

## OPINION 1

# Tests, Tests, Tests – Reviews, Reviews, Reviews

*Peter Morley*  
*Network Associates Inc, UK*

Ray Glath complained in a recent *Virus Bulletin* article (see November 2000, p12) that anti-virus vendors were giving little attention to virus prevention. He went on to say how they were concentrating their efforts on feeding their scanners with data, and were marketing 'scan, scan, scan'.

Ray is, of course, right. As a guilty party, I have been unable to reach the Holy Grail of UVP (Universal Virus Prevention) because I cannot see how to do it. Nor, I believe, can anyone else.

Viruses and Trojans are still flooding in. Each month, I receive up to 12 collections ('a collection' is those items the sender has dealt with in the last month) from other vendors, and I process them all. If we could reach the UVP nirvana, I would not have to do much work, the authors would get fed up with writing them and go back to sex, users could get on with their normal work, and anti-virus vendors could start finding something useful to do.

Meanwhile, the collections have to be processed. Vendors will tell you that each item they fail to handle is a potential field call. When the number of field calls rise significantly, life becomes sheer misery.

I think we have now reached the point where *all* anti-virus vendors are receiving most of these monthly collections, and there are some common elements in the way they deal with them. Most anti-virus reviewers receive them too, and do little with them other than take a few samples to add to their test suites. If they have to change their test procedures, they do that too, but reluctantly.

This article suggests they make a major change. You can expect a lot of resistance, and maybe even some debate!

The rest of the article covers 3 topics:-

- i) What the vendors do.
- ii) What the customers want, and what they want to know.
- iii) What the reviewers could consider, to satisfy the customers.

### **What the Vendors Do (or may do)**

To process a collection, all vendors first scan it with their latest, up-to-the-minute scanner. They are keen to see how much they already handle correctly, because they can

ignore most of it. They then classify the rest into groups, which have to be processed, and they usually do the easy ones first, followed by the ones they don't detect at all. Finally, the oddments...

That first category (which is already handled correctly) is the key. It will split immediately into 2 sub-categories:-

- i) Items which have been processed previously (not of interest).
- ii) Those which have not been seen before. These tell you how you are doing with any generic techniques being used.

Most vendors now take the approach that when they get a second variant of a virus they already have, they do a little extra work, to avoid having to do any work at all on the third and subsequent variants. That's what I mean by generic techniques, whether they are called that or not.

When they get a new group of viruses, these should be handled so that further variants are already non-events. In my case, I usually find we already catch over 60%. That 60% was 50% some two and a half years ago, and raising it has been a long hard slog. The 60% will rise slowly, but it may never get to 75%. That's the closest I think we will get to UVP, and it does not include prevention, which is a separate, extremely difficult exercise. As for the viruses not already detected, they have to be processed.

### What the Customers Want to Know

At *Virus Bulletin* conferences I get a chance to talk with lots of customers, and (what a surprise!), some of them ask awkward questions, and even make awkward comments.

How about this one, from a fairly large customer: 'I read reviews in *VB*, and find that all vendors detect nearly all the viruses. There are occasional problems, most of which have already been fixed by the time I read about them. But I

know that some vendors occasionally fall well behind. Remember Solomon's in 1993. How do I know which ones are falling behind now?'

Or this: 'You continually make a point about generic handling of viruses (at least he had read some of them!), but I never seem to get comments from reviewers. How



do I know you *really* detect and repair viruses you've never seen? And even if you do, how do I know it matters?'

### Possible Actions by Reviewers

I am writing this section as a result of a discussion between Igor Muttik of *Network Associates Inc* and Andreas Marx, of the University of Magdeburg. Andreas had already considered these problems and was beginning to take steps to handle them.

I should like these proposals to be considered by *all* reviewers, even if the result is outright rejection, and outraged written comment!

- i) Set up a test suite, which will change every time, and which consists of the latest monthly collections from *Sophos*, *Kaspersky Lab*, *Symantec* and *NAI*. Other collections could also be included. But make no attempt to edit these collections, or to remove the rubbish, (even leave in the few OFFVs!) and make it clear that detection failures are not up for discussion. Each time, use *only* the latest collections.
- ii) Review the test suite using *two* different editions of the same product from each vendor being reviewed.
  - a) Two months old
  - b) Four months old

In the case of the two-month old product, I mean not the latest but the one before that. This will give a view of how good the vendors are at processing what they currently get, since items they processed two months ago will appear in other vendors current collections.

In the case of the four-month old product, detection rates will be much lower, and will reflect the ability of the vendors to handle what they have never seen.

### Possible Effects of Accepting My Proposals

There will be considerable pressure from vendors who underperform to use the latest product too. If reviewers have to give in to this, it should be an additional test, not a substitute test.

I can see that there might be a lot of discussion about the effect of heuristic options, and whether they should be used at all. Most importantly, these proposals mean a substantial amount of work! However, they will produce useful debate, perhaps not least about the usefulness of the WildList.

The range of test results will be large compared with the range of traditional test results, and may vary, depending on how vendors respond to the new results. Last but not least, the question of whether the tests should replace traditional tests, or be done in addition. In my view, replacement would be preferable, because of the workload involved. I would like to hear your feedback, either direct to me or via the Editor of *Virus Bulletin*.