AUTOMATIC QUALITY TESTING AND DISTRIBUTION OF AV UPDATES

Andreas Marx
GEGA IT-Solutions GbR, Klewitzstr. 7, 39112 Magdeburg, Germany
Tel +49 391 6075466 • Fax +49 391 6075469 • Email amarx@gega-it.de

ABSTRACT

Even small changes in the software or databases a program uses can cause significant trouble. This happens especially to anti-virus software, regardless of whether 'only' weekly or daily updates are released. In our tests at the University of Magdeburg (www.av-test.org) we have found a lot of bad updates which have been released in the past. For example, only a small subset of viruses are found or anti-virus programs have destroyed user data due to bugs. So, before publication, it is important to check all parts of the software, and if it fulfils the quality standards. After this, the update has to be released and the customers should get and distribute it to the whole network easily. However, this is quite a complex task.

The idea behind the automatic test process is, that if nothing has changed (by the programmer or virus researcher), nothing should be changed (in the program or detection). First, this includes the detection of viruses. If the previous version has found a special sample as being infected by 'Foo.A', the next version should detect is as 'Foo.A', too, if nothing was changed in the detection part (signatures etc.) or virus names. The next step includes disinfection – the disinfected sample should be 1:1 identical to the sample that an older version has disinfected. This strategy sounds really trivial, however, most companies haven't implemented such strategies yet. Usually, there is only a strategy like 'if everything will be found, everything is good' – without looking at details.

Only the first step (say, how it should be) is time consuming, all other steps can be automated very effective. The paper will go into details and possible problems we found and how they can be solved or avoided. This does not only includes virus detection, disinfected, false positives etc., but other common problems we have found in updated versions, like wrong translation issues. Of course, not everything can be automated, but a lot of human work, time and money can be saved.

The second part of the paper will discuss low-resource consumption update strategies for program, engine and signature files. This includes how to make the signature file updates as small as possible using intelligent or generic compression algorithms as well as push and pull updates. A lot of papers have been written about this topic before, but there are still some details missing – like different behaviour of FAT and NTFS files during daylight saving time and their side effects. Therefore, this part includes theoretical and practical problems and bugs in current scanners and ideas how to improve and speed up the update process even in very large networks using more 'intelligent' mechanisms.

The complete paper and the presentation can be found at http://www.av-test.org during the Conference.