CONFERENCE REPORT

TOTALLY TORONTO: VB2003

Helen Martin

As the plane touched down in Toronto, the *Virus Bulletin* crew felt a certain sense of déjà vu: through the plane's windows, all that could be seen was torrential rain and a flooded runway. On countless occasions over the course of the last year we felt we could have kicked ourselves for having tempted fate as blatantly as with the closing slide of VB2002: '*See you in Toronto – come if you dare …*'

Toronto seemed like a perfectly 'safe' location for a conference but, as the organisation of the conference progressed, the world's media reported the outbreak of SARS in Toronto – and when the W.H.O. issued an advisory against travel to the city, the future of VB2003 hung in the balance. However, *VB* remained confident that Toronto would recover quickly and our optimism was rewarded when the city was declared a safe destination only a couple of weeks later.

A massive power cut across a large part of North America was the next to wobble our nerves and, in the week leading up to the conference it was with disbelief that we heard reports of a hurricane travelling toward the East coast of North America, and heading inland. But, despite initial concerns, the rain on arrival in Toronto was about as far as the similarities to VB2002 would go and VB2003 proved to be possibly one of the smoothest-running *VB* conferences on record.

THE FULL FAIRMOUNTIE

This was *VB*'s second visit to Canada, and the welcome was every bit as warm as the first. The grandeur of the Fairmont Royal York provided the perfect setting for the 13th *Virus Bulletin* conference. Characters of legend looked down on dining delegates from the magnificent hand-painted ceiling of the Ballroom, while the two conference halls were spectacularly ornate (and a healthy distance between the halls ensured that delegates had truly earned their chocolate cookies by coffee break).

Wot, no disasters? The relieved VB team.

An exhibition was set up in the spacious hallway between the two conference rooms and featured booths from *CA*, *Eset*, *Sophos*, *NAI*, *ICSA Labs* and *Virus Bulletin*. A caricaturist made an entertaining addition to the *NAI* booth and was kept busy by a constant stream of subjects waylaid en route between conference sessions.

As usual a drinks reception was held on the eve of the conference. Conversation, beer and wine flowed freely and our bona fide Mountie was kept busy talking to and posing for photographs with *VB* delegates. In fact, such was the draw of RCMP Allen Rodgers in his eye-catching uniform, that a stream of delegates from a different event sneaked along the corridor to have their photographs taken with him too.

Now, that's magic!

After the Canadian-themed welcome drinks, the entertainment for this year's gala dinner was on a magical theme. British magician David Penn made his way around the dinner tables amazing delegates with his award-winning close-up magic. His stage act followed and, for half an hour, all eyes in the room were glued to the stage while he performed the seemingly impossible. After dinner there was plenty to talk about as the naturally analytical minds of AV experts battled with the frustration of not being able to answer to the question: 'how *did* he do that?'. Theories were in abundance, but David Penn wasn't giving anything away.

THE PROGRAMME

With a wide range of AV-related subjects on the programme, delegates had plenty to choose from – indeed, some were heard lamenting the fact that they were not able to be present in both streams at the same time.

In the corporate stream, presentations by Chuck Springer and Jeannette Jarvis provided real-world examples of how large corporations deal with threat assessment and incident management. David Phillips outlined the reasons for setting up a new Open University course on 'vandalism in cyberspace', while David Perry proclaimed that it is not user education that is needed, but user understanding.

Bruce Hughes brought delegates up to date on *ICSA Labs*' progress with the Real-Time WildList. The project has involved developing a system which will allow WildList reporters to submit virus reports weekly, daily or even hourly. Bruce anticipated that HTTPS upload for sample submission should be available by the end of 3Q 2003 and that an online database will be ready by the end of 4Q 2003.

In the technical stream, Frédéric Perriot discussed his research into the use of code optimization techniques in

Richard Ford, James Wolfe and Shawn Campbell discuss their frustration with virus naming.

dealing with polymorphic viruses. Kurt Natvig showcased the use of the sandbox described in his papers at VB2001 and VB2002 to demonstrate the capabilities of real-life virus samples. Martin Overton picked up from where John Morris left off at VB2002 and described his own use and development of John's SMB-Lure design, while Neal Hindocha and Eric Chien impressed the audience with a practical demonstration of vulnerabilities in instant messaging.

VB2003 saw the introduction of a new style of panel discussion. The single vs multiple engine debate involved six AV vendor representatives debating the merits of single engine and multiple engine scanning methods. Thankfully disagreements were confined to the 40-minute session and intervention was not required to end any squabbling.

At the close of day one, a discussion panel was held on the subject of anti-virus testing. Panel members Michael Parsons (*West Coast Labs*), Larry Bridwell (*ICSA Labs*) and Matt Ham (*VB*) explained their current AV testing practices, outlining the factors that limit the ways in which they can test products. The panel members concurred that, given unlimited resources and time they would carry out a range of tests that would challenge aspects of anti-virus products *other* than their in the wild detection rates.

The traditional close of conference panel discussion was devoted to the emotive subject of virus-naming. It wasn't quite the virus-naming discussion to end all virus-naming discussions, but it provided the opportunity to hear from AV researchers (including CARO members) and from real-world end users who experience regular frustration and difficulties as a result of the lack of virus-naming standards.

AND SO TO VB2004 …

VB2003 was blessed with a very enthusiastic and faultlessly professional team of organisers, helpers and audio-visual crew, without whom the event would not have run as smoothly. Thanks are due to all those who helped put the conference together, to the conference sponsors and, of course, to all of the VB2003 speakers and panellists.

Not ones to rest on our laurels, we hope to build on the successes of VB2003 to make VB2004 a better event still. And now to the burning question: where will VB2004 be held – Zanzibar, Dublin, Baghdad, Chicago, Casablanca or Kathmandu? While contractual issues currently keep the location of VB2004 under wraps, all will be revealed shortly. Watch http://www.virusbtn.com/ for details.