

# CONFERENCE REPORT

## VB 95: Reaching the World

'I like to be in America; OK by me in America...' The words to the famous Leonard Bernstein song seemed very apt as the plane touched down at Boston's Logan International Airport; the beginning of *VB 95*. Over the next two days, delegates and speakers from around the world would register at what has become the world's most respected conference on computer viruses, held annually by *VB*.

This year saw an increase in the number of talks presented, with one corporate and two technical streams. Previous years have seen delegates concentrating on one or other of the streams: 1995 brought changes, with many attending a mixture of talks in all streams. Discussion centred on cooperation; on sharing of knowledge and information.

### Kick-Off

The first session of the conference was, as ever, the introductory talk on computer viruses by Dr Jan Hruska of *Sophos*. The seminar was well-attended, and gave delegates the opportunity to familiarize themselves with the current state of play in the anti-virus world.

Thursday morning's opening address saw many slightly bleary-eyed following the previous evening's cocktail reception sponsored by *McAfee Associates* (offers for next year's events, producers?!), but a blast of a certain Rolling Stones song, much touted with the advent of *Windows 95*, shook everyone out of their somnolescent states.

*VB* editor Ian Whalley discussed the pros and cons of *Microsoft's* latest operating system, and the ease with which *Windows 95*-specific viruses may be written. He also addressed problems associated with new types of viruses, particularly with regard to Concept (a topic which was to surface again and again over the next two days).

Professor Harold Highland, one of computing's 'elder statesmen' (who prefers to refer to himself as one of its dinosaurs), gave an informative and interesting keynote talk on his experiences in computer security – in fact, a short history of computer viruses. The first macro virus, to his knowledge, was written in 1989 – by Highland himself! After experiments, he realized its ability to spread was vast, so he stored it in a secure place, hoping such a virus would never be seen in the wild – this year saw that hope dashed.

### The First Goals

After a welcome coffee break, the conference separated into one corporate and two technical streams, and the real work of the day began. Sarah Gordon (*Command Software*) opened the corporate stream with an extension on her last year's talk on the

psychology of the virus writer; addressing the more general issues of why viruses are written and how to encourage end-users to implement anti-virus strategies.

At the same time, the technical streams had Jonathan Lettvin (*Lotus*) discussing the PC boot sequence, and *ESaSS's* Frans Veldman lecturing on one of his areas of expertise, heuristics. Paul Ducklin's (*Sophos*) presentation on learning from mistakes was salutary, and illustrated how human weakness could lead to errors being made and even remade.

After lunch, *VB's* technical editor, Jakub Kaminski, gave a talk on the Flash BIOS, and the problems which can arise when the BIOS contents are reprogrammed. He was followed, in the other technical stream, by *Symantec's* Shane Coursen, who gave a very topical lecture on the vulnerability of *Windows 95* to viruses. In his view, the discovery of the Concept virus shows that new types of virus are becoming more prevalent.

After the tea-break, while presentations were held in both technical streams, Wes Ames (*Boeing*) led a Corporate Stream discussion forum on problems encountered by IT security managers.

### Half-Time

Happily, Friday morning's sessions began somewhat later than the previous day's – after a large gala dinner, and an enormously entertaining casino evening, some faces still only surfaced after the coffee break!

Paul Robinson, editor of one of our fellow security publications, *Secure Computing*, opened the corporate stream for the final day with a lecture on how to test and review anti-virus products. Other highlights of the morning included Righard Zwienenberg's talk on heuristic scanners (involving two eggs!), and Pavel Lamacka's discussion as to whether it is possible to have harmless/useful viruses – he believes not.

Roger Riordan of *Cybec* was scheduled to give a talk on IDE hard disk security; however, as he had been rushed to hospital for emergency surgery just days before he was due to leave for the conference, a colleague, Robert Stroud, gave the talk in his place – twice, by popular demand! Riordan, however, did rush a specially-made videotape over from Australia, so that he could at least introduce his talk.

The afternoon sessions saw some of the heavyweight anti-virus 'names' take the rostrum: Fridrik Skulason on the latest trends in polymorphism, Dmitry Gryaznov on the future of the scanner, Steve White on a global perspective for computer viruses, and Jim Bates on virus writers. Former *VB* editor Richard Ford (now at the *NCSA*) presented a stimulating talk (including last-minute alterations and additions) on this year's most-discussed topic; macro viruses.



Fridrik Skulason at VB 95; here discussing things other than CARO and beer drinking!

The conference closed with an invigorating and lively panel session, in which speakers were posed questions by their audience. On the panel were Jim Bates, Paul Ducklin, Richard Ford, Sarah Gordon, Mike Lambert, and Steve White. This session carried on almost naturally from Richard Ford's talk on macro viruses, and led to the somewhat surprising discovery that many of the delegates had been caught by Concept, and that, in the larger companies, infections went into the hundreds.

Steve White posed the theory that macro viruses could possibly supplant all other types of virus, in terms of prevalence. Another speaker, Jonathan Lettvin (this time as part of the audience), put forward the widely-shared view that macro viruses are the beginning of a large new problem.

Discussion on the efficacy of product reviews followed, with participation from vendors, researchers, and a VB journalist. Much of the audience felt that disinfection should be an integral part of anti-virus software, and calls were made for comparative reviews of that capability.

### Taking a Gamble

Contrary to what readers may think after reading thus far, not every waking hour was spent with viruses, viruses, viruses – there was certainly time for play! Many delegates brought their partners, who enjoyed an extremely busy partner's programme on the first full day of the conference, touring Boston and its environs, and seeing local sites of historical interest.

Thursday night's Gala Dinner was, as always, enjoyed by the great majority of delegates and guests – the food was superb, as it was throughout our stay at the *Boston Park Plaza*, and copious amounts of wine were available for those of us who imbibe. In a departure from previous years, some delegates brought not only their partners, but also their children – they (and the grown-up children!) were kept entertained throughout dinner by roving magicians who performed card tricks and made balloon models.

After dinner we were regaled with a cabaret, the most memorable point of which was the artiste balancing a stepladder – indeed, at one point, there were two! – on his chin. The cabaret was interrupted from time to time, as had been much work on the previous day, by fire alarms – the broadcast message will stick in many memories for some time: 'The cause of the alarm is still being investigated. There is no need to leave your rooms...'

The real entertainment of the evening was the casino, with blackjack, roulette, a 'wheel of fortune', and crap tables. Every 'gambler' was given \$50,000 (sadly, fake...) on entering the ballroom, with the promise of a bottle of champagne to the person who won the most 'money' by the end of the night. This correspondent was proud of a \$285,000 final total [*I went bust. Ed.*], until realising that the winner, Maureen Morar, had made a cool \$¾ million.

This year saw another departure from tradition – rather than a speaker's dinner, there was a whale watch for speakers and staff. Despite warnings of heavy seas, most speakers decided to brave it, and were rewarded with sightings of five whales. Unfortunately, sightings of lunch proved more elusive: after a fire on the bottom deck, most of the food was ruined. However, as luck would have it, while Jan Hruska and the crew were running around putting the fire out and throwing smouldering cloths overboard, Philip Statham and Chris Baxter had the foresight to apply themselves to rescuing the sandwich trays, and managed to salvage enough to keep the weary travellers going until the end of the trip. Why do fires seem to follow the VB Conference so faithfully... ?

### Thanks and Thoughts

A great deal of hard work went into the organising: thanks are due to many people, in particular Dale Tabrum for sterling work in keeping everything under control and 'holding the fort' in England while we were all away, and to Julia Line for masterful efforts with conference papers and proceedings. Thank you to Penny Halliday and Kim Ducklin for helping out in Boston, and to conference pro John Merne for assisting our conference manager Petra Duffield. Petra, as always, was the brains behind the operation; special thanks to her. We understand she is already thinking about VB 96 (did someone mention Tahiti, Petra?).

Thanks of course to all the speakers; many more than there was space to mention in this report (apologies to those not covered). Without their expertise and their commitment, this conference could never have taken place. Finally, a vote of thanks to all the delegates: your active participation and continuing interest are the reasons we hold this conference.

The *Proceedings of the Fifth Annual Virus Bulletin Conference*, with copies of papers given at the event, are now available from *Virus Bulletin* offices; contact Dale Tabrum or Petra Duffield for information.

Those delegates who have not submitted a completed assessment form (to be found inside the Proceedings) may still do so – these enable VB to continue to improve next year's conference.