.asp?id=324

ISSN 1749-7027

score: the spam catch and false positive rates are two distinct metrics of a spam filter and any way in which they are combined into a one-dimensional metric is arbitrary. Readers who prefer to use a different weight – or a different formula altogether – are encouraged to do so given the numbers presented in this report.

THE EMAIL CORPUS

As usual, the test ran for 16 consecutive days, from 12am GMT on Saturday 22 December 2012 until 12am GMT on Monday 7 January 2013.

The corpus contained 74,240 emails, 64,988 of which were part of the spam corpus. Of these, 58,772 were provided by *Project Honey Pot*, and 6,216 were provided by *Spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the remaining emails, consisting of 9,073 legitimate emails ('ham') and 179 newsletters.

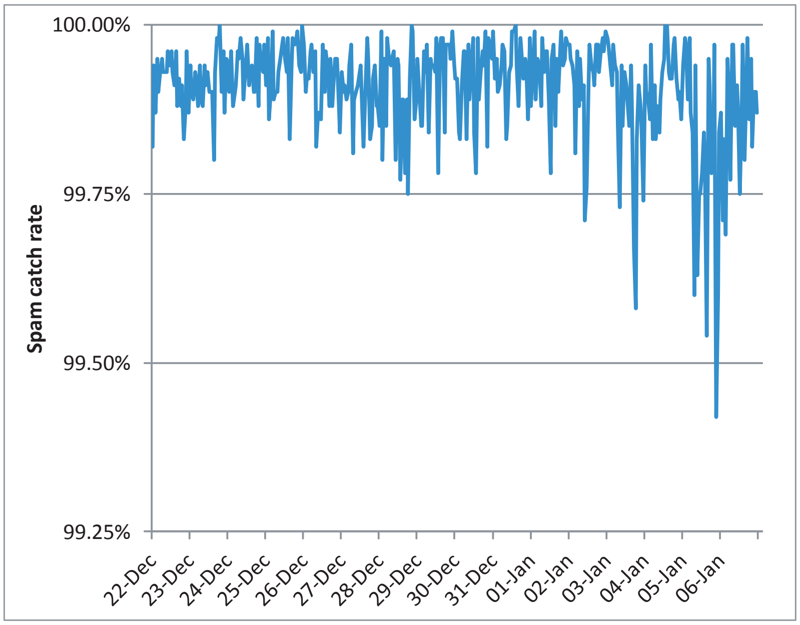


Figure 1: Spam catch rate of all complete solutions throughout the test period.

The testing period included the Christmas holiday, which has traditionally been a period during which a lot of spam is sent – not surprisingly, given that most spam has a commercial motive. However, these days, spammers are more limited in their ability to send large volumes of spam and spam levels follow a less predictable pattern.

The test team took some much needed time off over Christmas, which unfortunately meant that we were not able to fix some technical issues – as a consequence of which the *Wombat* phishing feed could not be included this time, and the size of the *Abusix* corpus in this test was relatively small. We hope to include both feeds at full capacity in the next test.

Figure 1 shows the catch rate of all complete 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. Once again, the graph shows that spam catch rates were very good – only once did the average performance drop below 99.5%.

SPF

While the VBSpam tests are an excellent way to see how well spam filters perform compared with their competitors, the tests also give an interesting insight into what kind of spam is most likely to be blocked by spam filters.

On this occasion, we looked into a possible relationship between how hard it is for an email to be blocked[2] and its SPF status.

SPF (Sender Policy Framework) is a mechanism designed to 'protect' the sending domain of the email. The domain owner uses a DNS TXT record to publish an SPF policy, which is a list or block of IP addresses that are allowed to send mail from that domain. The idea is that this prevents others from forging mail from the domain.

While this may sound promising – forged senders are a huge problem in spam – there are many caveats. For instance, there is nothing to stop spammers from setting SPF up for their own domains (e.g. domains of the type 'paypaI.com'), or from sending mail from domains for which no SPF policy is set. Also, the sender address 'protected' by SPF is the one used in the SMTP envelope, not the one that is seen by the recipient in the email headers.

More importantly, SPF doesn't survive some kinds of email forwarding, meaning that very few SPF policies are set to 'fail' for emails that do not come from the sender's IP range. Most SPF records return either 'neutral' ('we don't know') or 'softfail' ('it's probably not from us, but we can't be sure') for non-matching IP addresses.

Nevertheless, SPF has many uses. Its result can be used to determine the 'spamminess' of an email. Positive SPF statuses ('pass') are commonly interpreted as a sign that the

[2] In email circles, it is more common to refer to the 'delivery' rate of an email campaign. However, that seems a little wrong in a context where blocking emails is the correct thing to do.

sender is real – many large email receivers only send spam reports to senders that pass SPF. And, together with DKIM, an SPF pass is a sign that an email sent from a commonly phished domain is actually genuine: if it walks like a *Twitter* email, talks like a *Twitter* email and also passes *Twitter*'s SPF, then it probably *is* an email from *Twitter*.

Indeed, as can be seen in the tables later on in this report, most products use SPF in one way or another. (As with other qualitative checks, we do not wish to make a claim as to whether using SPF is important or even necessary – indeed, some products perform really well without using SPF.)

For this little piece of research, we looked at spam messages with five different SPF statuses and looked at how many products (out of the 21 complete solutions) missed the email. The five statuses were: 'pass', 'fail', 'softfail', 'neutral' and 'none' (indicating that there was no SPF record available for the domain). We excluded some emails where the SPF record wasn't interpreted properly, or where the sending domain wasn't active at the time the email was sent.

We should make it clear that this is intended as a rather informal piece of research – something that could help others understand the impact of SPF on spam filtering. Its conclusions should not be interpreted as hard data as there are too many side effects that could influence the results: the fact that this is, ultimately, a lab environment, and that some spam filters have a larger 'visibility' in the wild than others.

It should also be noted that in the context of the test, false positives are not counted for legitimate emails where the sender has made an explicit public statement that emails from that particular IP address are to be discarded. This includes emails from some ISPs' networks but it also includes SPF fails[3]. This could have affected the way some products are set up regarding SPF.

Table 1 shows the number of spam emails for each of the five SPF statuses, the average number of products that failed to block these emails and the standard deviation to this average. Because of the informal nature of this research we have not done any 'real' statistics, but the graph (Figure 2) indicates that an SPF 'pass' makes it less likely for an email to be blocked; an SPF 'fail' makes it more likely for an email to be blocked.

It may be tempting to conclude that it is in spammers' interest to send spam with valid SPF records, and to avoid those domains that would SPF fail their emails. Obvious caveats aside, this may not be a bad idea: SPF is a way of taking responsibility for emails[4], so it would be good if spammers did so too, while it would also encourage people to use SPF records as a means to avoid others sending emails with their domain in the SMTP envelope.

SPF status	No. of emails	No. of products that failed to block emails (average)	Standard deviation
fail	3171	0.24	0.04
pass	8106	0.93	0.23
softfail	8672	0.45	0.09
neutral	13466	0.34	0.04
none	26938	0.43	0.06

Table 1: Effect of SPF status.

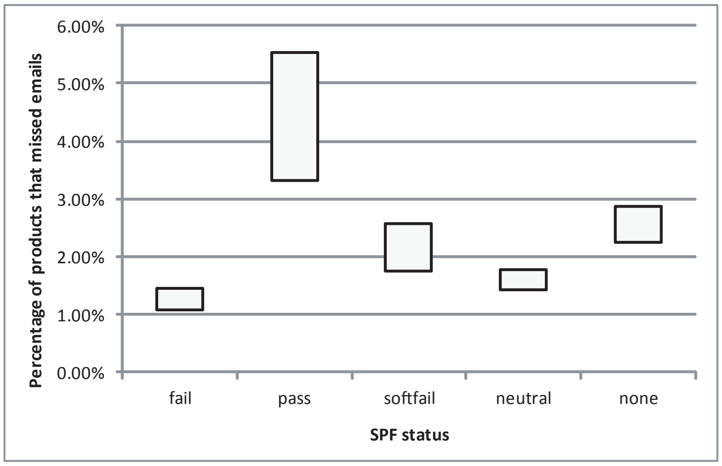


Figure 2: Effect of SPF status.

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 will have a much greater effect on the newsletter false positive rate than a missed legitimate email will have on the false positive rate for the ham corpus (e.g. one missed email in the ham corpus results in an FP rate of slightly less than 0.01%, while one missed email in the newsletter corpus results in an FP rate of almost 0.6%).

[3] The number of SPF fails we've seen on legitimate emails in the test is small, but not zero. The wisdom of using a product to block SPF fails in a real environment can be debated.

[4] Of course, SPF passes may be the result of compromised accounts; however, this would provide an incentive to prevent one's account from being compromised.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Bitdefender	9073	0	0.00%	92	64896	99.86%	99.86
ESET	9073	0	0.00%	113	64875	99.83%	99.83
FortiMail	9072	1	0.01%	236	64752	99.64%	99.58
GFI	9073	0	0.00%	138	64850	99.79%	99.79
Halon Security	9073	0	0.00%	225	64763	99.65%	99.65
IBM	9069	4	0.04%	1353	63635	97.92%	97.70
Kaspersky LMS	9073	0	0.00%	113	64875	99.83%	99.83
Libra Esva	9072	1	0.01%	17	64971	99.97%	99.91
Mailshell	9073	0	0.00%	104	64884	99.84%	99.84
McAfee Email Gateway	9064	9	0.10%	261	64727	99.60%	99.10
McAfee SaaS	9069	4	0.04%	467	64521	99.28%	99.06
Netmail Secure	9073	0	0.00%	119	64869	99.82%	99.82
OnlyMyEmail	9073	0	0.00%	0	64988	100.00%	100.00
Scrollout	9048	25	0.28%	17	64971	99.97%	98.59
Sophos	9067	6	0.07%	404	64584	99.38%	99.05
SPAMfighter	9056	17	0.19%	359	64629	99.45%	98.51
SpamTitan	9071	2	0.02%	79	64909	99.88%	99.77
Symantec	9073	0	0.00%	211	64777	99.68%	99.68
The Email Laundry	9065	8	0.09%	191	64797	99.71%	99.27
Vamsoft ORF	9067	6	0.07%	837	64151	98.71%	98.38
ZEROSPAM	9073	0	0.00%	73	64915	99.89%	99.89
Spamhaus ZEN+DBL*	9072	1	0.01%	3164	61824	95.13%	95.07
SURBL*	9072	1	0.01%	27183	37805	58.17%	58.11

* *Spamhaus* and *SURBL* are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

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

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.86%

FP rate: 0.00%

Final score: 99.86

Project Honey Pot SC rate: 99.85%

Abusix SC rate: 99.94%

Newsletters FP rate: 0.6%

This is the 23rd VBSpam test, and it sees *Bitdefender*'s product on the test bench for the 23rd time and winning its 23rd VBSpam award. The product achieved this month's fourth highest final score, and with no positives and a spam catch rate of over 99.50% (most of the fewer than 100 spam emails the product missed contained foreign character sets), it earns its first VBSpam+ award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.83%

FP rate: 0.00%

Final score: 99.83

Project Honey Pot SC rate: 99.83%

Abusix SC rate: 99.77%

Newsletters FP rate: 10.1%

ESET's *Mail Security* product earned the vendor its first VBSpam+ award in the last test. In this test, the product saw its spam catch rate increase to miss only one in 575 spam messages, while once again no legitimate emails were blocked. While the false positive rate on the non-business-critical newsletters remains relatively high, *ESET* has good reason to celebrate its second VBSpam+ award.

Fortinet FortiMail

SC rate: 99.64%

FP rate: 0.01%

Final score: 99.58

Project Honey Pot SC rate: 99.60%

Abusix SC rate: 100.00%

Newsletters FP rate: 0.0%

The results of this test will undoubtedly be the cause of some frustration for *Fortinet*'s developers, as once again a single false positive got in the way of it achieving a VBSpam+ award. Still, with yet another impressive catch rate (and no false positives among newsletters), *Fortinet* has reason to celebrate the continuation of its unbroken series of VBSpam awards – this month adding its 22nd award to the tally.

GFI MailEssentials

SC rate: 99.79%

FP rate: 0.00%

Final score: 99.79

Project Honey Pot SC rate: 99.79%

Abusix SC rate: 99.77%

Newsletters FP rate: 8.4%

In the last two tests, *MailEssentials* has blocked more spam than ever before, and this time it exceeded its previous record once more. This could have been a consequence of stricter filter settings, but that appears not to be the case: the *Windows Server* product did not block a single legitimate email, thus earning the vendor its first VBSpam+ award.

Halon Security

SC rate: 99.65%

FP rate: 0.0%

Final score: 99.65

Project Honey Pot SC rate: 99.66%

Abusix SC rate: 99.58%

Newsletters FP rate: 0.0%

Missing a shade over one in 300 spam messages (among the misses were a number of 'diploma spam' emails, as well as some seasonal spam), *Halon Security* saw its catch rate increase slightly. Once again, the product did not block any legitimate email (or even a newsletter), meaning that the Gothenburg-based company earns its second consecutive VBSpam+ award.

IBM Lotus Protector for Mail Security

SC rate: 97.92%

FP rate: 0.04%

Final score: 97.70

Project Honey Pot SC rate: 98.55%

Abusix SC rate: 91.99%

Newsletters FP rate: 0.0%

In this test, *IBM*'s spam filter for *Lotus Notes* missed more spam messages than any other complete solution; it had some difficulty with a number of spam messages in Russian, Chinese and Japanese. With four false positives as well, the product's final score fell well below 98 – and thus *IBM* is the first to fall 'victim' to the new VBSpam threshold, failing to earn an award on this occasion. The product's developers will no doubt work hard to improve its performance in time for the next test.

Kaspersky Linux Mail Security 8.0

SC rate: 99.83%

FP rate: 0.00%

Final score: 99.83

Project Honey Pot SC rate: 99.82%

Abusix SC rate: 99.90%

Newsletters FP rate: 0.0%

In the last VBSpam test *Kaspersky*'s *Linux Mail Security* product missed a VBSpam+ award by a whisker. This time it managed to banish all false positives, while barely compromising on its high spam catch rate. With no false positives on the newsletters either, the product earns a very well deserved VBSpam+ award.

Libra Esva 2.8

SC rate: 99.97%

FP rate: 0.01%

Final score: 99.91

Project Honey Pot SC rate: 99.97%

Abusix SC rate: 100.00%

SC rate pre-DATA: 92.61%

Newsletters FP rate: 1.7%

	Newsletters		Project Honey Pot		Abusix		pre-DATA[†]		STDev[‡]
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender	1	0.6%	88	99.85%	4	99.94%			0.35
ESET	18	10.1%	99	99.83%	14	99.77%			0.37
FortiMail	0	0.0%	236	99.60%	0	100.00%			0.54
GFI	15	8.4%	124	99.79%	14	99.77%			0.41
Halon Security	0	0.0%	199	99.66%	26	99.58%			0.50
IBM	0	0.0%	855	98.55%	498	91.99%			1.70
Kaspersky LMS	0	0.0%	107	99.82%	6	99.90%			0.37
Libra Esva	3	1.7%	17	99.97%	0	100.00%	4803	92.61%	0.15
Mailshell	16	8.9%	91	99.85%	13	99.79%			0.40
McAfee Email Gateway	2	1.1%	258	99.56%	3	99.95%			0.55
McAfee SaaS	0	0.0%	211	99.64%	256	95.88%			1.01
Netmail Secure	17	9.5%	106	99.82%	13	99.79%	5633	91.33%	0.39
OnlyMyEmail	0	0.0%	0	100.00%	0	100.00%			-
Scrollout	90	50.8%	17	99.97%	0	100.00%			0.16
Sophos	1	0.6%	346	99.41%	58	99.07%			0.80
SPAMfighter	6	3.4%	238	99.60%	121	98.05%			0.63
SpamTitan	4	2.2%	79	99.87%	0	100.00%			0.30
Symantec	0	0.0%	193	99.67%	18	99.71%			0.49
The Email Laundry	0	0.0%	185	99.69%	6	99.90%	1835	97.18%	0.46
Vamsoft ORF	3	1.7%	821	98.60%	16	99.74%			1.25
ZEROSPAM	4	2.8%	71	99.88%	2	99.97%	2948	95.46%	0.37
Spamhaus ZEN+DBL[*]	0	0.0%	1858	96.84%	1306	78.99%	4990	92.32%	2.67
SURBL[*]	0	0.0%	23889	59.35%	3294	47.01%			11.51

[*] *Spamhaus* and *SURBL* are both partial solutions and their performance is not to be compared with that of other products, neither should the performance of each be compared with the other.

[†] pre-DATA filtering was optional and was applied on the full corpus. One of the false positives for *The Email Laundry* occurred pre-DATA. The others were all 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.*)

Once again, a single false positive got in the way of *Libra Esva* winning its second VBSpam+ award. Still, with a spam catch rate as high as 99.97%, this can barely be considered a problem.

Libra Esva blocked more spam than all but one other product in the test. With the second highest final score this month, the product earns its 17th consecutive VBSpam award.

Mailshell Anti-Spam SDK

SC rate: 99.84%

FP rate: 0.00%

Final score: 99.84

Project Honey Pot SC rate: 99.85%

Abusix SC rate: 99.79%

Newsletters FP rate: 8.9%

VERIFIED
SPAM +
virusbtn.com

We were pleased to see the return of *Mailshell* to the VBSpam test bench, especially when it equalled the spam catch rate it achieved in September (its last entry). What is more, the anti-spam SDK – which is used in many third-party solutions – did not block any legitimate email. While the 16 missed newsletters may be a minor concern, *Mailshell*'s developers have good reason to celebrate converting the product's fourth VBSpam award into a VBSpam+ award.

McAfee Email Gateway 7.0

SC rate: 99.60%
FP rate: 0.10%
Final score: 99.10
Project Honey Pot SC rate: 99.56%
Abusix SC rate: 99.95%
Newsletters FP rate: 1.1%

vb
VERIFIED
SPAM
virusbtn.com

With nine false positives – all but one of which were in English – *McAfee*'s *Email Gateway* appliance finds itself at the higher end of the false positive spectrum. No doubt this is something the developers will want to improve upon in future tests, but in the meantime since the product missed just one in 250 emails and achieved a decent final score, it earns another VBSpam award.

McAfee SaaS Email Protection

SC rate: 99.28%
FP rate: 0.04%
Final score: 99.06
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 95.88%
Newsletters FP rate: 0.0%

vb
VERIFIED
SPAM
virusbtn.com

Like the company's hardware appliance, *McAfee*'s *SaaS* solution suffered a small increase in its false positive rate as well as a slight decrease in its spam catch rate – the interesting thing about the latter being that all but a handful of the missed spam was written in a foreign character set. This is obviously not something to be happy about, but overall the product's performance was decent, and it earns its tenth VBSpam award.

Messaging Architects Netmail Secure

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Project Honey Pot SC rate: 99.82%
Abusix SC rate: 99.79%
SC rate pre-DATA: 91.33%
Newsletters FP rate: 9.5%

vb
VERIFIED
SPAM +
virusbtn.com

The *Netmail* virtual appliance saw a small increase in its spam catch rate – most of the 119 emails missed were written in European languages – and did so without any false positives. With the newsletters perhaps a minor concern, the product from *Messaging Architects* earns its second VBSpam+ award in a row.

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.00%
Final score: 100.00
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%

vb
VERIFIED
SPAM +
virusbtn.com

This month's test sets included more than 60,000 spam emails, more than 9,000 legitimate emails and a number of newsletters as well. That is more than the average person receives in a full year. Keep this in mind when you consider the fact that *OnlyMyEmail*'s hosted anti-spam solution did not classify any of these emails incorrectly. Not a single one. To say that the product's VBSpam+ award is well deserved is quite an understatement.

Scrollout

SC rate: 99.97%
FP rate: 0.28%
Final score: 98.59
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 100.00%
Newsletters FP rate: 50.8%

vb
VERIFIED
SPAM
virusbtn.com

The anti-spam community owes a lot to developers of free, open-source software. *SpamAssassin*, one of the first spam filters, which is still used by many other products, is just one of many examples. The VBSpam tests would not be what they are without the availability of a large number of open-source programs and modules[5]. We were thus excited to see *Scrollout*, a free and open-source anti-spam product, arrive on the VBSpam test bench.

Installation of *Scrollout* was easy and no more difficult than the various commercial products we have used: we downloaded *Scrollout F1*, which allowed us to set up a virtual machine under *VMware*, and after some basic routing settings the product was ready to filter email. The web interface, where the product can be fine-tuned, was clear and easy to use.

[5] All MTAs used to manage the test run on *SuSE Linux Enterprise Server* and use the *qpsmtpd* software, and the large Perl library written to manage the test relies heavily on various third-party modules.

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	Multiple MX-records	Multiple locations
McAfee SaaS	McAfee	√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	√	√
The Email Laundry	Included[*]		√	√	√	√
ZEROSPAM	ClamAV			√	√	√

[*] Vendor prefers not to reveal identity of anti-malware engine.

Local solutions	Anti-malware	IPv6	DKIM	SPF	Interface			
					CLI	Desktop GUI	Web GUI	API
Bitdefender	Bitdefender	√			√		√	
ESET	ESET Threatsense				√	√		
FortiMail	Fortinet	√	√	√	√		√	
GFI	Five anti-virus engines	√		√			√	
Halon Security	Commtouch; Kaspersky; ClamAV; HRPS	√	√	√			√	√
IBM	Sophos; IBM Remote Malware Detection			√	√		√	
Kaspersky LMS	Kaspersky	√		√	√		√	
Libra Esva	ClamAV; others optional		√	√	√		√	
McAfee Email Gateway	McAfee	√	√	√	√	√	√	
Netmail Secure	Proprietary	√	√	√	√		√	
Scrollout	ClamAV			√	√		√	
Sophos	Sophos						√	
SPAMfighter	VIRUSfighter (optional)	√	√	√			√	
SpamTitan	Kaspersky; ClamAV	√	√	√	√		√	√
Symantec	Symantec	√	√	√	√		√	
Vamsoft ORF	Optional[†]			√		√		

[†] Various engines can be plugged in.

Mailshell (an SDK) is excluded from these tables as support for these properties depends on the implementation – the SDK itself uses neither DKIM nor SPF.

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

In its debut appearance, *Scrollout* blocked a stunning 99.97% of spam – the (joint) second highest catch rate in this test. However, against that stood the highest false positive rate, as the product missed more than two dozen legitimate emails. This, together with the fact that just over half of all newsletters were missed, makes one wonder if the product wouldn't perform better with slightly less strict spam filter settings. Nevertheless, even with its current settings the product's final score was well above 98 and thus *Scrollout* wins its first VBSpam award.

Like all participants, Scrollout's developers have received feedback on their product's performance for review and analysis. To reflect the fact that free products don't come with free support (although there is a Scrollout user forum) we decided not to give the developers access to the local installation. However, we will make configuration changes to adapt the product to the test environment should they ask us to do so.

Sophos Email Appliance

SC rate: 99.38%

FP rate: 0.07%

Final score: 99.05

Project Honey Pot SC rate: 99.41%

Abusix SC rate: 99.07%

Newsletters FP rate: 0.6%

vb
VERIFIED
SPAM
virusbtn.com

Sophos's *Email Appliance* has been filtering spam in our test lab for a long while. It was nice to see the product improve its spam catch rate slightly, although there is still a little room for improvement. The same holds for the false positive rate. Nevertheless, the product easily won its 18th VBSpam award, which should keep its developers motivated for the next test.

SPAMfighter Mail Gateway

SC rate: 99.45%

FP rate: 0.19%

Final score: 98.51

Project Honey Pot SC rate: 99.60%

Abusix SC rate: 98.05%

Newsletters FP rate: 3.4%

SPAMfighter is one of many products that have a language filter that allows users to block emails in certain languages. While we can't make any claims as to how well this works (the ham corpus is international enough for participants to want to avoid using such a setting), it might have helped *SPAMfighter* to have used such a filter in this test, as almost all of the missed spam was written in a foreign character set. Perhaps a more serious problem was the fact that 17 legitimate emails in various English-language threads were blocked. Still, there weren't enough of these to prevent the Danish product from winning its 11th VBSpam award.

SpamTitan 5.11

SC rate: 99.88%

FP rate: 0.02%

Final score: 99.77

Project Honey Pot SC rate: 99.87%

Abusix SC rate: 100.00%

Newsletters FP rate: 2.2%

SpamTitan's virtual solution blocked two legitimate emails – marking the first false positives for the product since July. This prevented the product from winning its third consecutive VBSpam+ award, but with a very good spam catch rate, there is little reason for the developers to be disappointed with their 20th VBSpam award.

Symantec Messaging Gateway 10.0

SC rate: 99.68%

FP rate: 0.00%

Final score: 99.68

Project Honey Pot SC rate: 99.67%

Complete solutions sorted by final score	
OnlyMyEmail	100.00
Libra Esva	99.91
ZEROSPAM	99.89
Bitdefender	99.86
Mailshell	99.84
Kaspersky LMS	99.83
ESET	99.83
Netmail Secure	99.82
GFI	99.79
SpamTitan	99.77
Symantec	99.68
Halon Security	99.65
FortiMail	99.58
The Email Laundry	99.27
McAfee Email Gateway	99.10
McAfee SaaS	99.06
Sophos	99.05
Scrollout	98.59
SPAMfighter	98.51
Vamsoft ORF	98.38
IBM	97.70

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

Abusix SC rate: 99.71%

Newsletters FP rate: 0.0%

The last time *Symantec*'s *Messaging Gateway* managed a clean sweep of legitimate emails was in May 2011 – well before the VBSpam+ awards were introduced. This month it repeated the achievement (and with a much larger ham corpus) and also saw a small increase in its spam catch rate. As a result, the security giant earns its first VBSpam+ award.

The Email Laundry

SC rate: 99.71%

FP rate: 0.09%

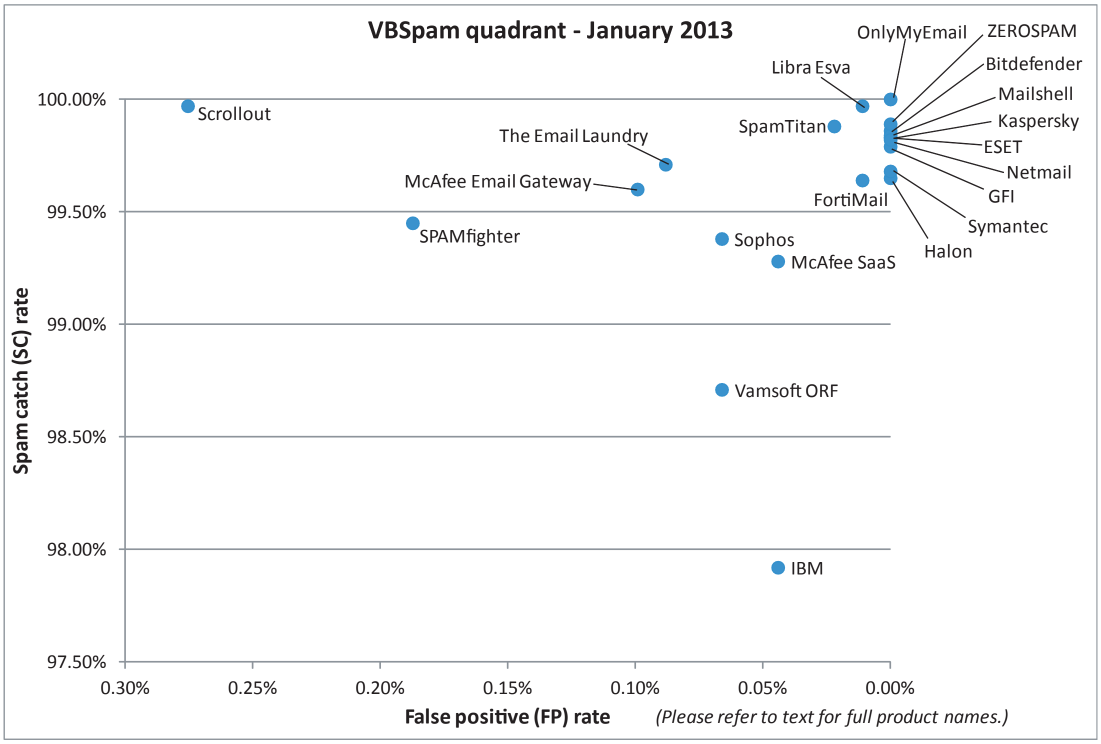
Final score: 99.27

Project Honey Pot SC rate: 99.69%

Abusix SC rate: 99.90%

SC rate pre-DATA: 97.18%

Newsletters FP rate: 0.0%



Of the products using the option to block email pre-DATA, *The Email Laundry* continues to achieve the highest pre-DATA catch rate. In fact, this rate increased by more than 1.5 percentage points on this occasion. The hosted solution blocked eight legitimate emails, in English and Russian, but no newsletters, and easily earns its 12th VBSpam award.

Vamsoft ORF

SC rate: 98.71%
FP rate: 0.07%
Final score: 98.38
Project Honey Pot SC rate: 98.60%
Abusix SC rate: 99.74%
Newsletters FP rate: 1.7%

vb VERIFIED SPAM virusbtn.com

A number of missed Japanese and Russian spam messages were to blame for a drop in *ORF*'s spam catch rate this month, while a number of erroneously classified legitimate English-language emails meant that it was not without false positives either. Nevertheless, the final score still exceeded 98 and *ORF* earns its 12th VBSpam award.

ZEROSPAM

SC rate: 99.89%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.97%
SC rate pre-DATA: 95.46%
Newsletters FP rate: 2.8%

vb VERIFIED SPAM + virusbtn.com

The tiny decrease in *ZEROSPAM*'s spam catch rate can hardly be described as a problem, given that only 73 spam emails were missed in total. Added to this was a lack of false positives (and a sharp decrease in the number of newsletter false positives), which means *ZEROSPAM* finishes its first full year of testing with its first VBSpam+ award.

Spamhaus ZEN+DBL

SC rate: 95.13%
FP rate: 0.01%
Final score: 95.07
Project Honey Pot SC rate: 96.84%
Abusix SC rate: 78.99%
SC rate pre-DATA: 92.32%
Newsletters FP rate: 0.0%

It was nice to see an increase in catch rate for *Spamhaus,* which blocked more than 19 out of 20 spam messages in this month's corpus based on the sender's IP address and domains present in the email and body alone. There was a single false positive this time – triggered by a somewhat dodgy-looking domain that had been included in an email – which is one of those cases where the blocking of the email is incorrect, yet understandable.

SURBL

SC rate: 58.17%
FP rate: 0.01%
Final score: 58.11
Project Honey Pot SC rate: 59.35%
Abusix SC rate: 47.01%
Newsletters FP rate: 0.0%

This test sees a first for *SURBL*: for the first time since joining the tests in July 2011, the domain blacklist incorrectly blocked a legitimate email. That is, a domain found in that email appeared on the blacklist – possibly because this particular domain was compromised to host malicious content; the email itself, however, was legitimate and did not link to anything dubious. Such mistakes are rare, and it remains a good thing that almost six out of 10 spam emails were found to contain at least one *SURBL*-listed domain.

In the previous report it was stated that SURBL did not block a single message in the Wombat phishing corpus. This was incorrect; a technical glitch on our side meant that none of these messages were scanned. We have strong evidence that some of these emails would have been blocked. This also affected the Spamhaus DBL blacklist. We apologize to readers, and to SURBL and Spamhaus for these mistakes.

CONCLUSION

With no fewer than ten VBSpam+ awards in a single test, this report will be received with great joy by many participants. And, of course, it is good news for the millions of people whose inboxes are protected by these products.

At the same time, outstanding performances like the ones seen in this test are a challenge for the tester: they are an encouragement to find some niche that presents ‘difficult’ emails that pose an even bigger challenge for participants. After all, the goal of the test is to show how products compare with each other – and if the differences become smaller, we need to find ways to make them visible.

The next VBSpam test will run in February 2013, with the results scheduled for publication in March. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

VIRUS BULLETIN

Editor: Helen Martin
Technical Editor: Dr Morton Swimmer
Test Team Director: John Hawes
Anti-Spam Test Director: Martijn Grooten
Security Test Engineer: Simon Bates
Sales Executive: Allison Sketchley
Perl Developer: Tom Gracey
Consulting Editors:
Nick FitzGerald, *AVG, NZ*
Ian Whalley, *Google, USA*
Dr Richard Ford, *Florida Institute of Technology, 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/

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2013 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2013/$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.