

virus

BULLETIN

EXCERPTS FROM VIRUS BULLETIN VBSPAM AND VB100 COMPARATIVE REVIEWS: MAY, JUNE, JULY, SEPT, OCT 2010

VBSPAM COMPARATIVE REVIEWS

The VBSpam test uses two live spam streams, which are sent to all the filters participating in the test in random order, thus exposing each to exactly the same email stream, in real time. In addition, hundreds of legitimate emails are sent through the products every day, also in real time. The test measures both the false positive rate and the spam catch rate of the products, and VBSpam certifications are awarded to products that exceed a predefined benchmark based on both measurements.

The test methodology can be found at <http://www.virusbtn.com/vbspam/methodology/>.

AWARDS

A VBSpam certification is awarded based on the 'final score' of a product, which is defined as the spam catch rate (the percentage of spam blocked) minus three times the false positive rate (the percentage of legitimate email blocked). A product wins an award if the value of $(SC - 3*[FP])$ exceeds 96.

$$SC - (3 \times FP) \geq 96$$

It should be mentioned that both the email corpus used in testing and the way in which a test is set up could significantly influence the test results; hence an SC rate of 98% recorded a VBSpam test does not necessarily indicate the same as an SC rate of 98% measured by a customer or in another test.

However, because all products are tested under the same conditions and are required to filter the same emails, the performance of two (or more) products in the same VBSpam test can be compared against each other. The VBSpam test therefore gives customers a good picture of how well a product performs relative to its competitors.



May 2010: BitDefender Security for Mail Servers 3.0.2

SC rate: 99.55%
SC rate (VB corpus): 91.15%
SC rate (image spam): 99.61%
SC rate (large spam): 99.78%
FP rate: 0.14%
FP rate (VB corpus): 0.50%
Final score: 99.14

BitDefender has been submitting its product for testing since the very first anti-spam test and the developers' trust in their product has been rewarded with six VBSpam awards to date. They can now add a seventh award to their collection, which not only makes this the only product to have won an award in every single VBSpam test, but with a very decent and somewhat improved spam catch rate, and just three false positives, *BitDefender* achieved the second highest final score in the May 2010 test.



July 2010: BitDefender Security for Mail Servers 3.0.2

SC rate: 99.91%
SC rate (image spam): 99.89%
SC rate (large spam): 99.69%
FP rate: 0.00%
Final score: 99.91

In the May 2010 test, *BitDefender* combined a very good spam catch rate with just three false positives – which the



developers considered to be three too many. They will thus be pleased to know that there were no false positives this time, while the spam catch rate was unchanged. With one of the highest final scores once again, the Romanian product wins its eighth consecutive VBSpam award.

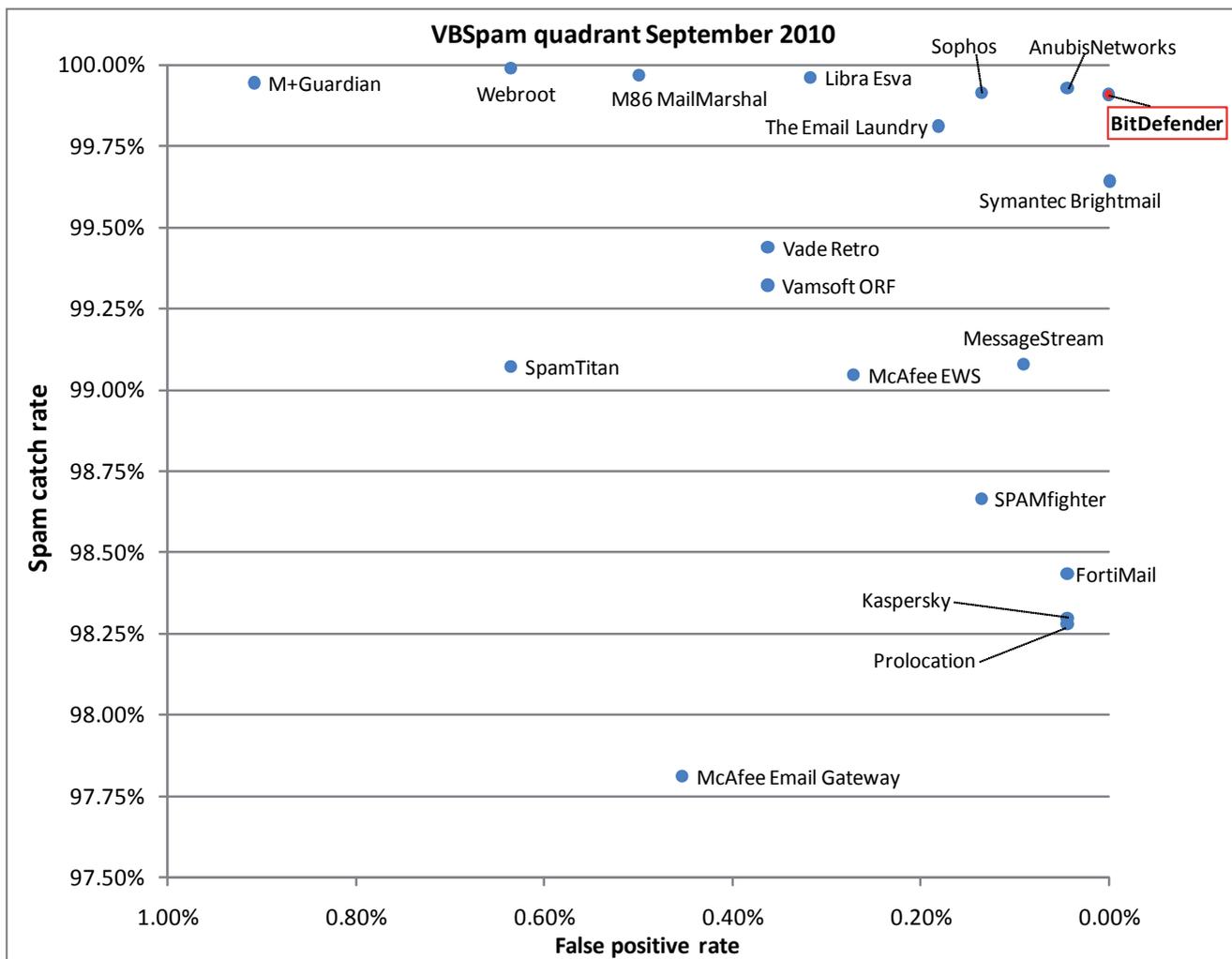
September 2010: BitDefender Security for Mail Servers 3.0.2

- SC rate:** 99.91%
- SC rate (image spam):** 99.81%
- SC rate (large spam):** 99.20%
- SC rate pre-DATA:** N/A
- FP rate:** 0.00%
- Final score:** 99.91

I like it when developers have confidence in their product, and *BitDefender's* developers demonstrated plenty of confidence when they were among the first to submit their product to the VBSpam tests in the early days. Despite their confidence, they have never stopped trying to find ways to improve the product and have always been eager to hear feedback on its performance.



BitDefender Security for Mail Servers is the only product to have won a VBSpam award in every single VBSpam test – and with one of the highest spam catch rates in this test, and no false positives, it outperforms all other products and achieves the highest final score in the September 2010 test.



VIRUS BULLETIN VB100 ANTI-MALWARE TESTING

The basic requirements for an anti-malware product to achieve VB100 certification status are that a product detects, both on demand and on access, in its default settings, all malware known to be 'In the Wild' at the time of the review, and generates no false positives when scanning a set of clean files.



Various other tests are also carried out as part of the comparative review process, including speed and overhead measurements and 'RAP' (Reactive and Proactive) tests.

The RAP tests measure products' detection rates across four distinct sets of malware samples. The first three of these comprise malware first seen in each of the three weeks prior to product submission and measure how quickly product developers and labs react to the steady flood of new malware. The fourth test set consists of malware samples first seen in the week after product submission. This test set is used to gauge products' ability to detect new and unknown samples proactively, using heuristic and generic techniques.

While the results of these secondary tests do not affect a product's qualification for VB100 certification, they are included to provide the reader with a better overall picture of product performance.

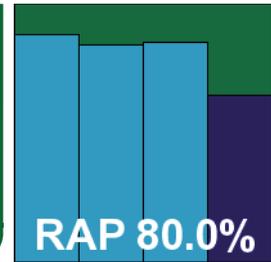
The testing methods of the VB100 certification process are provided in more detail at <http://www.virusbtn.com/vb100/about/100procedure.xml>.

June 2010 - Windows Server 2008 R2 - BitDefender Security for Windows Servers 3.4.11.141

| | | | |
|-------------------------|---------|------------------------|---------|
| ItW | 100.00% | Polymorphic | 100.00% |
| ItW (o/a) | 100.00% | Trojans | 93.17% |
| Worms & bots | 92.87% | False positives | 0 |

A full-blown server solution, using the MMC for its main control interface, *BitDefender's* product installed simply and proved equally straightforward to operate – with rather more colour and panache to the GUI than expected from this kind of approach. Navigation was logical and the scheduling system in particular drew approving nods from the lab team, with a quick and simple set-up process for jobs using a proper calendar for improved efficiency. A

few oddities were noted in some jobs, with a number of subfolders of the selected areas apparently skipped over in some scans, but after careful checking and a few re-runs, a complete set of results were safely in the bag.

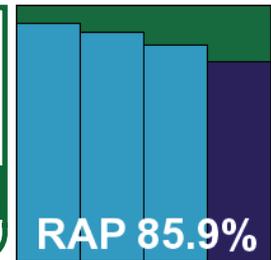


Scanning speeds were pretty good on demand and not bad on access once the product had familiarized itself with the files; the resource usage graph also showed a pretty light memory and processor footprint. Some highly respectable detection figures were obtained in the main sets, with decent coverage across the RAP sets too. The WildList was handled effortlessly, and with no false alarms either *BitDefender* adds another VB100 award to its solid testing history.

October 2010 - Windows Server 2003 - BitDefender Security for File Servers 3.4.141

| | | | |
|-------------------------|---------|------------------------|---------|
| ItW | 100.00% | Polymorphic | 100.00% |
| ItW (o/a) | 100.00% | Trojans | 95.42% |
| Worms & bots | 98.88% | False positives | 0 |

BitDefender's server solution is a fully fledged business product, again using the MMC console for its control system but installing rapidly, with



user interaction kept to a minimum and no need to reboot. The layout is good, making good use of the console base to provide complete and rational access to configuration and control. Scanning speeds were decent on the initial runs, and remarkable on repeat visits to known files, with excellent use of smart caching techniques. CPU use was very low, probably thanks to the same techniques, while memory use was perhaps a little above average.

In the infected sets, we had a few problems with scans apparently completing but presenting only a blank, unresponsive screen. Retrying the scans in smaller batches

yielded better results, implying that the logging system is easily overwhelmed by large numbers of detections – admittedly not something that most real-world users are likely to encounter. Further investigation showed that in some cases we may have been a little hasty, giving up on the logging system after only half an hour or so, as some logs did later emerge after long periods of unresponsiveness.

In the end, we managed to gather all the information needed, which showed solid scores in the infected sets and no problems in the clean sets; *BitDefender* thus earns a VB100 award.



BitDefender
 650 Castro St, Suite 240,
 Mountain View, CA 94041, USA
 Phone: + 1 800 388 8062
 Web: www.bitdefender.com

