MAY 2013

virus BULLETIN

Covering the global threat landscape

MAY 2013 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

Recent industry reports[1] have noted the return of pump-and-dump spam to inboxes – just one of the many examples of how spam continues to change.

As the VBSpam tests have repeatedly shown, the performance of spam filters changes too, both on a day-to-day basis and when taking a longer-term view. However, it is not easy to detect trends in these changes, and the long and short of it is that, overall, the performance of spam filters remains good.

This may not be particularly helpful for those developers who want to make small, but potentially significant improvements to their filters – for this, they would need to identify an area in which spam filters in general, or at least their filter in particular, has room for improvement.

In this review we highlight an area in which almost all filters could make improvements: that of identifying spam sent from web hosts.

During this test we noticed that spam sent from web hosts is three-and-a-half times as likely to make it past the spam filter than spam sent from other sources. This would explain why spammers appear to be keen to send spam from web hosts – some (unconfirmed) reports claim that as much as 50% of today's spam is sent in this manner.

Of course, we also looked at how well spam filters blocked spam in general. In this test, 19 out of 20 full anti-spam solutions performed well enough to earn a VBSpam award. Two of those combined a very high catch rate with a lack of false positives and thus 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. Six products chose to make use of this option.

For the products that run 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' recommendations and note that the amount of email we receive is representative of a small organization.

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:

$$SC - (5 \times FP) \geq 98$$

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

THE EMAIL CORPUS

The test ran for 16 consecutive days. A short holiday and a visit to the Infosecurity exhibition in London meant that the test was started a little later in the month than usual – 12am on 27 April – and finished at 12am on 13 May.

The late start proved to be a blessing. At the beginning of April, we had to move a number of machines to a new server rack. This should have been a straightforward operation, however, upon turning all the machines back on, it became clear that one machine's hard drive had crashed fatally and couldn't be restored.

[1] http://www.commtouch.com/threat-report-april-2013/.

ISSN 1749-7027

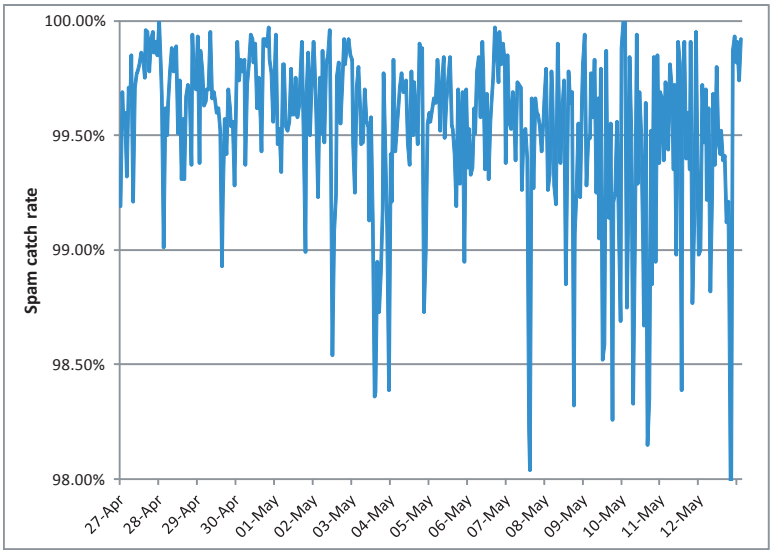


Figure 1: Spam catch rate of all complete solutions throughout the test period.

Several products were affected, each of which had to be set up again – thankfully, their developers were very helpful and made this as painless an exercise as possible, and all products were up and running again well before the start of the test.

One small glitch that occurred during the test period meant that we were unable to vouch for the stability of the network during the early hours of 10 May. As a result we have excluded emails sent during this period from the corpus.

In total, 77,993 emails were sent as part of the test, exactly 64,000 of which were spam. 54,668 of the spam messages were provided by *Project Honey Pot*, with the remaining 9,332 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 13,563 legitimate emails ('ham') and 430 newsletters, more on which below.

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.

Comparing this graph with that of the previous test, one can see less clear a trend, yet catch rates seem to be slightly higher. This is indeed the case: the average full solution saw its catch rate improve by 0.08%. This makes up for some of the deterioration we saw in March, though there are clear outliers both ways, and the improvement was far from uniform.

The average false positive rate remained more or less constant.

NEWSLETTERS

When we introduced a 'newsletter' feed of legitimate bulk emails in September 2011, we made the decision only to include double opt-in newsletters: an email is sent to the subscriber's address and this must be replied to, or a link contained within the email must be clicked, before the subscription is activated[2].

We believe this is the only proper way to prevent accidental subscriptions, as well as deliberate subscriptions by third-party 'pranksters', both of which would lead to unwanted and unsolicited emails being sent. Many senders have such a system in place – indeed, if your subscribers really want to receive your messages, confirming the subscription shouldn't be an unreasonable thing to ask of them.

However, the reality is that the majority of senders of bulk emails/newsletters do not confirm subscriptions. As the purpose of these tests is to reflect what is happening in the real world, rather than in some ideal world where all senders follow best practices, we have decided to broaden our feed and also include 'newsletters' that did not confirm their subscription.

We also reduced the number of emails from each sender to three (down from five) – this should prevent the corpus from being skewed by a few senders that send emails once a day or more.

SPAM FROM WEB HOSTS

As reported in a post on the *Mailchannels* blog[3], Ken Simpson recently looked into the largest sources of spam, based on emails received at the *CBL*'s spam trap network.

It would be natural to expect those sources all to be Internet service providers, with the top positions occupied by ISPs in developing countries, where many people run cracked and thus unpatched versions of *Windows XP* – a dream for botherders.

However, that is not what Ken found. Instead, the entire top ten consisted of web-hosting companies. Ken is not the first to point to the significant increase in spam sent from web hosts, either compromised or set up by spammers themselves.

[2] Pedants will be keen to point out that this did not verify whether the sender would have started sending emails even if the subscription hadn't been confirmed.

[3] http://www.mailchannels.com/blog/2013/03/worlds-largest-spam-sources-are-all-hosting-companies/

While this is an interesting fact, it doesn't necessarily make it a problem. Spam changes all the time. One country may suddenly find itself topping the spammers' rankings. While this is, of course, a problem for the country's ISPs, regulators and government, for recipients it hardly matters: spam isn't significantly more difficult to filter if it is sent from any particular country.

However, there are some reasons to believe that spam sent from web hosts *is* harder to filter: many such hosts actually send legitimate emails, and if they don't, their 'neighbours' will, making blocking based on the reputation of the sending IP address more difficult. The operating system (typically *Linux*) and the fact that such machines tend to be online 24/7 also makes them look more like typical mail servers.

So we decided to test this.

For the purpose of this research, we defined a 'web host' as an IP address listening for traffic on TCP port 80; we scanned each IP address in the email corpus once per day, using the *nmap* tool to verify whether it was listening on this port.

Of course, machines at hosting providers don't have to be listening on port 80 – they may only listen on port 443 (for HTTPS), or not run a web server at all. On the other hand, the fact that a machine is listening on port 80 doesn't mean that it is a web host: it could be that a router is doing so to allow for remote configuration[4]. Still, we believe that the correlation is strong enough to make this a useful definition for our purposes.

Among the 64,000 spam emails sent as part of this test, we found that 19,449 emails (just over 30%) were sent from web hosts.

We then found that the average email sent from a web host had a probability of 1.04% of being missed by a spam filter, compared to just 0.29% for other spam. This means that being sent from a web host makes a spam email more than 3.5 times more likely to bypass a spam filter.

Of course, 0.29% and 1.04% are both small numbers, but it is good to keep in mind that spam is still sent in very large quantities. On a (very small) campaign of one million emails, this is the difference between fewer than 3,000 and well over 10,000 emails making it to recipients' inboxes. It could be the difference between a spam campaign making a profit or a loss for the spammer.

This difference isn't simply skewed by a small number of emails sent from web hosts that have a very high delivery rate. If we restrict ourselves to those emails blocked by at least three-quarters of all solutions, we still find that spam messages sent from web hosts are more than 3.5 times as likely to make it past the filter.

[4] This is usually a bad idea, especially given the large number of vulnerabilities in routers.

This is not caused by the performance of just a few products, either. While there was significant variation in the relative difficulty products encountered with blocking spam from web hosts, each product[5] had more difficulty with web host spam than with other spam.

Our results don't provide a clear answer as to *why* spam sent via web hosts is more difficult to filter. For the five full solutions where we can measure pre-DATA catch rates (which largely measure the blocking of emails based on IP reputation), we did notice a significant performance difference, but it was no worse than that measured for the full spam catch rate. This means the difference in performance can't simply be attributed to the fact that IP blocking is less effective against web hosts.

In the result tables, we have included products' performance on spam sent from web hosts. This is mainly for the benefit of participating vendors: from a recipient's point of view, there is no reason for a single spam email to be considered worse than any other just because it is sent from a web host. But it might point to something filters can improve upon.

Ideally, of course, such emails wouldn't have been sent in the first place. We hope that this report also helps to raise awareness among hosting companies. During the past decade, many ISPs have made great efforts to reduce the amount of spam sent from their servers. We hope hosting companies will show the same willingness to fight a problem that affects us all.

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 more than 0.2%).

As mentioned above, significant changes have been made to the newsletter corpus. Please keep this in mind when comparing this month's results with those of previous tests.

[5] With the exception of *OnlyMyEmail*, which didn't miss a single spam message in this month's spam corpus.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Bitdefender	13563	0	0.00%	73	63927	99.89%	99.89
ESET	13562	1	0.01%	210	63790	99.67%	99.63
FortiMail	13563	0	0.00%	114	63886	99.82%	99.82
GFI	13561	2	0.01%	525	63475	99.18%	99.11
Halon Security	13556	7	0.05%	431	63569	99.33%	99.07
IBM	13552	11	0.08%	721	63279	98.87%	98.46
Kaspersky LMS	13562	1	0.01%	93	63907	99.85%	99.81
Libra Esva	13562	1	0.01%	84	63916	99.87%	99.83
Mailshell	13562	1	0.01%	163	63837	99.75%	99.71
McAfee Email Gateway	13552	11	0.08%	327	63673	99.49%	99.08
McAfee SaaS	13558	5	0.04%	140	63860	99.78%	99.60
Netmail Secure	13560	3	0.02%	147	63853	99.77%	99.66
NoSpamProxy	13530	33	0.24%	500	63500	99.22%	98.00
OnlyMyEmail	13562	1	0.01%	0	64000	100.00%	99.96
Scrollout	13532	31	0.23%	303	63697	99.53%	98.39
Sophos	13557	6	0.04%	544	63456	99.15%	98.93
SpamTitan	13562	1	0.01%	210	63790	99.67%	99.63
Symantec	13553	10	0.07%	202	63798	99.68%	99.31
The Email Laundry	13547	16	0.12%	1662	62338	97.40%	96.81
ZEROSPAM	13558	5	0.04%	166	63834	99.74%	99.56
Spamhaus ZEN+DBL*	13563	0	0.00%	5219	58781	91.85%	91.85
SURBL*	13561	2	0.01%	38885	25115	39.24%	39.17

* *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: 99.89%
FP rate: 0.00%
Final score: 99.89
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.74%
Newsletters FP rate: 0.0%

As the only product that has participated in every VBSpam test and achieved a VBSpam award on every occasion, *Bitdefender* has good reason to be proud of its VBSpam test record.

But it is not just quantity in which the *Linux*-based product stands out: it has regularly found itself ranked among the better performers in the tests, and in March 2013 achieved its second VBSpam+ award. This month, with a lack of false positives again (even among newsletters), *Bitdefender* ends up with the second highest final score of all products and earns another VBSpam+ award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.67%
FP rate: 0.01%
Final score: 99.63
Project Honey Pot SC rate: 99.68%
Abusix SC rate: 99.61%
Newsletters FP rate: 3.3%

Having only entered the VBSpam test five times so far, *ESET*'s *Mail Security* product has still some way to go before it can match the VB100 track record of the company's anti-virus solution. However, the signs look good for this product to achieve a similar string of awards:

yet again the product performed better than average in both spam catch rate and false positive rate.

A single false positive (an email containing nothing but a link in the body) denied the product its third VBSpam+ award by a whisker, nevertheless *Mail Security* notches up the company's fifth VBSpam award.

Fortinet FortiMail

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Project Honey Pot SC rate: 99.79%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.5%

FortiMail, the hardware appliance made by *Fortinet*, has a VBSpam history going back as far as June 2009. The product would have won no fewer than four VBSpam+ awards, had they been introduced any earlier than March last year.

Since then, *FortiMail* has edged very close to winning a VBSpam+ award several times – and on this occasion it finally managed to do so. The product's high catch rate gives it the fourth highest final score this month.

GFI MailEssentials

SC rate: 99.18%
FP rate: 0.01%
Final score: 99.11
Project Honey Pot SC rate: 99.69%
Abusix SC rate: 96.22%
Newsletters FP rate: 6.3%

Over its two-year VBSpam history, *GFI*'s *MailEssentials* has climbed up the ranks quickly. This month, however, the product's performance took a dive – albeit a relatively minor one. Some difficulties with email from the *Abusix* corpus saw the product's catch rate drop a fair bit.

Of course, that's only one way of looking at things – *MailEssentials* still blocked well over 99 out of 100 spam messages and missed only two legitimate emails, so despite the small drop in performance the product's 13th VBSpam award is well deserved.

Halon Security

SC rate: 99.33%
FP rate: 0.05%
Final score: 99.07
Project Honey Pot SC rate: 99.45%
Abusix SC rate: 98.63%
Newsletters FP rate: 0.5%

In this test *Halon* saw its spam catch rate increase – making up for (most of) the losses it had seen in March. The product's false positive rate increased too, but only a little, and thus *Halon* wins another VBSpam award with a nicely increased final score.

IBM Lotus Protector for Mail Security

SC rate: 98.87%
FP rate: 0.08%
Final score: 98.46
Project Honey Pot SC rate: 98.83%
Abusix SC rate: 99.10%
Newsletters FP rate: 5.8%

IBM was one of the products affected by the hard disk crash mentioned earlier and thus had to be set up again. I was pleasantly surprised, both by how easy it was to set up the virtual machine and by how eager *IBM*'s developers were to help ensure the product was set up correctly. This eagerness paid off, as yet again *IBM*'s catch rate improved significantly.

On the other hand, the product did miss 11 legitimate emails – in English, French and German. Speaking to the developers, I learned that the company blocked most of these emails because they had seen the same senders sending spam. As such, the decision to block is understandable – but it resulted in false positives nevertheless. Despite the relatively high incidence of FPs, *IBM*'s final score increased again and the product earns another VBSpam award.

Kaspersky Linux Mail Security 8.0

SC rate: 99.85%
FP rate: 0.01%
Final score: 99.81
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.85%
Newsletters FP rate: 0.2%

Kaspersky's developers must have worked hard in April, as the *Linux Mail Security* product from the security giant knocked three-quarters off its false negative rate in this test. It only missed one in 688 spam emails.

Unfortunately, a single false positive (somewhat ironically, it was in Russian, and on the subject of *Linux*) prevented the product from achieving a VBSpam+ award, but with the fifth highest final score, *Kaspersky* is well deserving of another VBSpam award.

	Newsletters		Project Honey Pot		Abusix		Web hosts		pre-DATA†		
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	STDev‡
Bitdefender	0	0.0%	49	99.91%	24	99.74%	46	99.76%			0.34
ESET	14	3.3%	174	99.68%	36	99.61%	87	99.55%			0.78
FortiMail	2	0.5%	113	99.79%	1	99.99%	88	99.55%			0.5
GFI	27	6.3%	172	99.69%	353	96.22%	346	98.22%			1.42
Halon Security	2	0.5%	303	99.45%	128	98.63%	182	99.06%			1.03
IBM	25	5.8%	637	98.83%	84	99.10%	332	98.29%			1.42
Kaspersky LMS	1	0.2%	79	99.86%	14	99.85%	40	99.79%			3.63
Libra Esva	16	3.7%	84	99.85%	0	100.00%	71	99.63%	6803	89.37%	0.46
Mailshell	18	4.2%	148	99.73%	15	99.84%	77	99.60%			0.71
McAfee Email Gateway	8	1.9%	281	99.49%	46	99.51%	169	99.13%			0.94
McAfee SaaS	20	4.7%	123	99.78%	17	99.82%	58	99.70%			0.46
Netmail Secure	18	4.2%	130	99.76%	17	99.82%	86	99.56%	6644	89.62%	0.69
NoSpamProxy	39	9.1%	311	99.43%	189	97.97%	270	98.61%	13444	78.99%	1.1
OnlyMyEmail	22	5.1%	0	100.00%	0	100.00%	0	100.00%			0.05
Scrollout	47	10.9%	301	99.45%	2	99.98%	154	99.21%			3.56
Sophos	0	0.0%	523	99.04%	21	99.77%	203	98.96%			1.22
SpamTitan	4	0.9%	209	99.62%	1	99.99%	143	99.26%			0.77
Symantec	1	0.2%	185	99.66%	17	99.82%	121	99.38%			0.68
The Email Laundry	13	3.0%	293	99.46%	1369	85.33%	1434	92.63%	3667	94.27%	2.47
ZEROSPAM	30	7.0%	161	99.71%	5	99.95%	125	99.36%	1575	97.54%	0.65
Spamhaus ZEN+DBL*	0	0.0%	2787	94.90%	2432	73.94%	3028	84.43%	6925	89.18%	6.05
SURBL*	0	0.0%	31662	42.08%	7223	22.60%	12342	36.54%			16.17

* *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. All of the false positives 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.*)

Libra Esva 2.9

SC rate: 99.87%
FP rate: 0.01%
Final score: 99.83
Project Honey Pot SC rate: 99.85%
Abusix SC rate: 100.00%
SC rate pre-DATA: 89.37%
Newsletters FP rate: 3.7%

I met *Libra Esva*'s CTO and main developer at the Infosecurity exhibition in London. It was flattering to learn how much the development team appreciates the VBSpam tests. The tests have always seen *Libra Esva* among the top performers – winning 18 VBSpam awards so far, two of which have been VBSpam+ awards.

A single false positive got in the way of the company earning a third VBSpam+ award, but with the third highest final score, *Libra Esva*'s developers have reason to celebrate another VBSpam award.

Mailshell Mail Agent

SC rate: 99.75%
FP rate: 0.01%

Mailshell Mail Agent contd.

Final score: 99.71
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.84%
Newsletters FP rate: 4.2%

Mail Agent is the new version of *Mailshell*'s SDK, an SMTP proxy to which OEMs and their customers redirect their incoming messages. It applies cloud-based filtering and policies based on user-defined preferences. Compared to the last time *Mailshell* took part in the tests (January 2013), there was a slightly lower catch rate – although the decline was in line with that seen in other products.

The product missed just a single legitimate email, and with a decent final score, earns the VBSpam stamp of approval.

McAfee Email Gateway 7.0

SC rate: 99.49%
FP rate: 0.08%
Final score: 99.08
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.51%
Newsletters FP rate: 1.9%

I was rather pleased with the performance of *McAfee*'s *Email Gateway* appliance in this test: the hardware appliance knocked significant chunks off both its previous false positive rate and its previous false negative rate.

The false positive rate was still a little higher than the average this month, the product having incorrectly blocked 11 legitimate emails – sent in a number of Western languages and including four from a new Venezuelan feed. Nevertheless, *McAfee Email Gateway*'s significantly improved final score earns the company another VBSpam award.

McAfee SaaS Email Protection

SC rate: 99.78%
FP rate: 0.04%
Final score: 99.60
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.82%
Newsletters FP rate: 4.7%

It was an all-round decent performance for *McAfee*, as its cloud-based *SaaS Email Protection* also saw an improvement in both false positives and false negatives. The improvement was even more impressive here, as the cloud-based solution reduced its false positive rate from 0.24% to 0.04%, and its false negative rate by an even bigger ratio.

Unsurprisingly, it gives the product a better-than-average final score – and thus sees *McAfee* regain its VBSpam certification for this product.

Messaging Architects Netmail Secure

SC rate: 99.77%
FP rate: 0.02%
Final score: 99.66
Project Honey Pot SC rate: 99.76%
Abusix SC rate: 99.82%
SC rate pre-DATA: 89.62%
Newsletters FP rate: 4.2%

The *Netmail Secure* virtual appliance was another of the products affected by the hard disk failure and thus had to be set up again. I was rather pleased to find I could do so using an OVF file, which made installation a trivial task.

Thankfully, the product's performance was barely affected: its catch rate was slightly lower, but this was made up for by a decrease in its false positive rate. This resulted in a very respectable final score of 99.66, earning *Messaging Architects* yet another VBSpam award.

Net At Work NoSpamProxy

SC rate: 99.22%
FP rate: 0.24%
Final score: 98.00
Project Honey Pot SC rate: 99.43%
Abusix SC rate: 97.97%
SC rate pre-DATA: 78.99%
Newsletters FP rate: 9.1%

It is always nice when vendors are confident enough about their products' performance to submit them to our tests. *NoSpamProxy* is a solution from *Net At Work*, a German company based in Paderborn. It runs on *Windows* servers (we ran it on *Server 2008 R2*), and set up was easy. *Windows* administrators will find the product very straightforward to use.

As we have seen in the past, developers of products that are new to VBSpam testing sometimes take a little while to find the right settings for the test. After all, much as our set-up resembles a real situation, it remains a test set-up. And thus, while *NoSpamProxy*'s 0.24% false positive rate in particular is rather high, I look forward to seeing whether it can be brought down in the next test – and perhaps the spam catch rate increased too. For now, the product finds itself with a final score of 98.00 – which is just enough to earn it a VBSpam award.

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.

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

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	√	√	√	√		√	
NoSpamProxy	Commtouch			√		√		√
Scrollout	ClamAV			√	√		√	
Sophos	Sophos						√	
SPAMfighter	VIRUSfighter (optional)	√	√	√			√	
SpamTitan	Kaspersky; ClamAV	√	√	√	√		√	√
Symantec	Symantec	√	√	√	√		√	

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

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.01%
Final score: 99.96
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 5.1%

OnlyMyEmail has always had very good catch rates, but in 2013 they have been outstanding: the Michigan-developed hosted solution hasn't missed a single email this year.

Of course, such a performance could be achieved merely by setting a filter to its strictest settings, but the product's consistently low false positive rates show that this isn't what has been done here – *OnlyMyEmail* missed only a single legitimate email in this test, thus doing credit to the company's name. This resulted in a final score of 99.96, the highest this month, and yet another VBSpam award.

Scrollout F1

SC rate: 99.53%
FP rate: 0.23%
Final score: 98.39
Project Honey Pot SC rate: 99.45%
Abusix SC rate: 99.98%
Newsletters FP rate: 10.9%

I was pleased to see the free and open-source product *Scrollout F1* return to the test bench this month:

Complete solutions sorted by final score	
OnlyMyEmail	99.96
Bitdefender	99.89
Libra Esva	99.83
FortiMail	99.82
Kaspersky LMS	99.81
Mailshell	99.71
Netmail Secure	99.66
ESET	99.63
SpamTitan	99.63
McAfee SaaS	99.60
ZEROSPAM	99.56
Symantec	99.31
GFI	99.11
McAfee Email Gateway	99.08
Halon Security	99.07
Sophos	98.93
IBM	98.46
Scrollout	98.39
NoSpamProxy	98.00
The Email Laundry	96.81

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

open-source tools such as *SpamAssassin* (which is used by *Scrollout*) have made important contributions to the fight against spam and it is nice to see that they still do a good job of protecting inboxes and mail servers.

In this test, *Scrollout*'s final score dropped quite a bit from that of its previous entry (in January 2013). This was mostly due to a drop in the catch rate, though the false positive rate remains high too. It would be fair to mention that most of this appears to be caused by the product blocking emails containing what look like links to *Windows* executables, but which are in fact scripts running on *Windows*-based servers – such emails are probably over-represented in our ham corpus. Nevertheless, *Scrollout* wins its second VBSpam award in as many tests.

Sophos Email Appliance

SC rate: 99.15%
FP rate: 0.04%
Final score: 98.93
Project Honey Pot SC rate: 99.04%
Abusix SC rate: 99.77%
Newsletters FP rate: 0.0%

This test saw the catch rate of *Sophos*'s *Email Appliance* drop a little, to just above 99%. No doubt, the product's developers will want to increase that and it is thus interesting to know that, for *Sophos*, spam sent from web hosts was only 1.3 times as hard to block as other spam: a lower factor than for any other product in the test.

On this occasion, *Sophos* missed a number of legitimate emails – six, in fact, although I can understand why two of these, with the subject 'Rolex', triggered the filter. Nevertheless, the product wins the company its 20th VBSpam award in as many tests.

SpamTitan 5.11

SC rate: 99.67%
FP rate: 0.01%
Final score: 99.63
Project Honey Pot SC rate: 99.62%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.9%

I visited *SpamTitan*'s stand at the Infosecurity exhibition in London and noticed the Irish company doing good business. No doubt, the 21 VBSpam awards the company has won have helped to build its reputation as a good spam filter.

This month, there was a bit of a slip in the product's spam catch rate, which dropped to the lowest it has been since September 2010 – though at 99.67% it was still higher than average. With just a single false positive, *SpamTitan*'s false positive rate dropped too, which is of course a good thing – and the product earns its 22nd consecutive VBSpam award.

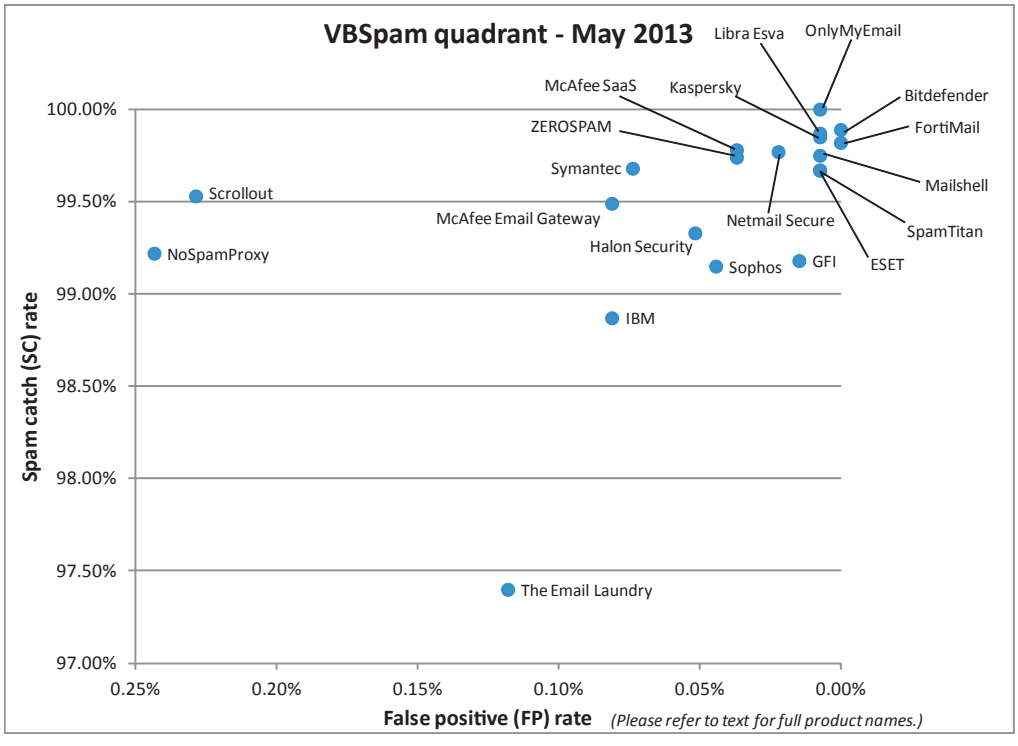
Symantec Messaging Gateway 10.0

SC rate: 99.68%
FP rate: 0.07%
Final score: 99.31
Project Honey Pot SC rate: 99.66%
Abusix SC rate: 99.82%
Newsletters FP rate: 0.2%

This test saw *Symantec Messaging Gateway*'s spam catch rate increase a little – though against this stood an increase in the false positive rate: the product missed ten legitimate emails, all of which were written in English. This resulted in a small drop in final score, but the security giant wins yet another VBSpam award – its 21st – for its virtual anti-spam solution.

The Email Laundry

SC rate: 97.40%
FP rate: 0.12%



The Email Laundry contd.

Final score: 96.81

Project Honey Pot SC rate: 99.46%

Abusix SC rate: 85.33%

SC rate pre-DATA: 94.27%

Newsletters FP rate: 3.0%

Difficulties with the *Abusix* feed, and in particular emails sent from web hosts, saw the catch rate of *The Email Laundry* drop well below 98%, thus automatically denying it a VBSpam award. On top of that, the product had a rather high false positive rate, missing 16 legitimate emails, compared with just one in the previous test. A serious glitch, but after winning a VBSpam award in each of its 17 previous entries, it is far too early to conclude that there is anything wrong with the product. Hopefully this will prove to have been a one-off upset.

ZEROSPAM

SC rate: 99.74%

FP rate: 0.04%

Final score: 99.56

Project Honey Pot SC rate: 99.71%

Abusix SC rate: 99.95%

SC rate pre-DATA: 97.54%

Newsletters FP rate: 7.0%

The vast majority of the 161 spam emails missed by *ZEROSPAM* in this test were sent from web hosts, thus highlighting an area in which some improvement may be made. On the other hand, of the products that were set up to block email pre-DATA, *ZEROSPAM* blocked the most emails based on the SMTP envelope – thus suggesting that the problem with web host spam isn't just the fact that these IP addresses are harder to block.

With five false positives (reduced from seven last time), *ZEROSPAM* saw its final score improve slightly, and thus the product wins its eighth VBSpam award in as many tests.

Spamhaus ZEN+DBL

SC rate: 91.85%

FP rate: 0.00%

Final score: 91.85

Project Honey Pot SC rate: 94.90%

Abusix SC rate: 73.94%

SC rate pre-DATA: 89.18%

Newsletters FP rate: 0.0%

A series of DDoS attacks on *Spamhaus*, affecting its web and email infrastructure but not its blacklists, made the security news headlines recently. The attackers' public face, the now imprisoned Sven Olaf Kamphuis, repeatedly

tried to make the argument that *Spamhaus* is too powerful and has its own agenda. Those who have fallen for his arguments should take note of the fact that, besides blocking close to 92% of all spam, the blacklist provided didn't block a single legitimate email and hasn't blocked any newsletters in this, or any previous VBSpam test.

SURBL

SC rate: 39.24%

FP rate: 0.01%

Final score: 39.17

Project Honey Pot SC rate: 42.08%

Abusix SC rate: 22.60%

Newsletters FP rate: 0.0%

For the seventh test in a row, we have seen a decline in the number of emails that contained a URL on a domain listed on *SURBL*'s blacklist. Of course, this isn't a good thing, but it would be interesting to find out whether this is caused by spammers making their URLs less detectable[6], spammers 'hiding' the URLs via redirects on legitimate sites, or simply the blacklist provider having a hard time catching up with new spam. Nevertheless, with close to 40% of emails blocked based on the URLs they contain alone – and just two false positives on the same domain – *SURBL* would be a valuable addition to many a filter.

CONCLUSION

It was good to see the decline in spam catch rates we reported earlier this year halted and, in fact, see a small improvement in the average scores. But these tests aren't just intended to show which spam filters do a better job at directing email traffic: where possible, we like to highlight areas in which products can improve their performance.

Recent reports showed that spam filters perform significantly worse on phishing emails and this month's report shows that spam sent from web hosts poses a bigger challenge for most filters. We hope that the information provided in this test will see both spam filters and hosting providers take on the battle against this particular kind of spam.

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

[6] The (public) script we use to detect URLs in email only does some basic decoding of the content. A more thorough search for URLs would perhaps have given higher catch rates, though it could also lead to strings incorrectly seen as URLs, thus leading to false positives.

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/