JANUARY 2015

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW JANUARY 2015

INTRODUCTION

In its annual security report[1], *Cisco* stated that the volume of spam had increased 250% between January and November 2014.

Whether this figure is accurate or not (measuring spam is notoriously difficult and the report itself doesn't even seem to back up the claim), unless your job is to administer large email systems, you are unlikely to have noticed such a change.

The spam problem is nowhere near solved, but it is very well mitigated – to the point that people working in other areas of online security have reason to be jealous. Spam filters aren't the only reason for this successful mitigation, but they do play an essential part.

To find out how big a part they play, you could simply turn off your organization's spam filter for a day and see how quickly email becomes unusable – actually, for that reason, you'd better not try that.

Spam isn't the most exciting aspect of cybercrime. It rarely, if ever, involves advanced techniques or highly skilled nation state actors. Nevertheless, it remains a threat to one of the greatest and most important functions of the Internet: email. For this reason, we feel that testing the performance of spam filters is no less important than it was when we started the VBSpam tests seven years ago.

Sixteen full solutions and a number of DNS-based blacklists were submitted for this test. All but three of the full solutions achieved a VBSpam award, and six of them achieved 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). However, no products chose to make use of this option on this occasion.

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 small organization.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the weighted false positive (WFP) rate. The WFP rate is defined as the false positive rate of the ham and newsletter corpora taken together, with emails from the latter corpus having a weight of 0.2:

WFP rate = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #newsletters)

Products earn VBSpam certification if the value of the final score is at least 98:

SC - (5 x WFP) ≥ 98

Meanwhile, products that combine a spam catch rate of 99.5% or higher with no false positives and no more than 2.5% false positives among the newsletters earn a VBSpam+ award.

THE EMAIL CORPUS

The test started on Saturday 20 December at 12am and was scheduled to finish 16 days later, on Monday 5 January at

[1] http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf.

ISSN 1749-7027

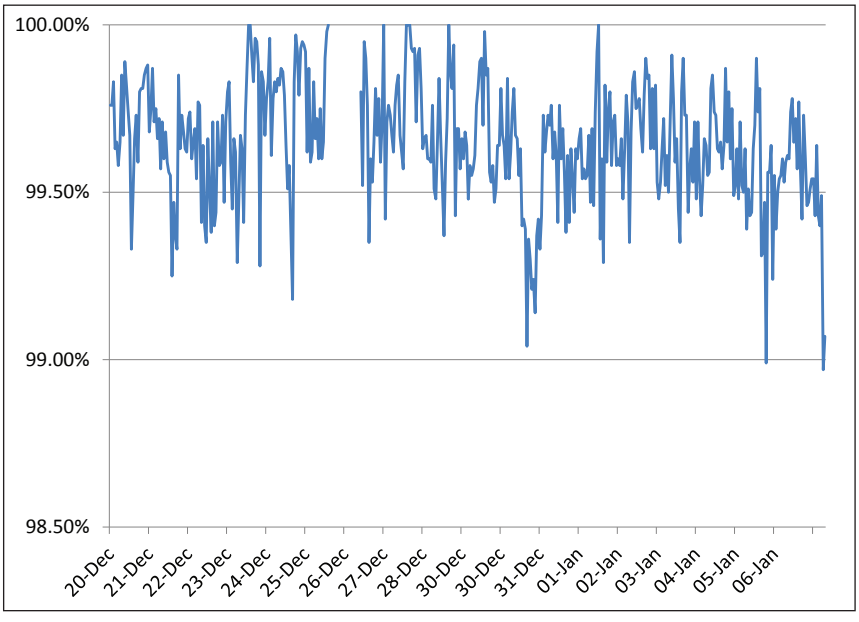


Figure 1: Spam catch rate of all full solutions throughout the test period.

12am. However, there were some issues during this period that led to sub-optimal network circumstances and thus the exclusion of 20 hours' worth of email. This, combined with the fact that the number of emails in our ham feed was rather small (as a result of the Christmas holiday lull in email traffic), led us to decide to extend the test period by two days. The test thus ended on Wednesday 7 January at 12am.

The test corpus consisted of 140,431 emails. 131,555 of these emails were spam, 47,477 of which were provided by *Project Honey Pot*, with the remaining 84,078 emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 8,603 legitimate emails ('ham') and 273 newsletters.

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 to the previous test, things seemed to have improved overall. However, due to two outliers, the average spam catch rate is actually slightly lower than it was in November.

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' refers to a message in that corpus that has been erroneously marked by a product as spam.

Axway MailGate 5.3.1

SC rate: 99.75%
FP rate: 0.00%
Final score: 99.51
Project Honey Pot SC rate: 99.68%
Abusix SC rate: 99.79%
Newsletters FP rate: 7.7%

This month's test saw *Axway MailGate*'s best performance to date. Not only did the virtual appliance achieve its highest spam catch rate so far (and it would have been even higher, had it not been for a single campaign of Brazilian banking spam), it also didn't block a single legitimate email.

This was almost enough to earn *Axway* its first VBSpam+ award. However, the product was one of several this month that had a high newsletter false positive rate, so that first VBSpam+ award remains just out of reach. The product's sixth VBSpam award is well deserved though.

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.96%
FP rate: 0.01%
Final score: 99.89
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.4%

We have always made it clear that filtering spam sometimes involves making impossible choices – hence no product is perfect. Indeed, on this occasion, after two years without any false positives, *Bitdefender*'s *Linux* product blocked its first legitimate email in our tests since 2012.

This is hardly the end of the world though, and with a more than decent final score, *Bitdefender* continues its unbroken run of VBSpam awards, this time notching up its 35th.

Egedian Mail Security

SC rate: 96.71%
FP rate: 0.05%
Final score: 96.46
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 94.94%
Newsletters FP rate: 0.4%

It is hard not to feel sorry for *Egedian Mail Security*, based on this month's performance. The vast majority of the spam emails that the product missed were part of a single campaign. In many a real environment, the product's administrator would have been able to set up ad hoc rules to block the campaign in question – something the product is designed to allow for.

However, the VBSpam tests are run without any user intervention, and as such, the number of spam emails missed by *Egedian* was too great for it to reach the required threshold for a VBSpam award. We are hopeful that the feedback we have sent to the developers will help them get the product back to form.

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.90%
FP rate: 0.00%
Final score: 99.87
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.98%
Newsletters FP rate: 1.1%

In the last test, *ESET* missed out on a VBSpam+ award due to a slightly low spam catch rate. This month, to say that the *Exchange*-based product bounced back would be an understatement: the product's catch rate increased to 99.90%, while yet again there were no false positives. With a relatively low newsletter false positive rate as well, the product earns another VBSpam+ award – its seventh.

Fortinet FortiMail

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.76
Project Honey Pot SC rate: 99.81%
Abusix SC rate: 99.97%
Newsletters FP rate: 4.8%

Fortinet's *FortiMail* appliance was one of many products that saw its spam catch rate improve this month – in this case jumping to over 99.9%, with traditional male enhancement and jewellery spam among the few emails that were missed.

The more than 8,500 legitimate emails proved no problem for the appliance, but unfortunately, 11 newsletters in a number of different Western languages did trip the product up, meaning that we couldn't give *Fortinet* another VBSpam+ award. The product's 34th VBSpam award in a row is still something for its developers to be happy with though.

GFI MailEssentials

SC rate: 99.87%
FP rate: 0.00%
Final score: 99.85
Project Honey Pot SC rate: 99.71%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.7%

GFI MailEssentials was another product whose performance bounced back significantly this month: after having been one of several products that saw its catch rate drop in the last test, this time the product blocked 99.87% of all spam sent through it.

Not only that, but it did so without blocking a single legitimate email – and misclassifying only two newsletters. *GFI* thus earns not only its 23rd VBSpam award but its fifth VBSpam+ award.

IBM Lotus Protector for Mail Security

SC rate: 99.93%
FP rate: 0.03%
Final score: 99.72
Project Honey Pot SC rate: 99.82%
Abusix SC rate: 99.99%
Newsletters FP rate: 1.1%

Three legitimate emails were missed by *Lotus Protector* in this test, meaning that there was no repeat of its November

Product name	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score
Axway	8603	0	0.00%	329	131226	99.75%	99.51
Bitdefender	8602	1	0.01%	56	131499	99.96%	99.89
Egedian	8599	4	0.05%	4334	127221	96.71%	96.46
ESET	8603	0	0.00%	129	131426	99.90%	99.87
FortiMail	8603	0	0.00%	115	131440	99.91%	99.76
GFI	8603	0	0.00%	167	131388	99.87%	99.85
IBM	8600	3	0.03%	91	131464	99.93%	99.72
Kaspersky LMS	8603	0	0.00%	122	131433	99.91%	99.91
Libra Esva	8603	0	0.00%	13	131542	99.99%	99.99
McAfee SaaS	8600	3	0.03%	78	131477	99.94%	99.64
Netmail Secure	8603	0	0.00%	300	131255	99.77%	99.69
OnlyMyEmail	8603	0	0.00%	2	131553	99.998%	99.998
Scrollout	8576	27	0.31%	455	131100	99.65%	97.46
Sophos	8595	8	0.09%	142	131413	99.89%	99.43
SpamTitan	8601	2	0.02%	4192	127363	96.81%	96.65
ZEROSPAM	8603	0	0.00%	143	131412	99.89%	99.83
Spamhaus DBL*	8598	5	0.06%	80521	51034	38.79%	38.50
Spamhaus ZEN*	8603	0	0.00%	10693	120862	91.87%	91.87
Spamhaus ZEN+DBL*	8598	5	0.06%	4623	126932	96.49%	96.20

**The Spamhaus products are partial solutions and their performance should not be compared with that of other products. Please refer to the text for full product names and details.*

performance when the product earned its first VBSpam+ award.

Nevertheless, missing fewer than 100 spam emails in an eclectic mix of languages did mean that *IBM* achieved its highest catch rate to date, and thus yet another VBSpam award (the product's 19th) is very well deserved.

Kaspersky Security 8 for Linux Mail Server

SC rate: 99.91%
FP rate: 0.00%
Final score: 99.91
Project Honey Pot SC rate: 99.89%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%

There were only three full solutions that managed not to block any emails in either the ham or the newsletter corpus this month. *Kaspersky*'s *Linux* product was one of them. Happily, it didn't do this by compromising on the spam catch rate, which at 99.91% remains high despite being slightly lower than in the last test (in part due to a single campaign promising 'hot videos'). Yet another VBSpam+ award thus goes to *Kaspersky*.

Libra Esva 3.4.1.0

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%

Several false positives in the last test – the first the product had picked up since May 2013 – meant that 2014 ended on a slightly minor note for *Libra Esva*. In contrast, 2015 has started brilliantly.

The virtual solution developed on the shores of Lake Como

	Newsletters		Project Honey Pot		Abusix		STDev†
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	
Axway	21	7.7%	151	99.68%	178	99.79%	0.5
Bitdefender	1	0.4%	28	99.94%	28	99.97%	0.14
Egedian	1	0.4%	78	99.84%	4256	94.94%	2.14
ESET	3	1.1%	110	99.77%	19	99.98%	0.22
FortiMail	13	4.8%	92	99.81%	23	99.97%	0.18
GFI	2	0.7%	136	99.71%	31	99.96%	0.25
IBM	3	1.1%	85	99.82%	6	99.99%	0.17
Kaspersky LMS	0	0.0%	53	99.89%	69	99.92%	0.2
Libra Esva	0	0.0%	8	99.98%	5	99.99%	0.07
McAfee SaaS	11	4.0%	39	99.92%	39	99.95%	0.16
Netmail Secure	7	2.6%	265	99.44%	35	99.96%	0.37
OnlyMyEmail	0	0.0%	0	100.00%	2	99.998%	0.02
Scrollout	81	29.7%	6	99.99%	449	99.47%	0.42
Sophos	0	0.0%	111	99.77%	31	99.96%	0.2
SpamTitan	4	1.5%	61	99.87%	4131	95.09%	2.07
ZEROSPAM	5	1.8%	87	99.82%	56	99.93%	0.21
Spamhaus DBL*	0	0.0%	19926	58.03%	60595	27.93%	13.41
Spamhaus ZEN*	0	0.0%	8801	81.46%	1892	97.75%	2.68
Spamhaus ZEN+DBL*	0	0.0%	3451	92.73%	1172	98.61%	1.49

**The Spamhaus products are partial solutions and their performance should not be compared with that of other products.*

† 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.)

missed just 13 out of more than 130,000 spam emails. Furthermore, there were no false positives, not even among the newsletters. The product's 11th VBSpam+ award is thus highly deserved.

McAfee SaaS Email Protection

SC rate: 99.94%
FP rate: 0.03%
Final score: 99.64
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.95%
Newsletters FP rate: 4.0%

After an absence of almost a year, it was nice to see *McAfee*'s *SaaS* product return to our tests. The spam landscape is notoriously volatile, so it isn't fair to compare performances between then and now, but a 99.94% catch rate is high even for the standards set by *McAfee* in the past.

There were three false positives and 11 blocked newsletters, meaning that the hosted solution missed out on a VBSpam+ award this time. However, it easily achieved its 16th VBSpam award.

Netmail Secure

SC rate: 99.77%
FP rate: 0.00%
Final score: 99.69
Project Honey Pot SC rate: 99.44%
Abusix SC rate: 99.96%
Newsletters FP rate: 2.6%

In recent tests, spam messages in East Asian languages have tended to be missed by many

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	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Netmail Secure	Proprietary	√	√	√		√		√	
Profil	Bitdefender	√				√		√	√
Scrollout	ClamAV			√		√		√	
Sophos	Sophos							√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√

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

products. This month things were entirely different, but the 300 spam emails missed by *Netmail Secure* were an exception as the majority were written in Chinese, Japanese or Korean.

What matters for this report is that missing just 300 spam mails is a very decent performance, giving the product a 99.77% spam catch rate. Moreover, there were no missed legitimate emails at all – down from six in the last test. All that would have been enough for a VBSpam+ award if it hadn't been for seven missed newsletters (just one too many for the required maximum threshold). The developers of the virtual server may thus feel unhappy – but they should be pleased with their 24th VBSpam award and a generally very good performance.

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.998%
FP rate: 0.00%
Final score: 99.998
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.998%
Newsletters FP rate: 0.0%

The performance of *OnlyMyEmail* in our tests has long been so impressive that we are able to look at each misclassified email individually. In this case, there were just two misclassified spam emails: a rather odd one, possibly

sent in error, and an email from someone who claimed to be looking forward to a weekend with a lot of fun and very few clothes.

Again, there were no false positives in either corpus and yet another VBSpam+ award (the product's seventh in a row) is achieved with the highest final score this month.

Scrollout F1

SC rate: 99.65%
FP rate: 0.31%
Final score: 97.46
Project Honey Pot SC rate: 99.99%
Abusix SC rate: 99.47%
Newsletters FP rate: 29.7%

Scrollout F1 – the free and open-source virtual solution – didn't have a very good test this time around: the product saw its spam catch rate drop, while both the false positive rate and the percentage of missed newsletters increased significantly.

As a consequence, the final score dropped too and ended up below the certification threshold. Thus, after two recent passes, we had to deny *Scrollout* a VBSpam award this time.

Sophos Email Appliance

SC rate: 99.89%
FP rate: 0.09%
Final score: 99.43
Project Honey Pot SC rate: 99.77%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%

In a month in which several products had issues with the newsletters, *Sophos*'s *Email Appliance* didn't block any. Unfortunately, the same couldn't be said for the larger ham corpus, in which it missed eight emails – more than all but one other product.

There was therefore no chance of a VBSpam+ award for *Sophos* this month, even though the product saw its spam catch rate increase to 99.89%. However it did very easily earn its 30th VBSpam award.

SpamTitan 6.00

SC rate: 96.81%
FP rate: 0.02%
Final score: 96.65
Project Honey Pot SC rate: 99.87%
Abusix SC rate: 95.09%
Newsletters FP rate: 1.5%

In each of the last 31 tests it has entered, *SpamTitan* has easily earned a VBSpam award and it has notched up some VBSpam+ awards along the way too. It was thus a little sad to see the virtual solution miss more than 3% of the spam corpus in this test. This was all the more frustrating as it was almost entirely due to a single campaign – something which, in a real environment, a systems administrator might easily have set up a rule to block after a few dozen misses.

We thus had to deny the product a VBSpam award on this occasion, but fully expect it to regain its certified status in the next test.

ZEROSPAM

SC rate: 99.89%
FP rate: 0.00%
Final score: 99.83
Project Honey Pot SC rate: 99.82%
Abusix SC rate: 99.93%
Newsletters FP rate: 1.8%

The last test of 2014 wasn't *ZEROSPAM*'s best, so I had been looking forward to seeing if the product would return to form this month. I am pleased to report that it did.

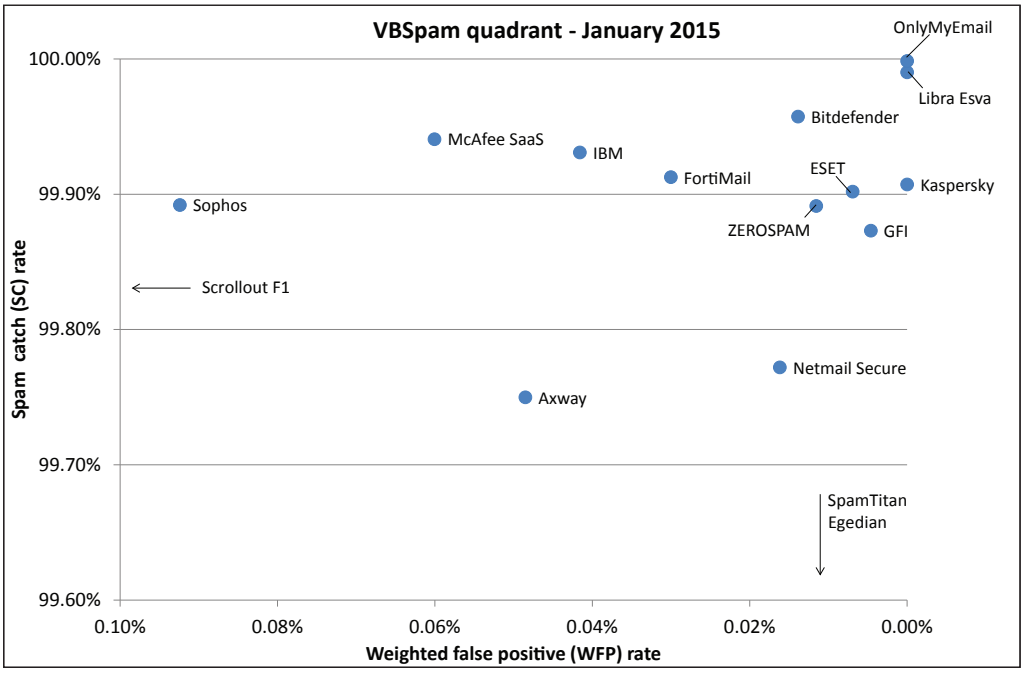
The product's spam catch rate increased to 99.89%, with not a single false positive. Among the newsletters, which in the past have caused some problems for the hosted solution, only five were incorrectly blocked. With an impressive performance all round, *ZEROSPAM* earns a VBSpam+ award – its first since July.

Spamhaus DBL

SC rate: 38.79%
FP rate: 0.06%
Final score: 38.50
Project Honey Pot SC rate: 58.03%
Abusix SC rate: 27.93%
Newsletters FP rate: 0.0%

Spamhaus ZEN

SC rate: 91.87%
FP rate: 0.00%
Final score: 91.87
Project Honey Pot SC rate: 81.46%
Abusix SC rate: 97.75%
Newsletters FP rate: 0.0%



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

Spamhaus ZEN+DBL

SC rate: 96.49%

FP rate: 0.06%

Final score: 96.20

Project Honey Pot SC rate: 92.73%

Abusix SC rate: 98.61%

Newsletters FP rate: 0.0%

In addition to *Spamhaus*'s *ZEN* IP-based blacklist and *DBL* domain-based blacklist, this month we are looking once again at the combination of the two lists: how much does the *DBL* add to *ZEN* (or vice versa)?

In this test, *DBL* reduced about half of the false negatives caused by *ZEN* and took the catch rate of the combined product to close to 96.5% – almost as high as some of the full solutions in this month's test.

That didn't come without a cost though: two domains listed on the *DBL* caused five false positives and served as a good reminder that no technique is without its mistakes: even when blocking less than 40% of all spam (by blocking messages that contain a blacklisted domain name), legitimate emails may also erroneously be blocked.

CONCLUSION

As mentioned previously, spam is notoriously volatile – and so is the performance of spam filters. For many, this was a good month after a somewhat disappointing performance in the November test. For a few others, this month's performance was rather disappointing and marked the end of a long run of VBSpam+ or even VBSpam awards.

As always, we'd like to point out that, in order to get a clear idea of how well a product really performs, it is best to look at several tests in a row.

The next VBSpam test will run in February 2015, with the results scheduled for publication in March. Developers interested in submitting products should email martijn.grooten@virusbtn.com.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Consultant Technical Editors: Dr Morton Swimmer, Ian Whalley

Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/