COMMENT

“ I must admit I did not envisage a multi-billion dollar AV business back then. ”

The Bigger Picture

I have a confession to make. In 1992 a friend of mine lent me all his back issues of *Virus Bulletin*. Very quickly I became hooked on the magazine. Before you attempt a guess I should let you know that my confession has nothing to do with worms of any kind …

Although my English was good enough to understand the footnote of each page of the magazine, I was not quick enough to read through all the issues in the short space of time available. Thus an illicit plan to copy all the three years of back issues entered my mind. Before I knew it I had copied all the magazines and returned them at the last minute to my friend (who obviously did not expect such reprehensible behaviour from me!). And now you know – I have confessed!

During the relatively short history of *VB* the content has changed a great deal. Do you remember the list of ‘known PC viruses’ with detection strings? How about the list of ‘known Mac viruses’? Oh dear, it’s been a while! I have a very clear memory of visiting the post office with a few hundred packaged diskettes to send out my anti-virus program’s quarterly (!) updates. The girl behind the glass looked back at me over the small mountain of diskettes and screamed while the line behind me stretched out onto the street. I must admit I did not envisage a multi-billion dollar AV business back then. My view of the AV industry has changed considerably over the years. It has been a great journey. I have seen it all, from freeware to shareware and from small to major corporate business. User requirements have changed a lot during these times, as has my understanding of the bigger picture. So what did I learn?

The same heuristics that appear to work with thousands of happy customers might not be an acceptable solution where there are millions of users. False positives (‘FP’s as we call them in the lab) might be generated when you start to scan millions of files. While your FPs with a thousand happy customers will never reach the visibility range, even a minor FP could cost you a fortune where there are millions of users who can become unhappy in the blink of an eye.

Some AV vendors might prefer to pack all the features into the scanner: we emulate DOS, *Windows* and the Internet. Where will be the end to all this? How much more code and data can be packed into our products? It is hard to say! An assembly-written scanner used to be a cool thing. ‘Speed is everything’, you say. Well hold on there, Tommy. Today’s diversified networks need integrated solutions from the desktop to the server on a variety of domains. IA32 is a good thing to support, but can the product run on *Itanium*? How about running on *Solaris* systems or AS400 to name just a few? *Virus Bulletin* tests have not covered such platforms but it would be interesting to measure these capabilities. And the assembly-written engine might not be able to resolve your problem. In this ‘everything, everywhere’ scenario you need portable solutions that can perform the same way both on demand and on access, and on a variety of platforms. It is interesting to see how many products already show differences in scanning performance on access and on demand.

The one thing you will always need is reliable detection. Reliable detection takes more than a good scanner that might work once in a while. You need a very stable solution. If a scanner does not handle the polymorphic and metamorphic threats very well, what can you expect in an emergency situation? Is it good enough to catch up with such detections six months or a year later? I do not think so. However, this argument often makes me want to tear my hair out as I work towards providing a standard response time. As Alan Solomon used to say ‘the virus lab always feels like being on a treadmill’, there is absolutely no time to waste.

In this business things happen so quickly! When we were all talking about macro viruses there was already something else knocking at the door: Win32 viruses. Now that we talk much more about Win32, there is already a set of new threats at the door: exploits built into computer viruses. These new threats need integrated security solutions. Yet more interesting times are ahead!

Péter Ször, Symantec Security Response

VIRUS BULLETIN **©2002 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /2002/$0.00+2.50**