NOVEMBER 2013

virus BULLETIN

Covering the global threat landscape

NOVEMBER 2013 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

All malware is bad, but some malicious programs are worse than others. CryptoLocker, which has been making the headlines since the late summer, is particularly nasty.

It locks up all the important files on your computer using strong encryption and demands a ransom of hundreds of dollars in exchange for the private key that is required to break the encryption. No one has been able to find a weakness in the malware and, although most people keep offline back-ups these days, if you don't, you either have to pay the ransom or forgo your data.

CryptoLocker spreads via spam.

Having spent half a decade looking at a great many spam filters, I tend to believe that we're doing particularly well when it comes to fighting spam – and that spam isn't the biggest problem with email[1]. The results of the VBSpam tests, which show that email security products tend to do a rather good job of preventing spam from reaching users' inboxes, reaffirm that belief.

But it only takes one email to slip through the filter, and one user to be tricked into believing a message is genuine (or who simply clicks a link or opens an attachment by accident) for an organization to be exposed to a nasty malware infection.

This is why it is important that we run these tests – and why we will continue to make a distinction between products that block, say, 99.3% of spam and those that block 99.7% of spam.

In this test, all but one of the 19 full solutions we tested achieved a VBSpam award. No fewer than eight of these managed to avoid false positives completely, while keeping their catch rate above 99.5% – earning them each a VBSpam+ award.

[1] http://www.virusbtn.com/virusbulletin/archive/2013/11/vb201311-comment.

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). Four products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. As different products have different hardware requirements – not to mention those running on their own hardware, or those running in the cloud – there is little point comparing the memory, processing power or hardware the products were provided with; we followed the developers' requirements and note that the amount of email we receive is representative of that received by a smaller organization.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the 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 days, from 12am on Saturday 19 October to 12am on Monday 4 November.

Some technical issues on our side led to there being two gaps in the final corpus. The first of these, on 25 October, was caused by a failed sending daemon. Once this had been discovered, it was decided that the emails that had

ISSN 1749-7027

been waiting in the queue for hours should be excluded from the test. Four days later, a programming error led to the loss of several hours' worth of emails that had been sent through the participating products.

Neither of these issues affected the remainder of the emails, nor did they affect any of the participating products. We thus ended up with a corpus of 94,675 emails, 81,313 of which were spam. 71,479 of the spam emails were provided by *Project Honey Pot*, with the remaining 9,834 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 13,016 legitimate emails ('ham') and 346 newsletters.

As always, new sources were added for the latter two kinds of email, thus creating a broader corpus of legitimate messages.

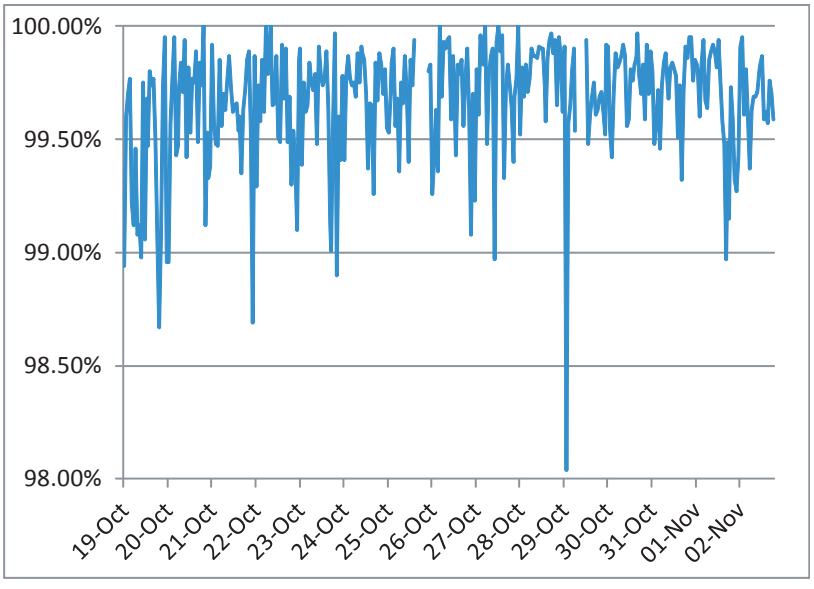


Figure 1: Spam catch rate of all complete solutions throughout the test period.

As in the last test, those emails in the spam corpus that were marked as legitimate by at least half the products *and* did not appear to be real spam were excluded from the corpus. This meant that products that made the most natural decision on, say, *Facebook* invites, wouldn't be penalized for doing so.

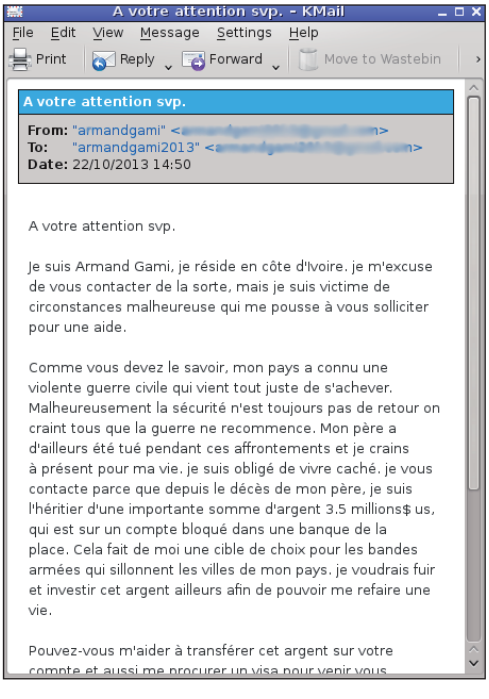
Figure 1 shows the catch rate of all full solutions throughout the test. To avoid the average being skewed by poorly performing products, the highest and lowest catch rates have been excluded for each hour.

Compared with a similar graph plotted in the last test, there isn't a significant difference – the downwards spike that can be seen on 29 October was caused by the fact that during this hour relatively few emails were sent, thus giving a single email a lot of weight towards the average.

Of the 81,313 spam emails in the corpus, 78,575 were blocked by all participating full solutions. That is 96.6 per cent of the spam emails. We acknowledge that a disproportionate number of spam emails used in the VBSpam tests are those that are easier to block (and as such, the percentages given in this test should always be considered *in the context* of the test) – nevertheless, this is an impressive statistic.

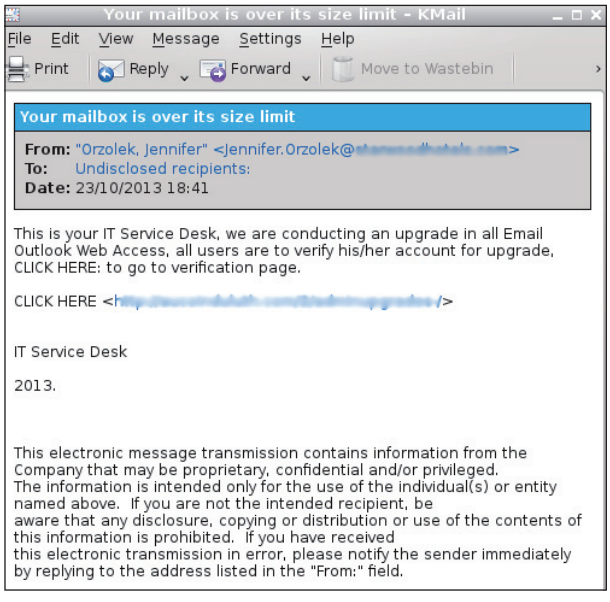
When you also consider the fact that there are very few electronic mailboxes that aren't protected by any kind of anti-virus software, it suggests that stories about spam emails sent out in the millions may be missing the point somewhat – most of the emails get blocked anyway. What matters is: what are the emails that are being missed?

The 'winner' in that respect in this test was a French 419 scam. Only four of the 19 participating full solutions blocked this email, despite the fact that a sob story, combined with an offer of a percentage of a large sum of money, is an obvious and well-known form of spam:



Two further instances of this email were sent the next day, when only one more product blocked them. 419 scams, particularly those in non-English languages, tend to be difficult to block.

More worryingly, there were a number of phishing emails that were missed by at least half the products. It only takes one employee to believe that their mailbox is indeed 'over its size limit' and to click on the 'verification' link for an 'upgrade' for an entire organization to be compromised:



Perhaps most surprising were three emails that were missed by eight or nine participants – the subject line of which had helpfully been tagged (presumably by an outbound spam filter) with the words 'suspected spam'.

On a more positive note, none of the 100 'most difficult' emails in the corpus (determined by the number of products that failed to block them) contained a malicious attachment. Although this test doesn't look at the blocking of malicious attachments in itself, it was pleasing to see that this kind of spam, which has seen a resurgence in recent years, is not reaching users' inboxes in very large numbers.

RESULTS

Axway MailGate 5.3.1

SC rate: 99.48%
FP rate: 0.15%
Final score: 98.71
Project Honey Pot SC rate: 99.49%
Abusix SC rate: 99.37%
Newsletters FP rate: 6.4%

Axway, a global company headquartered in Phoenix, Arizona, calls itself 'a market leader in governing the flow of data'. Email is one of these data flows, and it certainly needs to be 'governed' – for which purpose *Axway* provides the *MailGate* product. *MailGate* comes as a hardware appliance and a virtual appliance; we tested the latter.

Installation and set-up of the product was a smooth process. Once set up, the product can be managed using a web interface, which was comfortable to work with. It provides a lot of information on the status of both the mail stream and the product itself, and gives plenty of opportunity to fine-tune the product.

Other than customizing it for our environment, we used the product's default settings. Using these, *MailGate* missed just over one in 200 spam emails – mostly written in non-Latin character sets. The false positive rate was relatively high, but that can probably be attributed to the fact that this was *Axway*'s first VBSpam test. In any case, *Axway* earns a VBSpam award on its debut.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.94%
Newsletters FP rate: 0.3%

Just 29 spam emails were missed by *Bitdefender* in this test, thus increasing its spam catch rate to an impressive 99.96%. Once again, the solution correctly identified all of the legitimate emails, which means that it earns a VBSpam+ award, in doing so completing an unbroken string of VBSpam+ awards in 2013. It also remains the only product never to have missed either a VBSpam test or a VBSpam award.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.52%
FP rate: 0.00%
Final score: 99.52
Project Honey Pot SC rate: 99.60%
Abusix SC rate: 98.98%
Newsletters FP rate: 2.6%

ESET's *Mail Security* product narrowly missed out on a VBSpam+ award in the last test. On this occasion, there was a drop in the product's spam catch rate (we couldn't spot a clear trend among the almost 400 emails that were missed), but since it remained (just) above 99.5%, and there were no false positives, we were pleased to be able to give *ESET* its fourth VBSpam+ award.

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway MailGate	12996	20	0.15%	424	80889	99.48%	98.71
Bitdefender	13016	0	0.00%	29	81284	99.96%	99.96
ESET	13016	0	0.00%	389	80924	99.52%	99.52
FortiMail	13015	1	0.01%	102	81211	99.87%	99.83
GFI	13016	0	0.00%	363	80950	99.55%	99.55
Halon Security (ESXi)	13010	6	0.05%	308	81005	99.62%	99.39
IBM	13000	16	0.12%	444	80869	99.45%	98.84
Kaspersky LMS	13016	0	0.00%	69	81244	99.92%	99.92
Libra Esva	13016	0	0.00%	39	81274	99.95%	99.95
McAfee Email Gateway	13002	14	0.11%	379	80934	99.53%	98.99
McAfee SaaS	13013	3	0.02%	696	80617	99.14%	99.02
Net At Work NoSpamProxy	12966	50	0.38%	319	80994	99.61%	97.69
Netmail Secure	13016	0	0.00%	269	81044	99.67%	99.67
OnlyMyEmail	13014	2	0.02%	0	81313	100.00%	99.92
Scrollout	12991	25	0.19%	266	81047	99.67%	98.71
Sophos	13010	6	0.05%	281	81032	99.65%	99.42
SpamTitan	13016	0	0.00%	200	81113	99.75%	99.75
Symantec	13016	0	0.00%	299	81014	99.63%	99.63
ZEROSPAM	13010	6	0.05%	185	81128	99.77%	99.54
Spamhaus ZEN+DBL*	13016	0	0.00%	7375	73938	90.93%	90.93
SURBL*	13016	0	0.00%	63970	17343	21.33%	21.33

* *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.*)

Fortinet FortiMail

SC rate: 99.87%
FP rate: 0.01%
Final score: 99.83
Project Honey Pot SC rate: 99.88%
Abusix SC rate: 99.84%
Newsletters FP rate: 0.9%

419 scams, lottery spam and the kind of spam whose subject lines are not to be repeated in polite company were among the 102 emails *Fortinet*'s *FortiMail* appliance failed to block in its 27th VBSpam test. This was a small improvement compared with its score in the last test and, with a single false positive and the fifth highest final score, *Fortinet* achieves its 27th VBSpam award.

GFI MailEssentials

SC rate: 99.55%
FP rate: 0.00%
Final score: 99.55
Project Honey Pot SC rate: 99.61%
Abusix SC rate: 99.18%
Newsletters FP rate: 2.3%

Blocking spam is easy; blocking spam while not blocking legitimate mail is hard. In this test, *GFI MailEssentials* demonstrates how this works in practice: compared to the previous test, the *Windows* solution had a lower spam catch rate, but it didn't miss a single legitimate email (it missed four in the last test). As a consequence, the product's final score remained almost the same, but this time we were able to give *GFI* a well deserved VBSpam+ award.

	Newsletters		Project Honey Pot		Abusix		Web hosts		pre-DATA†		STDev‡
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway MailGate	22	6.4%	362	99.49%	62	99.37%	169	99.38%			0.89
Bitdefender	1	0.3%	23	99.97%	6	99.94%	21	99.92%			0.31
ESET	9	2.6%	289	99.60%	100	98.98%	186	99.32%			0.67
FortiMail	3	0.9%	86	99.88%	16	99.84%	76	99.72%			0.3
GFI	8	2.3%	282	99.61%	81	99.18%	193	99.29%			0.63
Halon Security (ESXi)	5	1.5%	202	99.72%	106	98.92%	116	99.58%			0.59
IBM	11	3.2%	440	99.38%	4	99.96%	208	99.24%			0.74
Kaspersky LMS	1	0.3%	67	99.91%	2	99.98%	29	99.89%			0.44
Libra Esva	12	3.5%	32	99.96%	7	99.93%	24	99.91%	9760	88.00%	0.21
McAfee Email Gateway	3	0.9%	302	99.58%	77	99.22%	170	99.38%			0.59
McAfee SaaS	11	3.2%	114	99.84%	582	94.08%	514	98.12%			1.16
Net At Work NoSpamProxy	42	12.1%	208	99.71%	111	98.87%	146	99.47%	19318	76.24%	0.62
Netmail Secure	14	4.1%	194	99.73%	75	99.24%	149	99.46%	9835	87.90%	0.56
OnlyMyEmail	11	3.2%	0	100.00%	0	100.00%	0	100.00%			0
Scrollout	55	15.9%	161	99.77%	105	98.93%	195	99.29%			0.56
Sophos	0	0.0%	266	99.63%	15	99.85%	100	99.63%			0.52
SpamTitan	5	1.5%	186	99.74%	14	99.86%	145	99.47%			0.55
Symantec	1	0.3%	269	99.62%	30	99.69%	182	99.33%			0.56
ZEROSPAM	33	9.5%	130	99.82%	55	99.44%	122	99.55%			0.48
Spamhaus ZEN+DBL*	0	0.0%	3633	94.92%	3742	61.95%	4920	82.00%	10753	86.78%	6.07
SURBL*	0	0.0%	57063	20.17%	6907	29.76%	21085	22.88%			11.4

* *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. 35 of the false positives for *NoSpamProxy* occurred pre-DATA; all 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.*)

Halon Security

SC rate: 99.62%
FP rate: 0.05%
Final score: 99.39
Project Honey Pot SC rate: 99.72%
Abusix SC rate: 98.92%
Newsletters FP rate: 1.5%

As per our request, *Halon Security*'s virtual machine was reinstalled on a new server prior to this test. Until that point, its developers told me, they hadn't touched their product since March 2011, when it was installed less than two days before its first participation in our tests. While our tests focus on performance rather than ease of maintenance, this is certainly something that speaks for the product, as was the fact that the reinstallation went as smoothly as the initial installation.

There was also good news on the performance side: *Halon* halved its false positive rate, while at the same time significantly increasing its spam catch rate. It thus continues its unbroken string of VBSpam awards with its 17th award.

IBM Lotus Protector for Mail Security

SC rate: 99.45%
FP rate: 0.12%
Final score: 98.84
Project Honey Pot SC rate: 99.38%
Abusix SC rate: 99.96%
Newsletters FP rate: 3.2%

While most products saw a small decrease in their catch rates, *IBM* saw a nice improvement. Against that, however, stood 16 false positives – all but three of which were emails written in English. It is always a shame to see products block legitimate emails, but there is no product that *never* does so. Hopefully *IBM* will be able to reduce its false positive rates in future tests – for now it completes its first dozen VBSpam awards with relative ease.

Kaspersky Linux Mail Security 8.0

SC rate: 99.92%
FP rate: 0.00%
Final score: 99.92
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%

Despite missing 18 emails from the same spam campaign, *Kaspersky*'s *Linux Mail Security* product completed the test with a spam catch rate of 99.92% – even higher than its score in the last test. What is more, there were no false positives and just a single blocked newsletter, which means that *Kaspersky* finishes this test with the third highest final score, and its third VBSpam+ award.

Libra Esva 3.0.1

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.95
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.93%
SC rate pre-DATA: 88.00%
Newsletters FP rate: 3.5%

The devil is in the details when it comes to spam filtering. *Libra Esva* is doing rather well when it comes to those details. It missed fewer than 40 spam emails – fewer than all but two other products and fewer than it did in the previous test in which it did so well. There was no compromise on the false positive score, as once again there weren't any. This gave the product the second highest final score, and for the third time in a row, *Libra Esva* earns a VBSpam+ award.

McAfee Email Gateway 7.0

SC rate: 99.53%
FP rate: 0.11%
Final score: 98.99
Project Honey Pot SC rate: 99.58%
Abusix SC rate: 99.22%
Newsletters FP rate: 0.9%

Among the close to 400 spam messages missed by *McAfee*'s *Email Gateway* appliance were emails in foreign character sets, but also a number of emails offering 'great job opportunities' while actually recruiting for money mules. This is just one of many examples of types of spam email that are more than just a nuisance – falling for their scams could have serious consequences.

Thankfully, *McAfee Email Gateway* actually blocked more than 99.5% of emails – about the same percentage as it did in the last test. Its false positive rate increased, which dented the final score to just below 99, but the product easily earns another VBSpam award.

McAfee SaaS Email Protection

SC rate: 99.14%
FP rate: 0.02%
Final score: 99.02
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 94.08%
Newsletters FP rate: 3.2%

With a spam catch rate of 99.14%, *McAfee*'s *SaaS* solution missed more spam than any other full solution in this test. We should point out that 99.14% is still a very decent score, and one that will keep many a customer happy, but it was a serious drop compared to the previous test (hopefully it was just a one-off glitch). On a more positive note, the product only blocked three legitimate emails (and saw a greatly reduced false positive rate on the newsletter corpus). It thus retained a final score of over 99, and achieved another VBSpam award.

Net At Work NoSpamProxy

SC rate: 99.61%
FP rate: 0.38%
Final score: 97.69
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 98.87%
SC rate pre-DATA: 76.24%
Newsletters FP rate: 12.1%

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	Multiple MX-records	Multiple locations
McAfee SaaS	McAfee	√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	√	√
ZEROSPAM	ClamAV			√	√	√

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	Interface			
					CLI	Desktop GUI	Web GUI	API
Axway MailGate	McAfee; Kaspersky	√	√	√			√	
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	√	√	√	√	√	√	
Net At Work NoSpamProxy	Commtouch			√		√		√
Netmail Secure	Proprietary	√	√	√	√		√	
Scrollout	ClamAV			√	√		√	
Sophos	Sophos						√	
SPAMfighter	VIRUSfighter (optional)	√	√	√			√	
SpamTitan	Kaspersky; ClamAV	√	√	√	√		√	√
Symantec	Symantec	√	√	√	√		√	

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

Compared to a relatively poor performance in the July test, *Net At Work*'s *NoSpamProxy* saw a huge increase in its spam catch rate, which at 99.61% was rather good. Unfortunately, the product once again blocked a large number of legitimate emails – more than any other product. A lot of these were from a relatively small number of senders, and it is possible that the product has issues with certain kinds of email that are common in our legitimate mail streams. If that is the case, it shouldn't be too difficult for its developers to tweak its settings and achieve a VBSpam award in future. This time, it missed the certification threshold by a small margin.

Netmail Secure

SC rate: 99.67%
FP rate: 0.00%
Final score: 99.67
Project Honey Pot SC rate: 99.73%
Abusix SC rate: 99.24%
SC rate pre-DATA: 87.90%
Newsletters FP rate: 4.1%

Netmail Secure has a long history of participating in the VBSpam tests, having participated in (and done

Complete solutions sorted by final score	
Bitdefender	99.96
Libra Esva	99.95
OnlyMyEmail	99.92
Kaspersky LMS	99.92
FortiMail	99.83
SpamTitan	99.75
Netmail Secure	99.67
Symantec	99.63
GFI	99.55
ZEROSPAM	99.54
ESET	99.52
Sophos	99.42
Halon Security (ESXi)	99.39
McAfee SaaS	99.02
McAfee Email Gateway	98.99
IBM	98.84
Axway MailGate	98.71
Scrollout	98.71
NoSpamProxy	97.69

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

impressively well in) the very first VBSpam test under the name *Messaging Architects*. Four and a half years later, spam has evolved in many ways but *Netmail* still offers a decent solution to protect against it.

The virtual appliance missed fewer than one in 300 emails in the spam corpus and did so without blocking a single legitimate email. It thus not only achieves another VBSpam award – it also earns its third VBSpam+ award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.02%
Final score: 99.92
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 3.2%

When told about the two false positives in this test, *OnlyMyEmail*'s developers said they had suffered a minor glitch on their side that would have been the likely cause. Indeed, the two emails were sent not long after each other, and when they were resent after the test, they were no longer blocked.

Not only were these the only two false positives, the product didn't miss a single spam email throughout the full 16 days of the test. This is not the first time the product has pulled this off either, and it remains a fantastic achievement. Even with the 'glitch', the product finished the test with the third highest final score – and yet another VBSpam award.

Scrollout F1

SC rate: 99.67%
FP rate: 0.19%
Final score: 98.71
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 98.93%
Newsletters FP rate: 15.9%

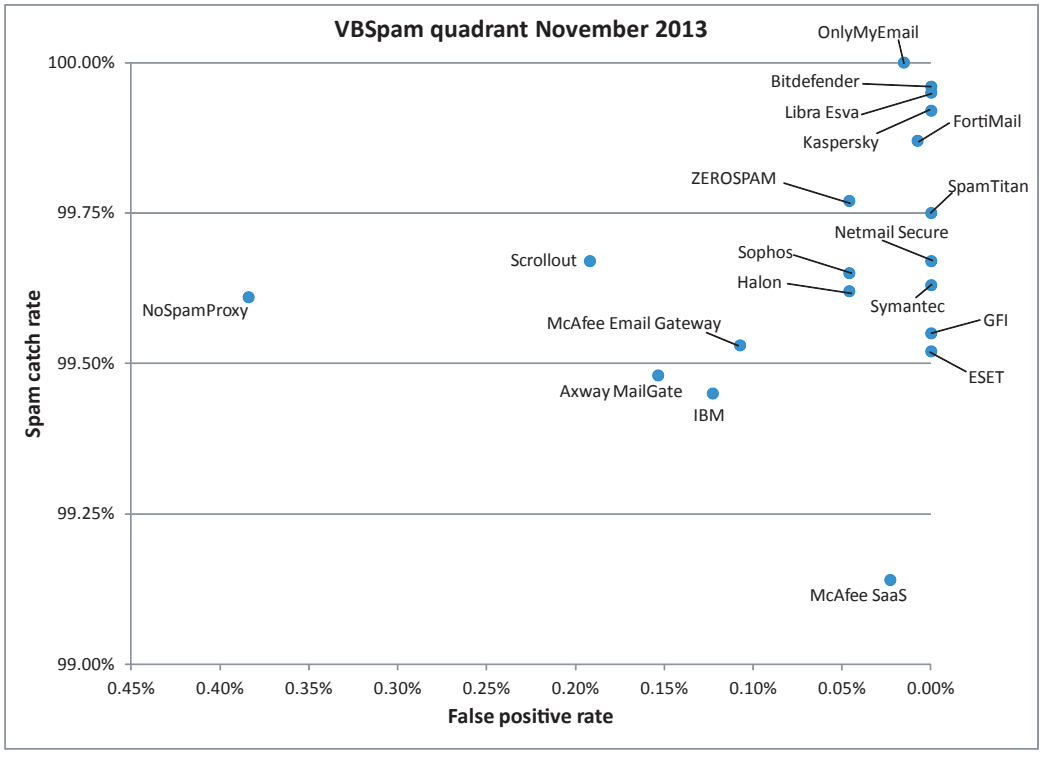
About 24 hours prior to the start of the test, on the request of *Scrollout*'s main developer, we installed a new version of the free and open source anti-spam gateway. This obviously had the desired effect, as the product's false positive rate almost halved, while it maintained a high spam catch rate. Sure, there were more false positives than for all but one other product, but after failing to reach the required threshold in the last two tests, *Scrollout* earned a VBSpam award.

Sophos Email Appliance

SC rate: 99.65%
FP rate: 0.05%
Final score: 99.42
Project Honey Pot SC rate: 99.63%
Abusix SC rate: 99.85%
Newsletters FP rate: 0.0%

As someone who often checks for offers in recently received mailings before going shopping, I know that many users don't want legitimate newsletters to be blocked (these tests have shown that they regularly *are* blocked). I was thus pleased to see that *Sophos*'s *Email Appliance* did not block any of them – the only full solution in this test to achieve a zero false positive score in the newsletter corpus.

Unfortunately, the hardware appliance did block six legitimate ('ham') emails which, unlike the newsletters, count towards the final score. The final score was thus a little lower than in the last test, but at 99.42 it was still decent and *Sophos* easily achieves its 21st VBSpam award in as many tests.



(Please refer to text for full product names.)

SpamTitan 5.11

SC rate: 99.75%
FP rate: 0.00%
Final score: 99.75
Project Honey Pot SC rate: 99.74%
Abusix SC rate: 99.86%
Newsletters FP rate: 1.5%

I was rather pleased to see *SpamTitan* reverse a slight downwards trend when it came to its spam catch rates. With a very impressive 99.75% of spam blocked, it did better than in any test since January. Even more pleasing was the fact that in this test, the virtual appliance didn't block a single legitimate email and thus achieves its third VBSpam+ award – its first in a year.

Symantec Messaging Gateway 10.0

SC rate: 99.63%
FP rate: 0.00%
Final score: 99.63
Project Honey Pot SC rate: 99.62%
Abusix SC rate: 99.69%
Newsletters FP rate: 0.3%

As a regular reader of the company's blog, I know that *Symantec* does some good research into unwanted and dangerous emails, from the most targeted to the most mundane. It is nice to see this research paying off – the product has earned 23 VBSpam awards in a row, and it adds its 24th this month.

Moreover, with a spam catch rate that was a little higher than that in the September test, and no false positives, *Symantec*'s *Messaging Gateway* earns its third VBSpam+ award.

ZEROSPAM

SC rate: 99.77%
FP rate: 0.05%
Final score: 99.54
Project Honey Pot SC rate: 99.82%
Abusix SC rate: 99.44%
Newsletters FP rate: 9.5%

Six false positives, four of which were in Russian and the other two in English, prevented *ZEROSPAM* from achieving another VBSpam+ award in this test. But with a spam catch rate of 99.77% (among the 185 spam emails the hosted solution did miss were fake job offers, dating spam and many emails in Chinese), *ZEROSPAM* earns its 11th VBSpam award.

Spamhaus ZEN+DBL

SC rate: 90.93%
FP rate: 0.00%
Final score: 90.93
Project Honey Pot SC rate: 94.92%
Abusix SC rate: 61.95%
SC rate pre-DATA: 86.78%
Newsletters FP rate: 0.00%

Yet again, the combination of *Spamhaus*'s *ZEN* IP blacklists and *DBL* domain blacklists blocked more than 90 per cent of all emails. This shows that blocking by domain and IP address remains an effective way to stop a large chunk of spam. No wonder, then, that most participating products use a DNSBL of some kind. And using *Spamhaus*, as some do, is not a bad choice at all – especially since the product once again didn't miss a single legitimate email.

SURBL

SC rate: 21.33%
FP rate: 0.0%
Final score: 21.33
Project Honey Pot SC rate: 20.17%
Abusix SC rate: 29.76%
Newsletters FP rate: 0.00%

The spam catch rates of *SURBL*'s domain-based blacklist have been going up and down this year, a volatility that can be explained by a large variation in the spam that is sent. In this test they went down a little over 21 per cent – lower than it had been since *SURBL* joined the test, though as mentioned before, this may well be because spammers are getting better at using URLs that can't be blocked.

CONCLUSION

With eight VBSpam+ awards granted, this was certainly a good VBSpam test. Nevertheless, there will be some product developers who won't be so happy with the results.

There are many good email security solutions on offer, and some of them perform exceptionally well. At the same time, the spam problem hasn't yet been solved and dangerous emails continue to slip through many a maze.

The next VBSpam test will run in December 2013, with the results scheduled for publication in January 2014. 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 Engineers: Scott James & 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/