JANUARY 2014

virus BULLETIN

Covering the global threat landscape

JANUARY 2014 VBSPAM COMPARATIVE REVIEW

INTRODUCTION

This month has been all about fridges sending spam[1]. Actually, it was only one fridge, and the jury is still out on whether it really was the fridge that was sending the spam. But if it was, it will have been a case of some run-of-the-mill malware that happened to infect a fridge that was running a vulnerable version of a popular operating system.

Fridges, like smart televisions and other Internet-connected home appliances, are unlikely to pose a serious challenge for spam filters. The latter tend to be rather good at blocking spam from home networks, and there is nothing that makes domestic appliances any better at sending spam than your average infected *Windows XP* PC.

I am slightly more concerned about the infected routers sending spam that were mentioned in the same report[2]. A lot of routers are known to have vulnerabilities, and the patching of routers is nowhere near as common a practice as it is with PCs. Given their location at the edge of networks, they may have some advantages when it comes to spoofing origins, and thus also when it comes to sending spam.

Only time will tell whether routers sending spam will become a serious problem, but what these recent revelations show is that, while we are doing very well in our fight against spam, anti-spam developers cannot afford to rest on their laurels: spam continues to evolve, and adaptation to the changes is essential.

Of course, we will continue to report on how well anti-spam products perform against live streams of ham and spam. In this month's test, the blocking of spam was very good, with each of the 18 participating full solutions achieving a very decent catch rate. However, for some products this came at the cost of blocking legitimate emails – and for three products that was enough to deny them a VBSpam award. On a more positive note, there were five solutions that did not block a single legitimate email and achieved a VBSpam+ award.

[1] http://www.virusbtn.com/blog/2014/01_21.xml

[2] http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-ll-details.php

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

ISSN 1749-7027

THE EMAIL CORPUS

The VBSpam test tends more or less to 'run itself', and an occasional check that everything is running smoothly is all that is needed – thus it isn't usually a problem for the test to run over the holiday period.

However, on this occasion, when I checked the system a few days prior to the scheduled end of the test, things *weren't* running smoothly. One of the hard drives was having a major issue and could neither be written to nor read from. It wasn't until a few days later (and with a lot of help from my colleague, John Hawes) that I was able to confirm that all data prior to the crash could be recovered.

We decided that, although the hard drive failure meant having to cut the test short by three days, enough data had been collected to provide a reliable report.

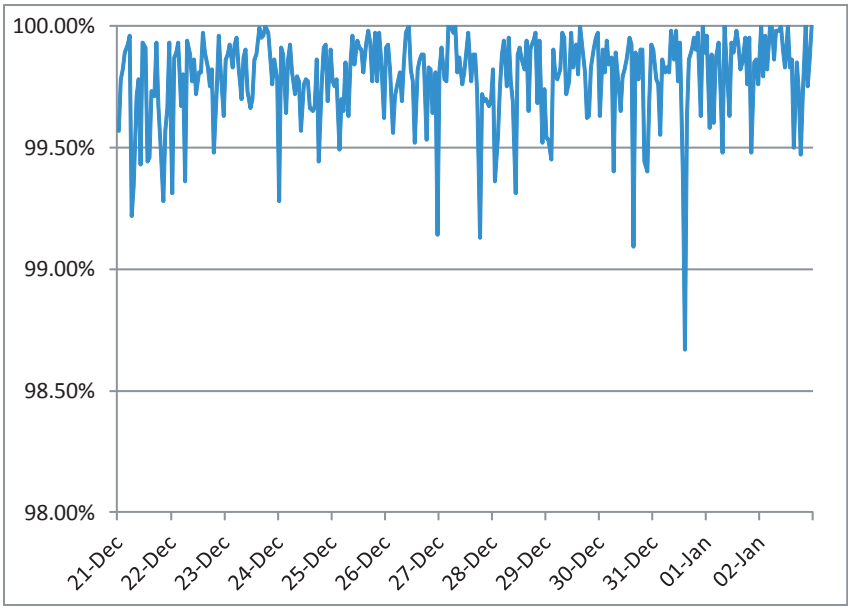


Figure 1: Spam catch rate of all complete solutions throughout the test period.

The test therefore ran for 13 days: from 12am on Saturday 21 December 2013 to 12am on Friday 3 January 2014 (it was later on 3 January that the hard disk issues materialized). There were no other issues during the 13 days of the test.

The corpus of emails sent during the test period consisted of 89,886 emails, 82,206 of which were spam. 72,490 of these were provided by *Project Honey Pot*, with the remaining 9,716 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 7,435 legitimate emails ('ham') and 245 newsletters.

Note that the actual number of emails sent during the test period is always larger than the number of emails that end up in the corpus. Emails for which we cannot prove delivery attempts have been made to all participating products are excluded, as are emails that are obviously misclassified. Moreover, corrections are made to remove some bias from the corpus. These happen automatically, without the testers having any idea of how it would affect individual products' measured performance.

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 to those included in recent reports, a difference can immediately be seen: the catch rate was a lot higher in this test than in previous tests. Indeed, most products saw their catch rates improve, and all full products blocked at least 99.4% of all spam in the corpus.

As we saw in the last test, spam filters tend to agree on which emails to block: 80,400 emails (96.7% of the spam corpus) were blocked by all 18 full solutions in the test.

The clear 'winner' among the spam emails (that which caused the most problems for the products in the test) was an Italian 'debt consolidation' email. At first glance (Figure 2), it may be clear why this email wasn't blocked: it is low on text and the two links, including one to 'unsubscribe', directed to *Google Drive*. However, on closer inspection the email had some clear characteristics of spam.

Figure 2: Italian spam email.

For instance, it claimed that it was sent from a hotmail.it address – but the email headers showed that it was not. Moreover, the text and HTML versions of the email contained slightly different texts.

DMARC

For some time, the VBSpam reports have indicated whether products support certain anti-spam technologies (DKIM/SPF), with the aim of providing information to potential customers as well as to the wider email community.

As of this report, we have added DMARC to the technologies listed. It should be noted that, in all cases, we rely on the product developers to provide us with the information on what features are used. Moreover, we don't make any judgement as to whether certain techniques should or should not be included in products.

DMARC is a fairly new protocol that takes DKIM and SPF to the next level. While these protocols provide some kind of integrity check on the content and the sender of the email, DMARC gives domain owners the opportunity to state what receivers should do with emails that fail DKIM or SPF checks.

John Levine wrote a good introduction to DMARC in the March 2012 issue of *Virus Bulletin*[3] – which I would encourage anyone wanting to find out more about the protocol to read. To demonstrate why DMARC can be useful, imagine you are the owner of the popular domain 'example.com'. Using DMARC, you can tell recipients what to do with emails that claim to have been sent from an example.com address, but which fail both SPF and DKIM checks.

Depending on how much you trust your own records and how important you consider the risk of phishing compared with the risk of legitimate emails not being delivered, you can tell receivers to accept the emails anyway, to turn up the filters, or to reject the emails. DMARC also provides ways to specify how and where you'd like to receive individual and/or aggregate reports on emails that failed to authenticate.

DMARC was started as a private project among some larger senders, including *Google*, *Yahoo!*, *PayPal* and *Facebook*. As the table in this report shows, adoption of the protocol among participating spam filters – which tend to cater for small and medium-sized organizations – is rather slow. It will be interesting to see whether this is because DMARC only provides significant benefits for the really big players, or whether it is simply a case of DMARC adoption taking its time.

[3] http://www.virusbtn.com/virusbulletin/archive/2012/03/vb201203-DMARC

RESULTS

Axway MailGate 5.3.1

SC rate: 99.64%
FP rate: 0.42%
Final score: 97.55
Project Honey Pot SC rate: 99.66%
Abusix SC rate: 99.44%
Newsletters FP rate: 8.6%

Looking at the number of false positives for *Axway*'s *MailGate* product in this test, it is hard not to imagine that – even though we only count a maximum of four FPs per sender and/or discussion thread – the addition of a few simple rules would have lowered that number. Indeed, like many other products, *Axway* offers users the opportunity to fine-tune the product.

However, to make the competition fair, we test all solutions without any special rules, and as such *Axway*'s false positive rate was just over 0.4%. Too high, even with an improved spam catch rate, to earn a VBSpam award on this occasion.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.90%
FP rate: 0.00%
Final score: 99.90
Project Honey Pot SC rate: 99.89%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.4%

The last time that *Bitdefender* missed a legitimate email was November 2012 – so long ago that the email has long since been deleted from our archive. Once again in this test, not a single legitimate email was blocked, and even among the newsletters there was only one that was incorrectly blocked.

Meanwhile, the product's spam catch rate remained high – with fewer than one in 1,000 emails missed, it didn't matter that it was slightly lower than it was in November. Not only does *Bitdefender* continue to be the only product to have won a VBSpam award in every test, but it earns a record-breaking seventh VBSpam+ award in a row.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.72%
FP rate: 0.01%
Final score: 99.65
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 98.80%
Newsletters FP rate: 2.9%

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	7404	31	0.42%	298	81908	99.64%	97.55
Bitdefender	7435	0	0.00%	81	82125	99.90%	99.90
ESET	7434	1	0.01%	231	81975	99.72%	99.65
FortiMail	7431	4	0.05%	102	82104	99.88%	99.61
GFI	7434	1	0.01%	243	81963	99.70%	99.64
Halon Security	7403	32	0.43%	246	81960	99.70%	97.55
IBM	7430	5	0.07%	165	82041	99.80%	99.46
Kaspersky LMS	7431	4	0.05%	84	82122	99.90%	99.63
Libra Esva	7435	0	0.00%	15	82191	99.98%	99.98
McAfee Email Gateway	7433	2	0.03%	394	81812	99.52%	99.39
McAfee SaaS	7430	5	0.07%	442	81764	99.46%	99.13
Net At Work NoSpamProxy	7395	40	0.54%	318	81888	99.61%	96.92
Netmail Secure	7434	1	0.01%	215	81991	99.74%	99.67
OnlyMyEmail	7435	0	0.00%	1	82205	99.999%	99.999
Scrollout	7422	13	0.17%	100	82106	99.88%	99.00
Sophos	7435	0	0.00%	159	82047	99.81%	99.81
SpamTitan	7434	1	0.01%	221	81985	99.73%	99.66
ZEROSPAM	7435	0	0.00%	78	82128	99.91%	99.91
Spamhaus ZEN+DBL*	7435	0	0.00%	7439	74767	90.95%	90.95
SURBL*	7435	0	0.00%	53864	28342	34.48%	34.48

* *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.*)

With an above average improvement in its spam catch rate, *ESET* blocked more than 99.7% of spam. Among the spam messages that were missed were a lot of emails in non-English languages as well as several from an odd campaign that used a time as the subject line and contained only a single link.

Against that stood a very low false positive rate: *ESET* blocked just a single legitimate email. Of course, that's one too many and the product – which has won four VBSpam+ awards in the last eight tests – will have to console itself with 'just' a VBSpam award this time.

Fortinet FortiMail

SC rate: 99.88%
FP rate: 0.05%
Final score: 99.61
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.8%

A product accidentally blocking legitimate emails is never a good thing, but I couldn't help but smile when I saw the content of four legitimate emails that *FortiMail* erroneously blocked: they all discussed the current state of spam and spam filters[4].

Thankfully, these were the only legitimate emails that *Fortinet*'s appliance blocked, and with an impressive 99.88% spam catch rate, the product achieves a final score of 99.61 – and wins its 28th VBSpam award in a row.

GFI MailEssentials

SC rate: 99.70%
FP rate: 0.01%
Final score: 99.64
Project Honey Pot SC rate: 99.80%

[4] Note that the emails didn't mention or quote *actual* spam. Although we believe that ideally such emails shouldn't be blocked, if they had mentioned or quoted real spam, we would have excluded them from the corpus as this would have been beyond the scope of the tests.

	Newsletters		Project Honey Pot		Abusix		pre-DATA†		STDev‡
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Axway	21	8.6%	244	99.66%	54	99.44%			0.48
Bitdefender	1	0.4%	79	99.89%	2	99.98%			0.26
ESET	7	2.9%	114	99.84%	117	98.80%			0.41
FortiMail	2	0.8%	101	99.86%	1	99.99%			0.28
GFI	2	0.8%	143	99.80%	100	98.97%			0.47
Halon Security	11	4.5%	234	99.68%	12	99.88%			0.65
IBM	2	0.8%	164	99.77%	1	99.99%			0.41
Kaspersky LMS	1	0.4%	67	99.91%	17	99.83%			0.23
Libra Esva	6	2.5%	15	99.98%	0	100.00%	14044	82.92%	0.10
McAfee Email Gateway	2	0.8%	306	99.58%	88	99.09%			0.56
McAfee SaaS	4	1.6%	305	99.58%	137	98.59%			0.75
Net At Work NoSpamProxy	22	9.0%	232	99.68%	86	99.11%	38488	53.18%	0.54
Netmail Secure	2	0.8%	119	99.84%	96	99.01%	14081	82.87%	0.45
OnlyMyEmail	7	2.9%	1	99.999%	0	100.00%			0.03
Scrollout	103	42.0%	93	99.87%	7	99.93%			0.33
Sophos	0	0.0%	156	99.78%	3	99.97%			0.39
SpamTitan	11	4.5%	219	99.70%	2	99.98%			0.75
ZEROSPAM	14	5.7%	76	99.90%	2	99.98%			0.25
Spamhaus ZEN+DBL*	0	0.0%	5794	92.01%	1645	83.07%	14410	82.47%	4.15
SURBL*	0	0.0%	50115	30.87%	3749	61.41%			17.49

* *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.*)

GFI MailEssentials contd.

Abusix SC rate: 98.97%

Newsletters FP rate: 0.8%

You win some, you lose some. That's certainly the case for *GFI*, whose *MailEssentials* product managed to increase its catch rate to a nice 99.70%. Against this stood a single false positive – and two false positives among the newsletters.

Blocking one email out of 7,500 legitimate emails is hardly the end of the world, but it does mean *GFI* has to be content with an ordinary VBSpam award on this occasion.

Halon Security

SC rate: 99.70%

FP rate: 0.43%

Final score: 97.55

Project Honey Pot SC rate: 99.68%

Abusix SC rate: 99.88%

Newsletters FP rate: 4.5%

Halon is another product whose false positive rate would, I believe, have been a lot lower had the product been fine-tuned and some extra rules added. The product even comes with its own scripting language to add extra rules, so it would be easy for users to do this. Unfortunately, we are only able to give VBSpam awards based on our performance measures (which don't include fine-tuning) – and, despite a catch rate of 99.70%, *Halon Security*'s final score fell below the VBSpam threshold in this test.

Interestingly, *Halon* is the only product that both verifies the

DMARC status of incoming emails and provides feedback to the organizations the emails come from. While we won't make any judgements about whether DMARC is a good idea, this does show that *Halon* takes the wider email community into consideration.

IBM Lotus Protector for Mail Security

SC rate: 99.80%
FP rate: 0.07%
Final score: 99.46
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.8%

While writing this report, I came across a blog post by one of *IBM*'s main anti-spam developers on a sudden surge in image spam[5]. I like it when developers don't just focus on making their own product better, but also share what they've learned with the wider community.

Of course, what we measure in these tests is merely how well developers can make their own products work. Thankfully, for its *Lotus Protector* product, *IBM* did really well in this aspect too: the spam catch rate increased to 99.80%, while the number of false positives – which was rather high in the last test – decreased to five. The product thus earns its 13th VBSpam award.

Kaspersky Linux Mail Security 8.0

SC rate: 99.90%
FP rate: 0.05%
Final score: 99.63
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.83%
Newsletters FP rate: 0.4%

Being headquartered in Russia, *Kaspersky* has historically had relatively few problems with legitimate emails in foreign languages and character sets – something that other products have struggled with. But no product is flawless, and in this test *Kaspersky*'s *Linux Mail Security* product erroneously blocked three Turkish emails.

Of course, such things happen – and with a spam catch rate of 99.90%, it doesn't affect the product's overall performance much. It does mean there was no VBSpam+ award in the bag this time, but yet another VBSpam award is well deserved.

[5] http://securityintelligence.com/image-spam-return/

Libra Esva 3.2

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 100.00%
SC rate pre-DATA: 82.92%
Newsletters FP rate: 2.5%

With a spam catch rate of 99.95% in the previous test, there was little room for improvement for *Libra Esva*. Still, it managed to improve its performance just a tiny bit: with just 15 missed spam emails, all from the *Project Honey Pot* feed, it achieved a spam catch rate of 99.98%.

99.98 is also the product's final score (the second highest this month), as the virtual solution didn't miss a single legitimate email. It missed six newsletters, which isn't too many either, and there is plenty of reason for *Libra Esva* to celebrate its sixth VBSpam+ award – its fourth in a row.

McAfee Email Gateway 7.0

SC rate: 99.52%
FP rate: 0.03%
Final score: 99.39
Project Honey Pot SC rate: 99.58%
Abusix SC rate: 99.09%
Newsletters FP rate: 0.8%

As in the November test, *McAfee*'s *Email Gateway* appliance missed about 400 emails in this month's corpus, and once again, the majority of them were written in a non-Latin character set. Spam is a global problem, and while for many users these emails pose no serious danger, for the speakers of the languages they are written in, it is these emails rather than English-language spam, that is the biggest concern.

A catch rate of just over 99.5% is not something to be ashamed of though – and I was pleased to see that the product only missed two legitimate emails, thus edging ever closer to a VBSpam+ award. For now, the product has a full dozen VBSpam awards.

McAfee SaaS Email Protection

SC rate: 99.46%
FP rate: 0.07%
Final score: 99.13
Project Honey Pot SC rate: 99.58%
Abusix SC rate: 98.59%
Newsletters FP rate: 1.6%

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

*OnlyMyEmail verifies DMARC status, but doesn't provide feedback at the moment.

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

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky; McAfee	√	√	√				√	
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	√	√	√		√		√	√

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

While it's true that *McAfee*'s *SaaS* product missed more spam than any other full solution, that statement doesn't do justice to what was actually a pretty good performance: fewer than one in 185 spam emails slipped through the net.

The product blocked just five legitimate emails (as well as four newsletters), and achieved a pretty decent final score, which earns the hosted solution its 15th VBSpam award.

Net At Work NoSpamProxy

SC rate: 99.61%
FP rate: 0.54%
Final score: 96.92
Project Honey Pot SC rate: 99.68%
Abusix SC rate: 99.11%
SC rate pre-DATA: 53.18%
Newsletters FP rate: 9.0%

Within this month's ham corpus there was a fairly large group of legitimate emails – all written in English and with nothing I could see that made them look significantly spammy – that caused problems for a few products. *NoSpamProxy* was one of those products.

I hope this will prove to have been a one-off issue – perhaps even an unfortunate coincidence – solved by the time the next report is published. For now, despite a decent 99.61% catch rate, we are unable to grant *NoSpamProxy* its second VBSpam award.

Netmail Secure

SC rate: 99.74%
FP rate: 0.01%
Final score: 99.67
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.01%
SC rate pre-DATA: 82.87%
Newsletters FP rate: 0.8%

Netmail missed 142 spam emails in this test, several of

Complete solutions sorted by final score	
OnlyMyEmail	99.999
Libra Esva	99.98
ZEROSPAM	99.91
Bitdefender	99.90
Sophos	99.81
Netmail Secure	99.67
SpamTitan	99.66
ESET	99.65
GFI	99.64
Kaspersky LMS	99.63
FortiMail	99.61
IBM	99.46
McAfee Email Gateway	99.39
McAfee SaaS	99.13
Scrollout	99.00
Axway	97.55
Halon Security	97.55
Net At Work NoSpamProxy	96.92

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

which were Chinese-language emails from the *Abusix* feed. This was a small improvement compared to the last test, in which the product achieved its fourth VBSpam+ award.

However, a fifth such award was not in the bag for *Netmail Secure* this month, as the virtual appliance missed a single legitimate email: a technical discussion that a few other products also had difficulty with. But with a very decent final score and just two missed newsletters, there is no reason for *Netmail*'s developers to be disappointed with this month's results and a VBSpam award.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 2.9%

When it comes to blocking spam, *OnlyMyEmail* has outperformed its fellow participants in every VBSpam test it has taken part in (including this one). Of course, a high catch rate alone might not say much, but the hosted solution tends to have very low false positives rates too. This test was no exception: the product didn't miss a single legitimate email and only blocked seven emails from the newsletter corpus – from four different senders. The single false negative was one without a payload (containing only a generic holiday greeting), rather harmless as spam goes.

Incidentally, *OnlyMyEmail* is also one of the few products that check the DMARC status of emails – but until adoption of the standard is more widespread, no feedback mechanism has been implemented.

For now, the product achieves its 20th VBSpam award in succession and, with the highest final score, its third VBSpam+ award.

Scrollout

SC rate: 99.88%
FP rate: 0.17%
Final score: 99.00
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 99.93%
Newsletters FP rate: 42.0%

It was a good month for *Scrollout*: the free, open source virtual appliance saw its catch rate rise to an impressive 99.88%, while the product's false positive rate decreased slightly. At 0.17%, it was still a little higher than that of most other products, however. That, and the slightly worrying 42% of newsletters that were blocked, means that users of the product may want to tweak it a little, or take a regular look in their spam quarantine.

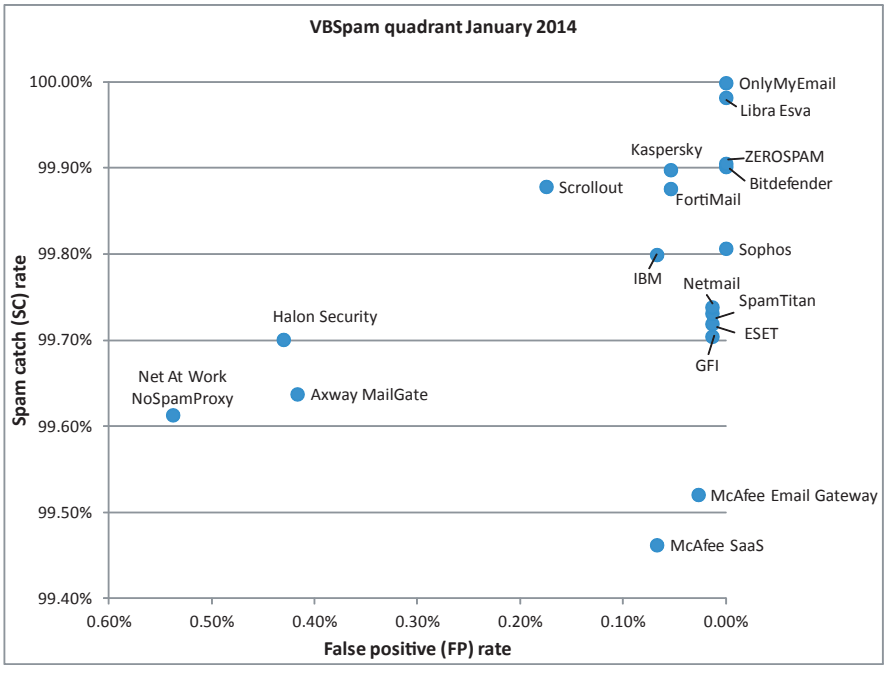
But that shouldn't stop the volunteers who manage *Scrollout* from celebrating the product's fourth VBSpam award, along with its highest final score to date.

Sophos Email Appliance

SC rate: 99.81%
FP rate: 0.00%
Final score: 99.81
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.0%

The newsletter feed is an easily overlooked part of the VBSpam tests. And while seeing the odd newsletter appear in the spam folder might be something many users can live with, it is still better if it doesn't happen. Kudos therefore to *Sophos,* whose appliance has avoided false positives in this corpus in most of the previous tests, and thereby outperformed other full solutions in this category.

This time, *Sophos* didn't miss any emails in the ordinary legitimate mail stream either, while the product blocked over 99.8% of all spam – a significant improvement



(Please refer to text for full product names.)

compared to the last test. With this performance, *Sophos* earns its first and very well-deserved VBSpam+ award.

SpamTitan 6.00

SC rate: 99.73%
FP rate: 0.01%
Final score: 99.66
Project Honey Pot SC rate: 99.70%
Abusix SC rate: 99.98%
Newsletters FP rate: 4.5%

This is the 26th successive test in which *SpamTitan* has participated, yet the first time we have seen the new 6.00 version of the virtual appliance. Among the changes in this version is the addition of support for role-based administration, which allows domain administrators and end-users to manage their own policies, as well as support for greylisting.

Neither of these features is tested in our set-up, and with a spam catch rate of 99.73%, *SpamTitan* performs very well out of the box. Still, these features could help improve the performance further in a live environment.

Unfortunately for *SpamTitan*, there was a single false positive: an email containing a lot of shouty capitals. This means that the product misses out on a VBSpam+ award, nevertheless its 26th consecutive VBSpam award is something to be proud of.

ZEROSPAM

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.98%
Newsletters FP rate: 5.7%

This test marks the two-year anniversary of *ZEROSPAM* joining our tests, and there is plenty of reason to celebrate. Not only did the product achieve its highest spam catch rate to date (missing just 78 spam messages), but it did so without blocking a single legitimate email.

In a test in which competition was stiff, the Canadian hosted solution achieved the third highest final score, and with that its third VBSpam+ award.

Spamhaus ZEN+DBL

SC rate: 90.95%
FP rate: 0.00%
Final score: 90.95
Project Honey Pot SC rate: 92.01%
Abusix SC rate: 83.07%
SC rate pre-DATA: 82.47%
Newsletters FP rate: 0.00%

For some time now, *Spamhaus*'s catch rate has remained at just above 90%, showing that, while blocking spam based on the sending IP address and the domains present in the email has become less effective than it was some years ago, it continues to take out a significant chunk of spam.

It is also interesting to note the decline in the pre-DATA catch rate for *Spamhaus* – showing that blocking based on the IP address has become less effective.

SURBL

SC rate: 34.48%

FP rate: 0.00%

Final score: 34.48

Project Honey Pot SC rate: 30.87%

Abusix SC rate: 61.41%

Newsletters FP rate: 0.00%

After a long decline, *SURBL*'s catch rate has fluctuated throughout the past six months; on this occasion it was higher than in previous months. Much of this is due to changes in the content of spam emails – for example, whether they include blockable domains, or even include domains at all (note that a lot of spam includes malicious attachments as the payload, thus there is no need for a domain in the body of the email) – rather than the performance of the blocklist. With the increasing difficulty of blocking email based on the IP address, it is good to know there is a list that can take out one third of spam, simply by checking the domains present in the email.

CONCLUSION

Almost five years of VBSpam tests have shown that, while the spam problem is nowhere near solved, it has been mitigated pretty well – to the point where those working in other areas of cybersecurity have reason to be envious. Indeed, the high spam catch rates in this test show that spam filters all do a really good job at blocking spam.

Still, there are many improvements to be made. For several of the participating products, false positives are one of the areas in which improvements can be made. Hopefully the next test will see lower false positive rates all round, without compromising on the spam catch rates.

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

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Dr Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Scott James

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/