CONFERENCE REPORT

ONE TOWN THAT WON'T LET YOU DOWN ...

Helen Martin

'Chicago is one town that won't let you down', sang Frank Sinatra in *My Kind of Town*. Well, it certainly didn't let *VB* down – VB2004 ran smoothly (not a hurricane, infectious disease, customs delay or terrorist attack in sight), with record delegate numbers and was described by a number of delegates as the best *Virus Bulletin* conference they had attended.

WON'T YOU PLEASE COME TO CHICAGO

The Fairmont Chicago provided a luxurious venue for the 14th *Virus Bulletin* conference. The hotel's positively palatial conference rooms were ideal for what was the largest audience the *VB* conference has ever had, with more than 330 in attendance. And such was the hotel's impeccable service that barely an eyelid was batted when the request was made for the video-taping, and later screening, of the US presidential debate. Delegates were able to sit back and enjoy Thursday's gala dinner, safe in the knowledge that they would be able to keep up to date with politics later in the evening.

BORN IN CHICAGO

VB2004 saw the *VB* conference's first ever 'pre-conference' sessions, on Wednesday afternoon.

Each of the four conference sponsors was invited to make a 50-minute presentation on a topic of their choice. Representing *Trend Micro*, David Perry kicked off the afternoon's proceedings with a look at the players and faces of the anti-virus industry. Andrew Lee followed, with a look at 'The *Eset* virus radar', and the afternoon was rounded off with sessions from Sam Curry, who presented an overview of the ever-evolving threat environment for *Computer Associates*, and *Microsoft*'s Matthew Braverman, who spoke about the role of security in the company's vision of seamless computing. All sessions were well attended and each of the sponsor representatives must be congratulated for steering well clear of marketing babble.

Also taking place on Wednesday afternoon was the 'AVIEWS Live!' discussion forum. Andrew Lee hot-footed it from his *Eset* presentation to chair the session, in which a panel of five AVIEN members each introduced a subject of interest then opened it up for discussion. Such was the popularity of the AVIEWS forum that some attendees were overheard expressing disappointment at the brevity of the *two-hour* session. Indeed, the feedback from delegates on all of the pre-conference sessions was overwhelming – you liked them and you want more!

After a gentle warm-up for the conference on Wednesday afternoon, the evening's drinks reception provided the traditional opportunity for delegates to have a couple of drinks, catch up with acquaintances and make some new ones – indeed, the organisers of the conference were delighted that this year's conference saw an influx of new faces as well as the regulars.

YOU'LL LOSE THE BLUES IN CHICAGO

Over the years, the *Virus Bulletin* conference has become well known for two things: mishaps and great entertainment. Given the former, some might say it was a brave, or even reckless, decision to engage an entertainment act for the gala dinner comprising a husband and wife team who shoot at each other with 125-pound cross bows.

But world record holders Ross and Elisa Hartzell were faultlessly professional and their astounding skills had everyone on the edge of their seats (for some reason delegates kept their distance from the stage). The jaw-dropping finale of the act involved a William Tell-style performance in which Ross Hartzell fired a single arrow to trigger a rally of shots which ended in the simultaneous impaling of apples balanced on each of the couple's heads.

As something of a relief from the tension aroused by the first act of the evening, the raucous Blooze Brothers rounded off the evening by playing into the night in true Chicago style – and even managed (eventually) to persuade a respectable number of delegates to abandon their seats for a makeshift dance floor at the front of the room.

To add (further) to the excitement of the evening, *VB* decided to hold a charity auction of special, limited edition 'VB2004 Chicago Virus Expert' baseball caps. Delegates were

invited to submit sealed bids, the idea being that the top 30 bids would each win one of the highly sought after caps. Somewhat foolishly, *VB* had overlooked the mischievous japes and capers that tend to arise as a direct result of plying delegates with alcohol – and by the end of the evening certain conference attendees had *apparently* pledged more than $30,000. Luckily, the sharp eyes of the *VB* crew members managed to sort the real from the bogus, and a total of $828 was donated to Geekcorps, a division of the International Executive Service Corps which places technical volunteers in developing nations.

SWEET HOME CHICAGO

This year's conference programme saw the first *VB* conference stream dedicated to spam. A series of four presentations relating to spam and anti-spam techniques took place on Friday morning. John Graham-Cumming, author of email sorting program POPFile, provided an overview of the trends in content trickery in spam. John Morris and Chris Lewis gave us an insight into the anti-spam infrastructure at *Nortel Networks*, and described the lessons that have been learned over the five years since its deployment. Steen Pedersen looked at the Sender Policy Framework (SPF), and Phyllis Schneck focused on the epidemiology of spam.

Also on the programme, of course, were the old regulars the corporate and technical streams. Past editor of *VB* Richard Ford, now of Florida Institute of Technology (FIT), presented Gatekeeper II, a generic virus prevention system developed by researchers at FIT. Richard's students Jason Michalske and Matt Wagner gave a live demonstration of some of the spin off tools of the system, including Gatekeeper Yo Yo – a tool which undoes all the changes made by an application – as well as Gatekeeper's viral behaviour detection capabilities.

Eric Chien introduced *Microsoft Shell*, a scripting platform currently in beta which is due to ship with *Longhorn*. After introducing the architecture and language syntax of *MS Shell*, Eric gave a series of demonstrations of *MS Shell*'s functionality, looking specifically at the functionality of which he belives worms, viruses and other miscreants are likely to take advantage.

Steve Garfink and Mary Landesman's presentation started with an AV game show, 'The Virus Price is Right', in which volunteers from the audience were asked to guess the correct answer to 'How big is Sobig?'. Of course all of the choices, ranging from $50 million to $36 billion were correct, each having been quoted by various analyst firms in the media. Steve and Mary went on to describe how a malware cost forecasting system can be used to provide more useful figures for the cost of virus attacks, on an individual organisation basis.

John Lyons provided a fascinating overview of what the UK's National Hi Tech Crime Unit is doing towards crime reduction and its intelligence regarding organised crime on the Internet, in particular phishing and DDoS attacks.

A panel discussion on malware threats to mobile devices took place on Friday afternoon – just 24 hours after the first confirmed reports of SymbOS/Cabir in the Wild. Panellists Vanja Svajcer, Mikko Hyppönen, Randy Brown, Chris Lewis and John Alexander agreed that, while we have not seen any really concerning malware for mobile devices yet, they are likely to become prime targets for malware in the near future – both in terms of malware coming from 'traditional' virus writers/script kiddies and malware written with the specific aim of collaborating with spammers.

David Perry led the closing panel session of the conference, 'What is an infection?'. David and *ICSA*'s Larry Bridwell are about to embark upon a project which, through surveys, ballots and open discussion, will attempt to define 16 AV terms over the course of one year. Panel members Jeannette Jarvis, Andrew Lee, Steve Christie, Nick FitzGerald and Richard Ford each described some of the problems they encounter with the lack of clarity in AV terminology (in their roles as customer, vendor, government representative, 'elder statesman and curmudgeon' and academic, respectively). In general, there was agreement that the lack of clarity in AV terminology is a problem, but there were few concrete suggestions as to how to solve the problem. David himself admitted that he and Larry think they 'should completely be able to fail entirely to [define the 16 terms] in one year'. Watch this space!

VB2005: THE IRISH ROVER

After three years in North America, the time has come for *VB* to visit European shores once again. VB2005 takes place 5–7 October 2005 in Dublin, Ireland. You can book your place for VB2005 now at at http://www.virusbtn.com/. Put it in your diaries and join us next year to experience the legendary craic in Dublin!