virus BULLETIN COMMENT

‘Well executed and comprehensive tests will light the way to better products.’

**Andreas Marx, AV-Test.org**

## MALWARE VS. ANTI-MALWARE: (HOW) CAN WE STILL SURVIVE?

The days of the ‘hobbyist’ virus writer are over. Today’s threats are created by a commercial malware industry which has developed quickly and which has access to some billion-dollar resources. The number of MD5-unique malware samples received by *AV-Test.org* increased from about 333,000 in 2005 to 972,000 in 2006, and 5,490,000 in 2007. The AV industry has reacted to the changing situation by issuing more frequent updates to product signatures. Some vendors have switched from weekly updates to daily, or even half-hourly updates.

*VTEST*, an in-house system we use to measure the response time and proactive detection of 45 AV products, downloaded a total of 111,566 unique AV updates in 2005, compared with 134,484 in 2006 and 148,869 in 2007. These numbers don’t sound too extreme when compared with the number of distributed and spreading malware samples. However, the total size of the updates was only 520 GB in 2005, while we had to deal with 1.0 TB in 2006 and 1.6 TB in 2007. The average size of the signature databases has at least doubled and in some cases tripled within the last 18 months. The trend seems to be clear: more updates and more signatures, and with them longer scan times, higher memory consumption, higher false positive rates and the like.

**Editor:** Helen Martin

**Technical Consultant:** John Hawes

**Technical Editor:** Morton Swimmer

**Consulting Editors:**
Nick FitzGerald, *Independent consultant, NZ*
Ian Whalley, *IBM Research, USA*
Richard Ford, *Florida Institute of Technology, USA*
Edward Wilding, *Data Genetics, UK*

In the past there has often been discussion about the future of signature scanners and speculation as to when they will become obsolete. The AV industry is still alive and quite healthy, however it can only be a matter of time until we need to switch our protection mechanisms to a more effective technology – even if it’s not yet clear exactly what form the future products will take.

One possible solution would be a centralized database containing fingerprints of all known good and bad programs, with online checks being performed for all newly received files. However, such a database would need billions of entries in order to keep up with all the programs and patches being released, and some users might have concerns about privacy. Besides this, of course, there is the question as to who should define what is bad and what I can run on a user’s PC.

One very promising idea is the behaviour-based technology which is integrated in a good number of security suites already. These offer ‘dynamic detection’, based on the knowledge of the typical behaviour of ‘good’ programs and of what combination of actions are likely to be suspicious. In some cases these products present hard to understand or incomplete information to the user, so we need to work on improving these – it is important for the program not to ask the user what to do, but to act automatically, based on all information gathered from the runtime behaviour.

A lot of ideas as to the form future AV products might take have been discussed during the last few months. These include, but are not limited to: buffer overflow protection, URL filtering, web reputation services, browser sandboxing, virtualization, patch management and the like. Let’s see what happens and how, alongside the development of new products, the testing of new technologies matures.

Indeed, it is important for testers to understand the importance of their work, as most developers focus on the aspects of a product that are frequently reviewed by testing organizations and which are used to compare and rank products. Developers often only get approval of the required budgets and help from management if they can be shown to help improve the product’s performance in tests.

Well executed and comprehensive tests will light the way to better products – it is not only the developers who contribute towards the improvement of products. Thus, it is essential for testers to move on to the next level of product testing, focusing on everything besides the ‘traditional’ signature detection. If this doesn’t happen, an entire industry might run into trouble and with it, billions of users may be misled by inadequate tests.