

# CONFERENCE REPORT

## IN DUBLIN'S FAIR CITY

Helen Martin

VB2005 was a double record breaker – *Virus Bulletin's* longest and largest conference to date. We were delighted to welcome well over 360 delegates to The Burlington hotel in Dublin for the debut of the event's new longer format – and, for the second year in a row, the conference was described by delegates as the best *VB* conference they had attended.

### THE IRISH ROVER

In a change from tradition, this year's conference programme kicked off at 2pm on Wednesday afternoon, but delegates also had the option of attending sponsor presentations in the morning. Each of the four conference sponsors (*BitDefender*, *Computer Associates*, *Eset* and *Trend Micro*) was invited to make a presentation on a topic of their choice and the result was four highly engaging and well attended sessions – their popularity largely due to the companies' excellent selection of speakers and topics (and their wise decision to steer clear of too much self-promotion).

By 2pm, as the last of the delegates took their seats for the conference opening address and the opening credits rolled, the larger of The Burlington's two conference halls was filled almost to capacity. Amongst the crowd it was great to see a large number of familiar faces – some of whom we hadn't seen since the conference was last in Europe a couple of years ago – as well as a very respectable number of new faces, who we hope will also become conference regulars.

Four presentations in each stream (technical and corporate) made for a relatively gentle start to the conference on Wednesday afternoon and gave delegates a taste of what was to come over the course of the next two days.

Despite the new start time and the new format, some *VB* traditions are not for changing. One of these is the informal welcome drinks reception held on Wednesday evening. This year drinks were served in the hotel's Buck Mulligan's bar – a traditional Irish-style bar which was soon packed to the rafters with *VB* delegates sampling the local 'water'.

Indeed, the local water became something of a theme at the VB2005 – rarely was a *VB* delegate seen without a glass of the stuff in their hand (after hours of course), and if you don't believe me, just take a look at the photographs!

### WHEN IRISH EYES ARE SMILING

If the turnout for the conference was good, the turnout for the gala dinner was exceptional, the numbers boosted by accompanying partners as delegates took the opportunity to



*Pure genius – the cream of the AV industry relax after hours at VB2005.*

show their loved ones that *VB* conferences are not all work and no play. The 420 diners were led Pied Piper-style into dinner by four barefoot Celtic drummers who then proceeded to raise the roof with a spectacular performance on stage, culminating in a frenzied crescendo that was enough to leave ears ringing through the first course of the meal.

Continuing with the traditional Irish theme, the evening's entertainment was rounded off by a Riverdance-style dance troupe who gave a highly energetic performance that was enough to get even the most rhythmically-challenged tapping their toes.



## THE SERIOUS STUFF

Of course, between the fun and the Guinness breaks there was a very full programme of presentations which provided excellent fodder for lobby lounge discussions long into the evening.



Continuing where we left off last year, the spam stream was expanded for VB2005, with presentations in both the corporate and technical streams. On the corporate side, Oren Drori looked at commercial and non-commercial ways of fighting spam, Dmitri Alperovitch revealed some of the interesting spam-related statistics drawn from *CipherTrust's* sender reputation systems, and Jamz Yaneza looked at some best practices for evaluating anti-spam solutions. In the technical stream, Dmitry Samosseiko must be congratulated, not only for managing to keep his audience alert and engaged first thing on Friday morning, but also for drawing a sizeable crowd while Vesselin Bontchev presented in the other stream – neither of which could be described as a mean feat.

Ex *VB* editor Nick FitzGerald explained why he believes user authentication is a bad idea – even going so far as to say that authentication is ‘worse than nothing at all’. John Graham-Cumming described his experience of introducing ‘pseudo-words’ to his Bayesian text classifier, and Matthew Prince reported on the work of Project HoneyPot, urging engineers to work together with legislators and law enforcement officials in the fight against spam.

Vesselin Bontchev pulled the crowds in with his presentation on the current status of the CARO Malware Naming Scheme. As well as describing the scheme in full, Vesselin took the opportunity to make a mini-presentation, explaining in his own indomitable style why he believes *MITRE's* newly-launched Common Malware Enumeration (CME) initiative will end up causing, rather than alleviating, confusion.

In the technical stream Jarno Niemelä revealed ‘what makes *Symbian* malware tick’ and, with a little help from able assistant Mikko Hyppönen and a video camera, demonstrated *Symbian* Trojans in action live on stage.

Eric Chien outlined some of the ways in which spyware makes its way onto users’ machines and described the methods used by spyware to build profiles of its victims. He

illustrated the type of detailed data that is relayed by spyware applications. Meanwhile, Joe Telfaci and Seth Purdy presented the results of several weeks investigation into ‘the Transponder Gang’, a convoluted network of interrelated sites, people, companies and unwanted programs, highlighting some of the difficulties that are faced by spyware researchers.

Jason Bruce concentrated on spyware’s close relative adware, presenting his ideas on defining ‘acceptable’ adware so that malicious adware can be blocked while legitimate advertisers can be free to go about their business.

Other highlights included Martin Overton’s comprehensive overview of bots and botnets, in which he detailed the full extent of the problem and called for improved security policies and procedures. Charles Renert outlined *Microsoft's* Data Execution Protection (DEP) and put it to the test against recent exploitation techniques – concluding that, although not a cure-all, DEP is a laudable first step in the fight against vulnerability exploitation. And Kimmo Kasslin demonstrated the stealth techniques used by advanced *Windows* rootkits as well as presenting techniques for detecting hidden objects.

This year’s panel discussions were lively as usual. The first of these sessions, led by Gabrielle Dowling, was based around the subject of information provision in a virus outbreak situation. Although the discussion was somewhat hijacked by the topic of media reporting (see p.2), panellists Nick FitzGerald, Eric Chien, Jeannette Jarvis, Dmitry Gryaznov, Andrew Lee and Martin Overton did manage to air some of their opinions. In the second panel discussion, chairman David Perry asked panellists Vesselin Bontchev, John Aycock, Costin Raiu, Andrew Lee, Morton Swimmer and Alex Shipp ‘who is hiding the virus writers?’ but alas the 50-minute time slot was insufficient for the investigators to truly get to the bottom of the matter.

There is not enough room to mention more than a small selection of the presentations here, but my thanks go to all of the VB2005 speakers for the time and effort they invested – the overall standard of papers this year was exceptional and key to the success of the event.

## CANADIAN QUEEN

Although pleased with this year’s achievements, it is in the nature of the *VB* team to strive to put on an even better event next year, and planning has already begun for VB2006. Next year *VB* will revisit Canada, this time landing in Montréal – a city that effortlessly combines French flair with North American modernity. The conference will take place 11–13 October 2006 at the Fairmont The Queen Elizabeth. I look forward to seeing you there.