FEATURE 1

A View from the Lab

Peter Morley
Dr Solomon's Software

[*The views expressed here are those of the author, and are not necessarily endorsed by* VB. *Ed.*]

Nearly four years ago, I was invited into the Virus Lab at *S&S* (now *Dr Solomon's*), and have not escaped since. It is a strange and peaceful place, providing a unique vantage point from which to view the computer industry in general, and the machinations of the small group of anti-virus companies in particular. These can be more entertaining than old-fashioned music hall, but music hall jokes were more credible than some of the advertising literature I see!

Some History

In September 1993, there existed over 3000 viruses and variants, and most anti-virus companies could detect nearly all of them. There was a *laissez-faire* attitude to whether it was necessary to deal with every new virus, and most organizations had a 'backlog' of a couple of hundred viruses. As I saw it, we were in the middle of the wolf pack and running hard. The first question which came to mind was 'What do we have to do to get so far ahead that the others can't bite our tails?'

I was told by Alan Solomon that there were fewer than ten people in the world with the knowledge and experience necessary to disassemble new viruses, and write the code to deal with them. We calculated that we needed to process 150 viruses per month as well as new ones, so that by mid-1994 there would be no backlog. At the time, about 50 viruses per month were being processed, with laborious analysis performed on each. To increase from 50 to 150 per month required both more manpower, and totally different work practices. Mid-1994 came and we made it, albeit a month late.

I think Alan was the first anti-virus guru to perceive that processing had to become an efficient, no-frills, production operation. That realization has made him a multi-millionaire. I was joined by Dmitry Gryaznov, already acknowledged as one of the top ten experts, and Duncan Long, whose assembly language skills were adequate to design and write his own Operating System. It was up to me to provide the production operation.

As I write this, in July 1997, new viruses and variants are appearing at over 250 per month. There are occasional gluts, such as the release of the two Ludwig CD-ROMs, and the shenanigans of the past three months. There seems to be a quiet patch each August and September, but do not bank on it this year!

Any organization which cannot process 300 viruses per month in times of stress, has no chance of keeping in the game. We have been joined by Igor Muttik (another of the the top ten), and we *have* processed all the viruses (14,117 as detected in *Dr Solomon's AVTK* v7.75) which have come our way. These are passed freely between members of the anti-virus community, so any processing omissions are *not* due to 'We haven't seen it'. They are due either to a failure to implement the necessary resources and working practices, or to a deliberate policy of only processing a subset.

Anti-virus Organizations

As I see it, anti-virus organizations can now be split into three categories. Category A comprises those which process nearly every virus. I personally know of four such companies – the others are *Sophos*, *Alwil*, and *AVP*. These organizations excel in technical competence, and are pretty good at technical organization. This does not, necessarily, mean their products sell well. I recall the early, derisory efforts of what was then *S&S* in the US market… which are now being rectified. Further, *AVP* seems to have made little effort outside the former USSR. This indicates that the emphasis has been on virus detection rather than on making user interfaces really friendly. *Dr Solomon's* is putting this right, too.

Category B's companies are those which try to process every virus, but fail. They fail because they do not put in place the necessary organization and resources. To them, virus processing is just another part of the programming operation. This has little or no bearing on commercial success. With top-class user interfaces, and excellent marketing to a customer base which cannot adequately test the product, in geographical areas with little competition, commercial success is still virtually assured.

It is possible for organizations to slip from category A to B. This happens gradually, one day at a time. Could a company move back up? Bearing in mind that back in 1993, *every* anti-virus organization was in category B, the answer must be 'yes'! The simple way is to arrange to use the engine, and/or detection database from one of the category A companies. Early in 1997, *McAfee* introduced *VirusScan* v3.0, which suddenly detected more than 1000 additional viruses and variants (I actually tested!). I do believe in fairies, but not in miracles. History shows that there is a rational explanation for them; in this case incorporating another scanning engine helped.

Category C consists of companies which accept that they cannot process every new virus, and which advocate alternative strategies. These include prevention and change detection. Subset processing is a third tactic. All this is as old as the hills. Prevention and change detection are two of the wider facilities also offered by category A and B companies. Both play a part in a comprehensive anti-virus strategy, in addition to the use of scanners.

Change detection, as a main weapon, becomes less attractive when you have to perform it on every macro in your word-processing suite. Also, it is totally ineffective when you have just installed a major new set of software from CD-ROM. You have to wait and see if running the new suite causes executables to change. If it does, you have more work to do. Maybe a lot more work.

The WildList

Before discussing this term (which I hold in some disdain), let me suggest a scenario, and pose a question. Someone telephones our technical support unit, and says 'We've just had a bad outbreak of a virus which adds 1027 bytes to each executable, and I'm sending some samples. None of the present anti-virus scanners, including yours, detects it. It seems to affect boot sectors on hard disks, too. Please ring me as soon as you have looked at the samples.'

All absolutely normal. The virus, in this case, was Junkie, a kid's stuff multi-partite virus, distributed via the Internet and suddenly world-wide. The samples came to me, and I contacted the sender, explaining the virus (and the fact that it infected floppies too), and arranging to send an Extra Driver by return, so he could detect all instances, and repair them. Everyone was happy.

My question is 'Do you want to minimize the number of times the above scenario occurs? Or are you happy to telephone your anti-virus vendor, even when they have had the virus for months, but have not bothered to process it?' Your workload will be lighter if your scanner identifies and repairs the virus, and you will not need to make the call. If your vendor hides behind an 'In the Wild' list, the scenario will occur much more often. Various people have different ideas, but the one most used is attributed to Joe Wells. For a virus to get on this list, two of Joe's 'reporters' must have received samples of it from the field.

Each month I receive about six new viruses from our distributor in India. As far as I'm concerned, they are 'in the wild', but they will not make the official WildList until another vendor finds and reports them. This may be several months later, or never. It seems that India may be a little *too* 'wild'! I also come by forty or more South American viruses every month. I do not get them directly from the 'wild', but I have no doubt many of them are in it. I process them all, but they are not reported to Joe by *Dr Solomon's*. Later on, when they *are* 'in the wild' over here, and Findvirus detects and repairs them, nobody will call, so they may *never* get on the list.

The latest Ludwig CD-ROM contains well over 4000 viruses and is available world-wide to anyone who is prepared to pay. A third version may be imminent, providing several thousand more. Some IT managers bought the second release to test anti-virus products. (This is a misconception; when the list becomes available, it is already several months out of date, and will fall behind by another month, for each month which passes.) Relatively few of the viruses on it are on the WildList, which contains less than 600 of the 1500 viruses which I believe to be truly 'in the wild'. Even 1500 may be an underestimate – it is just 10% of the viruses known to exist.

My conclusion is that the WildList is an excuse often adopted by those vendors who cannot handle the viruses they receive. It is of no value whatever to end-users, or to category A vendors. The WildList has progressed from an indication of what should be processed next to an excuse for falling well behind in the game. Some category A vendors use it for no better reason than that they used to be category B, and are just continuing the habit. I see that as playing second division football, *after* promotion! Some will disagree with my conclusion, but few will dispute that any such list will inevitably be at least three months out of date, or that there are hundreds of field viruses which never get listed, particularly those which do not go memory-resident, and which are easy to clean up.

Opting Out

Macro viruses have provided a heaven-sent opportunity for category B and C vendors to claim that boot-sector and file viruses are now relatively unimportant, and the essential strategy is to protect against *Word* macro viruses which are now becoming prevalent. Try telling that to a German IT manager who has just had an outbreak of the Manzon virus! Of course, since there are fewer than 1200 macro virus variants, these vendors have not fallen too far behind in processing these yet.

The Choice

Some corporate IT managers find it difficult to choose software because they do not have the viruses against which to test. They, like me, may be suspicious of advertising claims (particularly those destined to be drawn to the attention of the ASA), and even more so of the adverts' omissions. If you wish to select one of two or three vendors, and are in the market for a site licence, try the following approach.

Ask each vendor to provide the latest shipping version of the software in question. Suggest they hold a half-day event, at which you can test each of the three products against a virus library to be provided. This should consist solely of those viruses which the vendor has added to his own detection capability in the last six months. If you want to be really fair, remove the last two months. You will not meet the Cascades, Jerusalems and Dark Avengers of yesteryear, but you can expect the samples to include new viruses received from the 'wild' by that vendor. If your vendor is category B or C, you will soon know! Try to handle the folklore as kindly as you can. The procedure I suggest has a major advantage for you – the vendors have nowhere to hide.