EDITORIAL

The Unbearable Lightness of Testing

Next month sees the publication of the biannual *VB* DOS Scanner Comparative. Despite the rise of *Windows 95* and *NT*, this is still very much our flagship review; the one which garners most attention. It has figures quoted from it left, right and centre, and, inevitably, attracts the most criticism.

The testing of anti-virus products is, as has been well documented in these and other pages in previous years, an incredibly difficult thing to do – or at least, to do well. *VB* is fortunate in being one of the few well-regarded organisations to perform comparative testing: it is not least for this reason that I take such care when carrying out these reviews.

“ it is unreasonable to expect people to have to run multiple programs to detect different types of virus ”

As I write, I have reached the stage where preliminary sets of results are sent to developers in each company – this system has proven worthwhile in the past as far as catching small errors at an early stage goes, and offers time for the results to be discussed and suggestions to be made. Having valuable ideas put forward after publication is not immediately useful, after all…

Say what you like about the people who make virus scanners, each company certainly cares greatly how its product is reviewed. This initial, very restricted, distribution of results inevitably leads to a manifold increase in the level of email coming into my computers, and a flurry of extra checking of virus samples inevitably ensues as developers compare the results of their internal tests with ours.

During this period, there can be a certain antagonism between myself and the developers; testing methodology is often a sticking point. This time, the discussion has focused on the treatment of macro viruses. When it comes to adding new features to a scanner (e.g. the ability to scan with OLE2 *Word* documents), the DOS environment offers more problems than most, the most significant of which is the 640K memory limit.

With scanners already groaning under the load of the ever-increasing number of viruses, adding complex new scan capabilities threatens to be the last straw for some. The clear stopgap solution is to provide a second executable. Simply place the macro-scanning functionality in a program on its own, and the problem is solved – indeed, several products in this January’s tests do this. However, this system has drawbacks. First, re-educating a product’s users to execute *two* programs instead of the one they had to run previously will take time – it is inconvenient for these users to have to adjust their behaviour in this way. And is a one-stop solution too much to ask?

My problem with this particular solution is on a simpler level. Should the detection rate of the product’s macro add-in be included in the product’s score? That is to say, should the macro detector be run over the macro samples and that score added to that of the main program on the more traditional parasitic and boot sector viruses? My conclusion at this stage is that it should not. It is unreasonable to expect people to have to run multiple programs to detect different types of virus – it smacks of the thin end of the wedge. To take the situation to extremes, imagine a product consisting of 9500 separate executables, one for every virus…

Needless to say, the manufacturers of products with add-ins do not agree – to some extent, they are right. It would indeed be unfair to imply that they were incapable of handling macro viruses, so the presence and functionality will be discussed in the article, but they will not be used to form part of the headline detection figures. These will remain the sole domain of the main scanner.

There must be an interesting dilemma in the minds of these companies: on one level they cannot wait for the demise of DOS and its puny memory limits and annoyingly restrictive design. The eventual end to DOS’ incredibly long-drawn-out death throes will bring all that to a close, and relegate problems of this nature to distant memory (at least until the limit of the next OS is reached…). On the other hand, DOS was where it all began for anti-virus companies; it will be a shame to see it fade away. Nonetheless, the products will live on, converted to the new generation of operating systems. Plus ça change, plus c’est la même chose?