MAY 2012

virus BULLETIN

Fighting malware and spam

MAY 2012 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

Spam levels are falling. There are few statistics that all anti-spam companies agree on, but this is one of them. Ever since the takedown of the *McColo* rogue ISP at the end of 2008, the steady growth in spam levels has ceased. Rather, we have seen an overall decline in spam – albeit one with the occasional sharp increase – and, today, spam levels are generally believed to be about half what they once were.

This is good news. One of the most troublesome effects of spam is that it uses up network resources. Even taking into account the fact that a lot of spam is blocked early during the SMTP transaction, spam once effectively threatened to perform a denial-of-service attack on parts of the Internet.

But volume is not the only problem. There is also the risk of recipients being tricked into believing spam messages are genuine; of unfiltered spam clogging up recipients' inboxes; and of malicious attachments making it into a corporate network. It is here that spam filters' catch rates become important. These catch rates dropped significantly in the last VBSpam test, and failed to recover ground in this test.

However, spam catch levels are not low *per se*: in this test, the average complete solution blocked 99.65% of all spam – which means that, on average, 1 in 286 emails would have made it to a user's inbox. That may not sound like a number to worry about. However, it is good to keep in mind that all of the spam used in this test was sent to spam traps. As such, it is representative of the vast majority of spam, but our experience[1] (and that of others) has shown that non-spam-trap spam (i.e. the spam that only ends up in real users' mailboxes) is a lot more difficult to filter. Therefore, the performance of all products can be expected to be slightly poorer in real-world use than under test conditions. For this reason, the actual numbers in this test should be considered only within the context of the test itself.

As mentioned, most products saw a significant drop in performance in the last test, and while some products saw their spam catch rates rise again this month, others saw it drop even further. I would not want to go as far as to say that the current spam catch rates are worrying in themselves (the vast majority of spam is still being caught), but they do signal a trend towards spam that, for one reason or another, is more difficult to block.

19 complete solutions took part in this month's test, each of which won a VBSpam award. One of the two participating partial solutions (DNS blacklists) also achieved a VBSpam award, but on this occasion, none of the products met the requirements for a VBSpam+ award.

[1] In early VBSpam tests, we included a real-time feed of unfiltered spam sent to existing *Virus Bulletin* addresses. Performance on these emails was significantly poorer than on spam-trap spam.

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. Four 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 *SuSE Linux Enterprise Server 11*; 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 97:

ISSN 1749-7027

SC - (5 x FP) ≥ 97

To earn a VBSpam+ award, products must combine a spam catch rate of 99.50% or higher with a zero false positive rate.

THE EMAIL CORPUS

The test ran for 16 consecutive days, from 12am GMT on Saturday 14 April 2012 until 12am GMT on Monday 30 April 2012.

The corpus contained 253,390 emails, 242,703 of which were spam. Of these, 147,989 were provided by *Project Honey Pot*, and 94,714 were provided by *Spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 10,486 legitimate emails ('ham') and the remaining 201 emails, which were all legitimate newsletters.

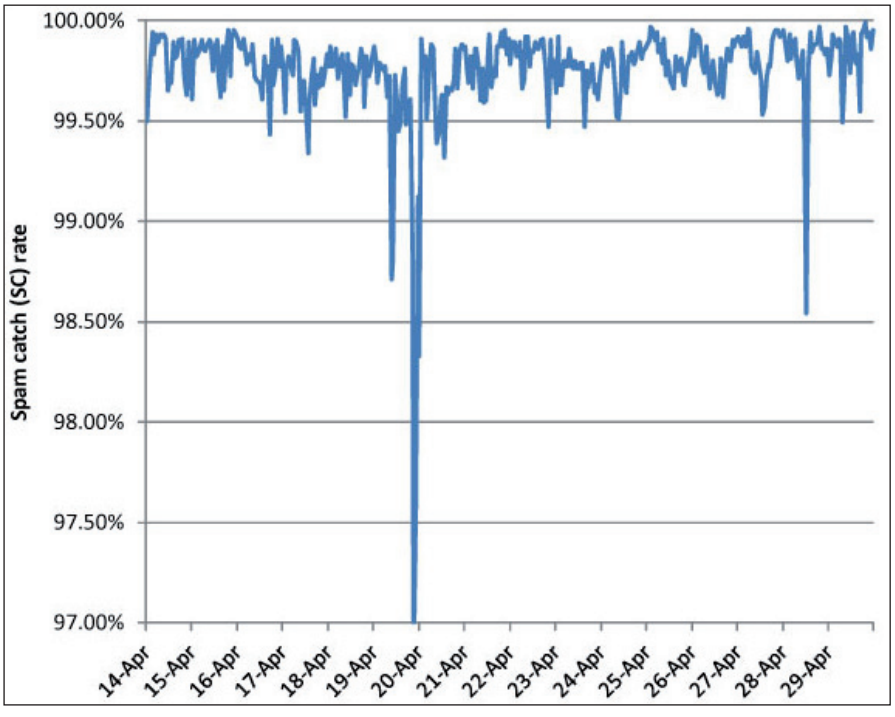


Figure 1: Spam catch rate of all complete solutions throughout the test period.

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.

As in the previous test, the average spam catch rate dropped below 99% several times, most strikingly on the evening of 19 April, when not even 97% of spam was caught. The various dips were all caused by German-language spam advertising (fake) Viagra – which is still a popular subject among spammers.

Looking at the spam feed, we continued to see a lot of emails claiming to come from popular websites: *PayPal*, *Twitter*, *LinkedIn* etc. In previous reports, we have remarked how, rather than linking to phishing sites, these emails linked to fake pharmacy websites. A new, and slightly worrying trend is for these emails to link to websites containing exploit kits[2], which makes the click itself harmful, even if the recipient subsequently realizes that the email was fake.

This may hint at further differentiation in the sending of spam. It has long been known that the spam infrastructure (the botnets and sometimes fake accounts sending spam) is run by criminals who are hired by other criminals who manage the (possibly non-existent) services advertised in the emails[3]. This new trend suggests the content of the emails is part of the 'deal'. Popular websites are used to lure people into clicking, and they are then redirected to whatever destination the criminals are paid to send them to.

This month also saw a further increase in the size of the ham corpus, which now contains well over 10,000 emails.

One worrying trend we have seen in this corpus is an increase in spam sent from compromised webmail accounts. These emails tend to be sent to users in the sender's address book, which increases both the chances of them making it through a spam filter and their chances of being opened by the recipient. Moreover, most of these emails contain little more than a URL. As spammers are increasingly using compromised legitimate websites for these landing URLs, this makes it hard for filters to recognize them. This kind of spam is also a lot less likely to be sent to spam traps.

We have, of course, excluded these emails from the ham corpus. Due to the low absolute number of these emails (18, or about 0.17% in this test), we haven't used them in the results, but we wanted to highlight this trend anyway. Should the trend continue, and should we be able to get hold of a larger number of such emails, we will look into including them in the results.

[2] See for instance http://www.virusbtn.com/news/2012/05_02.xml.

[3] This is not unique to spam. The vast majority of legitimate newsletters are sent by email service providers (ESPs), rather than by the companies advertised in the emails.

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.

The 'false negative rate', mentioned several times in the text below, is the complement of the spam catch rate: the percentage of spam messages that were not blocked. It can be computed by subtracting the SC rate from 100%.

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 0.5%).

AnubisNetworks Mail Protection Service

SC rate: 99.84%
FP rate: 0.20%
Final score: 98.84
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.5%

AnubisNetworks' spam catch rate dropped a little in this test, but remained fairly high. This came as little surprise, since the product has performed well in its ten previous tests. What was of slightly more concern was the false positive rate: the product missed 21 legitimate emails – more than most other products and (perhaps more strikingly) more than it has missed in all of the previous tests put together. Since it usually performs so much better in this area, we are inclined to believe that this is a temporary glitch. *AnubisNetworks* still earns a VBSpam award, and hopefully will return to its usual performance levels in the next test.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.86%
FP rate: 0.01%
Final score: 99.81
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.72%
Newsletters FP rate: 0.0%

Bitdefender is the only product to have participated in all 19 VBSpam tests – and it has won a VBSpam award in all of them. For this test, the product was upgraded to version 3.1.2, which can be controlled via a web GUI. More importantly, however, we saw a stunning improvement in performance, with the product's spam catch rate increasing by almost a percentage point. The one missed legitimate email is the only fly in the ointment – preventing the product from winning a VBSpam+ award – but the final score that wins *Bitdefender* its 19th VBSpam award is the fifth highest this month.

CronLab Anti-Spam

SC rate: 99.15%
FP rate: 0.00%
Final score: 99.15
Project Honey Pot SC rate: 98.93%
Abusix SC rate: 99.50%
Newsletters FP rate: 0.0%

Someone who receives over 10,000 legitimate emails in a year (remember that this test's ham corpus included close to 10,500 emails) receives more than 27 emails per day, including weekends and holidays. That is a lot, and those who receive as many emails will probably be used to occasionally having to fish one out of the spam folder. Thus it is impressive that *CronLab* blocked none of the legitimate emails – the only complete solution to manage a zero false positive rate this month. The spam catch rate was a little too low for a VBSpam+ award, but with well over 99% it was still impressive. The company easily earns its second VBSpam award.

Fortinet FortiMail

SC rate: 99.86%
FP rate: 0.01%
Final score: 99.81
Project Honey Pot SC rate: 99.83%
Abusix SC rate: 99.90%
Newsletters FP rate: 0.0%

Like many products, *FortiMail* suffered a drop in performance in the last test. It was pleasing, therefore, to see its performance pick up again in this test – which is not something that can be said for all products. With 99.86% of spam blocked, *FortiMail* had one of the higher spam catch rates, while just a single legitimate email got in the way of the product winning a VBSpam+ award. The company's 18th VBSpam award, with the fourth highest final score, is very well deserved.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
AnubisNetworks	10464	21	0.20%	378	242325	99.84%	98.84
Bitdefender	10485	1	0.01%	348	242355	99.86%	99.81
CronLab	10486	0	0.00%	2058	240645	99.15%	99.15
Fortinet FortiMail	10485	1	0.01%	339	242364	99.86%	99.81
GFI	10476	10	0.10%	487	242216	99.80%	99.32
Halon Security	10481	5	0.05%	1675	241028	99.31%	99.07
IBM	10479	7	0.07%	592	242111	99.76%	99.42
Libra Esva	10484	2	0.02%	77	242626	99.97%	99.87
McAfee Email Gateway	10469	11	0.10%	691	242012	99.72%	99.19
McAfee SaaS	10480	6	0.06%	290	242413	99.88%	99.59
M+Guardian	10440	31	0.30%	873	241830	99.64%	98.16
OnlyMyEmail	10484	2	0.02%	9	242694	99.996%	99.90
Sophos	10483	3	0.03%	693	242010	99.71%	99.57
SPAMfighter	10473	13	0.12%	2253	240450	99.07%	98.45
SpamTitan	10483	3	0.03%	183	242520	99.92%	99.78
Spider	10481	5	0.05%	962	241741	99.60%	99.37
Symantec	10482	4	0.04%	651	242052	99.73%	99.54
Vamsoft ORF	10485	1	0.01%	3309	239394	98.64%	98.59
ZEROSPAM	10484	2	0.02%	207	242496	99.91%	99.82
Spamhaus ZEN+DBL*	10485	1	0.01%	4040	238663	98.34%	98.29
SURBL*	10486	0	0.00%	56839	185864	76.58%	76.58

* 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.*)

GFI MailEssentials

SC rate: 99.80%
FP rate: 0.10%
Final score: 99.32
Project Honey Pot SC rate: 99.75%
Abusix SC rate: 99.88%
Newsletters FP rate: 1.0%

While a few other products have versions for *Microsoft Exchange*, *GFI*'s *MailEssentials* is the only product currently in our test that makes use of this popular MTA. While the MTA may have the reputation of being a little difficult to manage, we are glad to report that since *MailEssentials* joined the test more than a year ago, both product and MTA have run smoothly and not given us any cause to look into them. We are also pleased to report that *GFI*'s spam catch rate increased a little compared to the previous test – though the false positive rate also did, which led to a slight decrease in final score. Still, the product meets the requirements to win its seventh VBSpam award in as many tests.

Halon Security

SC rate: 99.31%
FP rate: 0.05%
Final score: 99.07
Project Honey Pot SC rate: 99.06%
Abusix SC rate: 99.71%
Newsletters FP rate: 0.0%

The version of *Halon Security* that we have run in our test for over a year is a virtual server – probably the easiest format to run in a test set-up – but it should be noted that the Swedish company also offers a hardware appliance and a hosted solution, thus catering for a range of different customers. Though the product saw its spam catch rate drop a little and its false positive rate increase slightly, it easily wins its eighth VBSpam award in as many tests.

IBM Lotus Protector for Mail Security

SC rate: 99.76%
FP rate: 0.07%
Final score: 99.42
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.79%
Newsletters FP rate: 0.0%

It is always pleasing to see products improve on all fronts: *IBM*'s virtual anti-spam solution combined a small increase in spam catch rate with a drop in false positive rate. (And the newsletter FP rate was already at zero.) This earns the industry giant another VBSpam award (its sixth in a row), once again confirming that it can be trusted to look after your mail servers.

Libra Esva 2.6

SC rate: 99.97%
FP rate: 0.02%
Final score: 99.87
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.96%
SC rate pre-DATA: 97.50%
Newsletters FP rate: 0.0%

Libra Esva has achieved the highest final score twice in a row and in the last test it was the only product to win the newly introduced VBSpam+ award. It was not able to repeat those achievements this time around, but the difference in performance was tiny. With two false positives and the second highest spam catch rate the Italian product achieved the second highest final score overall, and earns its 13th VBSpam award.

McAfee Email Gateway 7.0

SC rate: 99.72%
FP rate: 0.10%
Final score: 99.19
Project Honey Pot SC rate: 99.66%
Abusix SC rate: 99.80%
Newsletters FP rate: 1.5%

A merger of two previously tested *McAfee* appliances, *McAfee Email Gateway 7.0* debuted in the last test. It had no difficulty winning a VBSpam award on that occasion, and it was pleasing to see it perform even better this time, improving both its spam catch rate and its false positive rate. The product earns its second VBSpam award.

McAfee SaaS Email Protection

SC rate: 99.88%
FP rate: 0.06%
Final score: 99.59
Project Honey Pot SC rate: 99.85%
Abusix SC rate: 99.93%
Newsletters FP rate: 4.0%

McAfee's hosted solution stood out a little in the previous test as the product with the highest false positive rate. We were thus pleasantly surprised to see the false positive rate drop significantly, to a little below average. There was also a small drop in spam catch rate, but it was still significantly better than average, thus positioning the product close to the top right-hand corner of the VBSpam quadrant. The final score was also better than average and earns the hosted solution its sixth VBSpam award.

Messaging Architects M+Guardian

SC rate: 99.64%
FP rate: 0.30%
Final score: 98.16
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.87%
SC rate pre-DATA: 97.11%
Newsletters FP rate: 1.0%

The *M+Guardian* virtual appliance from *Messaging Architects* had a higher false positive rate than any other product – it incorrectly blocked more than two dozen legitimate emails. Moreover, the product's spam catch rate dropped, resulting in a somewhat disappointing performance overall. Nevertheless, the product's final score exceeded the level required to qualify *M+Guardian* for its eighth VBSpam award – we hope that its developers will have made some improvements in time for the next test.

	Newsletters		Project Honey Pot		Abusix		pre-DATA†		
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	STDev‡
AnubisNetworks	1	0.5%	281	99.81%	97	99.90%			0.28
Bitdefender	0	0.0%	83	99.94%	265	99.72%			0.50
CronLab	0	0.0%	1583	98.93%	475	99.50%			1.22
Fortinet FortiMail	0	0.0%	247	99.83%	92	99.90%			0.33
GFI	2	1.0%	369	99.75%	118	99.88%			0.30
Halon Security	0	0.0%	1396	99.06%	279	99.71%			0.68
IBM	0	0.0%	396	99.73%	196	99.79%			0.42
Libra Esva	0	0.0%	37	99.97%	40	99.96%	6069	97.50%	0.11
McAfee Email Gateway	3	1.5%	497	99.66%	194	99.80%			0.42
McAfee SaaS	8	4.0%	219	99.85%	71	99.93%			0.24
M+Guardian	2	1.0%	749	99.49%	124	99.87%	7018	97.11%	0.34
OnlyMyEmail	4	2.0%	3	99.998%	6	99.99%			0.02
Sophos	1	0.5%	554	99.63%	139	99.85%			0.40
SPAMfighter	5	2.5%	1626	98.90%	627	99.34%			1.10
SpamTitan	3	1.5%	109	99.93%	74	99.92%			0.21
Spider	1	0.5%	770	99.48%	192	99.80%			0.53
Symantec	0	0.0%	423	99.71%	228	99.76%			0.57
Vamsoft ORF	0	0.0%	2841	98.08%	468	99.51%			1.05
ZEROSPAM	16	8.0%	88	99.94%	119	99.87%	5319	97.81%	0.29
Spamhaus ZEN+DBL*	0	0.0%	3036	97.95%	1004	98.94%	6824	97.19%	1.27
SURBL*	0	0.0%	51192	65.41%	5647	94.04%			10.37

* *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 *ZEROSPAM* occurred pre-DATA; all the other 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.*)

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.99%
FP rate: 0.02%
Final score: 99.90
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.99%
Newsletters FP rate: 2.0%

OnlyMyEmail has a reputation to live up to in these tests, and it didn't disappoint this time. As on previous occasions, it missed strikingly few spam messages – it failed to block just nine out of more than 240,000 messages. This can be achieved relatively easily simply by using a very strict filter, but the fact that only two legitimate emails were blocked proves that this was not the case. The product's final score came to 99.90 – the highest this month – and *OnlyMyEmail* deservedly wins its tenth VBSpam award.

Hosted solutions	Anti-malware	Multiple MX-records	Multiple locations
AnubisNetworks	ClamAV	√	√
CronLab	ClamAV, Bitdefender optional	√	√
McAfee SaaS	McAfee	√	√
OnlyMyEmail	Proprietary (optional)	√	√
Spider	F-Prot, ClamAV, proprietary; others optional	√	√
ZEROSPAM	ClamAV	√	√

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

Local solutions	Anti-malware	Interface			
		CLI	GUI	Web GUI	API
Bitdefender	Bitdefender	√		√	
FortiMail	Fortinet	√		√	
GFI	N/A		√		
Halon Security	Commtouch, Kaspersky, ClamAV	√		√	√
IBM	Sophos	√		√	
Libra Esva	ClamAV; others optional			√	
M+Guardian	Proprietary	√			
McAfee Email Gateway	McAfee	√	√	√	
Sophos	Sophos			√	
SPAMfighter	VIRUSfighter (optional)			√	
SpamTitan	Kaspersky, ClamAV	√		√	√
Symantec	Symantec	√		√	
Vamsoft ORF	optional		√		

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

Sophos Email Appliance

SC rate: 99.71%
FP rate: 0.03%
Final score: 99.57
Project Honey Pot SC rate: 99.63%
Abusix SC rate: 99.85%
Newsletters FP rate: 0.5%

Sophos's *Email Appliance* was one of several products whose false negative rate doubled in the last test, so it was nice to see it bounce back this month with a significantly improved catch rate. What's more, its false positive rate decreased, thus resulting in an increased final score and the appliance's 14th consecutive VBSpam award.

SPAMfighter Mail Gateway

SC rate: 99.07%
FP rate: 0.12%
Final score: 98.45
Project Honey Pot SC rate: 98.90%
Abusix SC rate: 99.34%
Newsletters FP rate: 2.5%

The *SPAMfighter* product we have been testing for well over two years uses its own MTA, but the same engine is used in another product that works together with *Microsoft Exchange*. In this test, the Danish solution missed more spam than in the last test, and also blocked more legitimate emails – thus resulting

Products ranked by final score*	
OnlyMyEmail	99.90
Libra Esva	99.87
ZEROSPAM	99.82
FortiMail	99.81
BitDefender	99.81
SpamTitan	99.78
McAfee SaaS	99.59
Sophos	99.57
Symantec	99.54
IBM	99.42
Spider	99.37
GFI	99.32
McAfee Email Gateway	99.19
CronLab	99.15
Halon Security	99.07
AnubisNetworks	98.84
Vamsoft ORF	98.59
SPAMfighter	98.45
M+Guardian	98.16

*Complete solutions only.
(*Please refer to text for full product names.*)

in a decreased final score, although one that still earns it a VBSpam award. We hope to see *SPAMfighter* come back stronger in the next test.

SpamTitan

SC rate: 99.92%
FP rate: 0.03%
Final score: 99.78
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.92%
Newsletters FP rate: 1.5%

SpamTitan's performance this month was barely any different from in the previous test. That is a good thing, as the solution continues to have a very high spam catch rate and a low false positive rate: missing three legitimate emails is not a significant problem. With a slightly improved final score, the Irish virtual solution wins its 16th VBSpam award.

Spider Cloud MailSecurity

SC rate: 99.60%
FP rate: 0.05%
Final score: 99.37
Project Honey Pot SC rate: 99.48%
Abusix SC rate: 99.8%
Newsletters FP rate: 0.5%

Spider Cloud MailSecurity suffered from a higher than average false positive rate in the last test and it was nice to see that decrease significantly this time. The spam catch rate dropped a little as well, but not enough to prevent the final score from improving, indicating an improved experience for the product's users. The product's sixth VBSpam award is well deserved.

Symantec Messaging Gateway 9.5

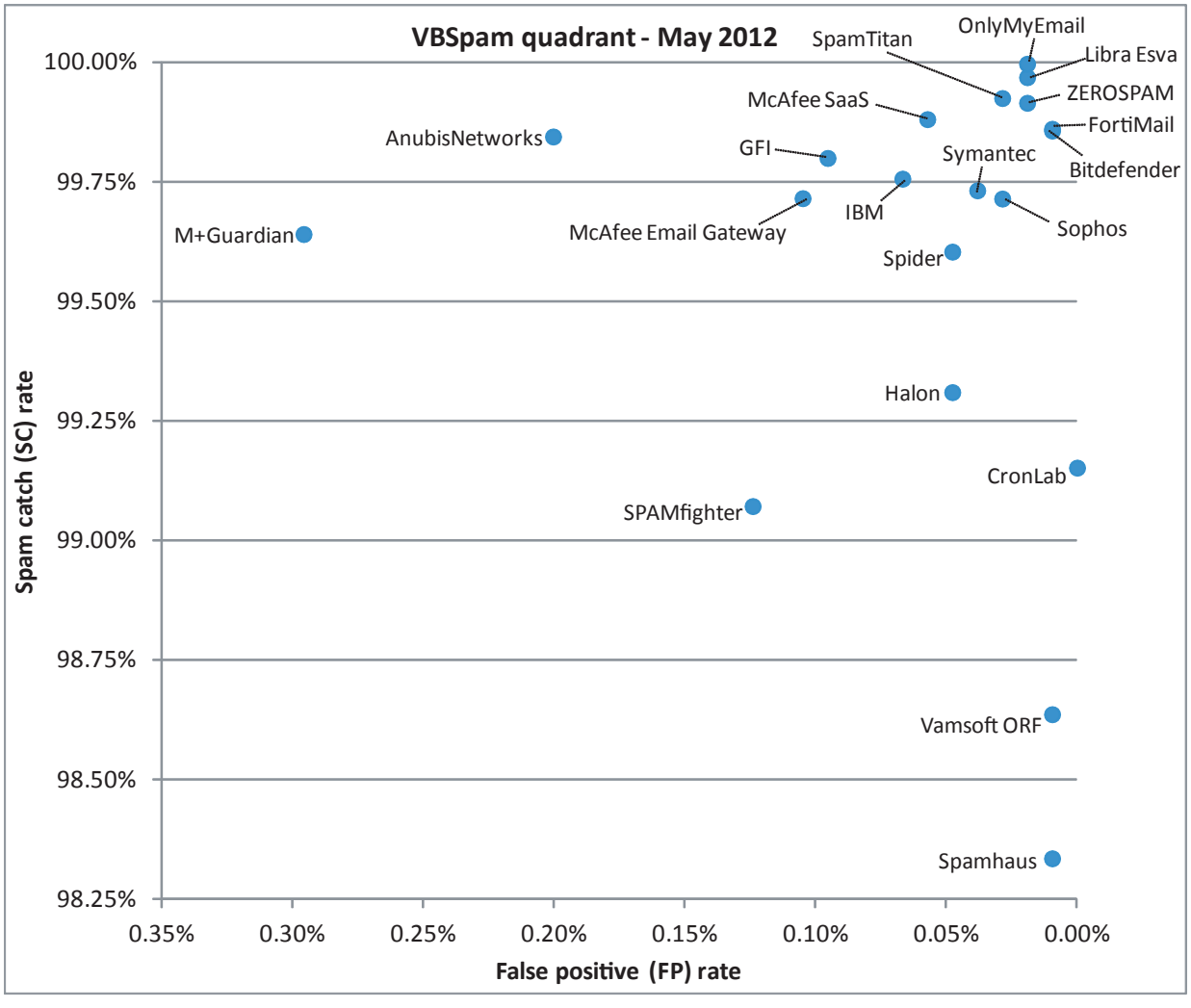
SC rate: 99.73%
FP rate: 0.04%
Final score: 99.54
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.76%
Newsletters FP rate: 0.0%

Symantec was one of several products to see a slight drop in its spam catch rate in this test, but thankfully this is only half of the picture. The product also blocked fewer legitimate emails in a larger ham corpus, and as a result it saw a small improvement in its final score. The security giant receives its 15th consecutive VBSpam award.

Vamsoft ORF

SC rate: 98.64%
FP rate: 0.01%
Final score: 98.59
Project Honey Pot SC rate: 98.08%
Abusix SC rate: 99.51%
Newsletters FP rate: 0.0%

The last time *Vamsoft ORF* missed a legitimate email was in September last year, so although it was a little disappointing to see it miss one in this test, the company can still pride itself on being exceptionally good at recognizing legitimate email. The spam catch rate was a little lower than that of most other solutions, but not enough to jeopardize the product's 13th VBSpam award.



ZEROSPAM

SC rate: 99.91%
FP rate: 0.02%
Final score: 99.82
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.87%
SC rate pre-DATA: 97.81%
Newsletters FP rate: 8.0%

This was *ZEROSPAM*'s second visit to the VBSpam test bench, having made an impressive debut in the last test. The product's spam catch rate increased even further this month, while its false positive rate dropped – just two legitimate emails were missed. This resulted in the third highest final score and earned the product its second VBSpam award.

Spamhaus ZEN+DBL

SC rate: 98.34%
FP rate: 0.01%
Final score: 98.29
Project Honey Pot SC rate: 97.95%
Abusix SC rate: 98.94%
SC rate pre-DATA: 97.19%
Newsletters FP rate: 0.0%

The drop in spam catch rate in the last test was most striking in *Spamhaus* – a fact which hinted at spammers increasing their use of compromised legitimate mailers and domains to send their spam: the IP- and domain-based blacklist cannot block these. It was nice to see the product's spam catch rate improve again this month – it blocked well over 98% of all spam, more than 97% of

which was purely based on the sender's IP address. The product missed one legitimate email – its first false positive in almost a year – based on a domain in an email signature. However, that was not enough to prevent *Spamhaus* from winning another VBSpam award.

SURBL

SC rate: 76.58%
FP rate: 0.00%
Final score: 76.58
Project Honey Pot SC rate: 65.41%
Abusix SC rate: 94.04%
Newsletters FP rate: 0.0%

SURBL's domain-based blacklist blocked well over three out of four emails in our spam corpus based on the domains in header and body alone, which is a huge increase compared to the last test. As mentioned, spammers are increasingly using legitimate compromised domains as an initial landing page, which makes the task of distinguishing the good from the bad domains far from trivial. The fact that yet again no legitimate email was blocked should therefore be applauded.

CONCLUSION

After the significant drop in spam catch rates seen in the last test, we had hoped to see an increase this month. Unfortunately, we did not see one. (Pedants will rightly point out that if we only look at products that took part in both tests, the average catch rate increased by 0.03% – but that is nowhere near enough to make up for the previous drop.) With all the caveats mentioned in the introduction, it does look as if spammers – hit hard in their ability to send large volumes of spam – have improved the 'quality' of the spam they send, making it harder to block.

The increasing use of legitimate sources to send spam makes it more difficult to distinguish between legitimate and illegitimate email, but thankfully we did not see a rise in false positive rates, and most products missed few of the over 10,000 legitimate emails in this test. Still, all but one full solution have something to improve here too.

In the next VBSpam report we hope to include a few more quantitative checks which, due to a tight schedule, didn't make it into this month's report.

The next VBSpam test will run in June 2012, with the results scheduled for publication in July. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Web Developer: Paul Hettler

Consulting Editors:
Nick FitzGerald, *Independent consultant, NZ*
Ian Whalley, *Google, USA*
Richard Ford, *Florida Institute of Technology, US*

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/