CONFERENCE REPORT

MONTRÉAL IN THE FALL

Helen Martin

This year the *VB* conference travelled to the second largest French-speaking city in the world – the vibrant Canadian city of Montréal. The venue for this year's event was the Fairmont Queen Elizabeth – a hotel whose claims to fame include having hosted the second of John Lennon and Yoko Ono's legendary 'bed-ins'. John and Yoko spent seven days at the Queen Elizabeth in 1969, during which they recorded the song *Give Peace a Chance* in the hotel.

There was no time for bed-ins at the *VB* conference though: continuing the trend of the last two years, VB2006 was the longest and most content-filled *Virus Bulletin* conference to date. The full three-day format seemed to be a hit with delegates, with a greater number of presentations on offer, as well as increased networking (and drinking?) time.

GETTING THE BALL ROLLING

The conference programme kicked off at 10.30am on Wednesday morning and straight after the official conference opening Mikko Hyppönen took to the stage for his keynote presentation 'Case: Virus X'. At least that was the plan. Mikko explained that he had been prepared to present an interesting case study of a several-month-long criminal investigation with which he had been involved, which had followed the movements of a for-profit botnet gang. Unfortunately, three weeks prior to the conference Mikko received a phone call from a 'friendly police officer' telling him he couldn't speak publicly about the case. Instead, Mikko pulled together a sharp and entertaining presentation on the major developments in malware over the last 20 years. While possibly not as sexy a subject as originally planned, the presentation was exceptionally well executed and got the conference off to a roaring start.

Rob Murawski followed with a presentation that was the start of what proved to be something of a theme for the conference – Rob was the first of several speakers to look at different aspects of cybercrime, his presentation concentrating in particular on how attackers steal sensitive data.

Wednesday afternoon saw the conference split into its traditional two-stream format (technical and corporate). Peter Cooper and Stefan Görling battled it out in the corporate stream over the virtues or otherwise of user education. Stefan Görling was first to speak, the crux of his argument being that, since security will always be a secondary goal for users, teaching them how to be safe online will never solve any problems. Peter Cooper's paper, meanwhile, argued that user education can be significantly more effective if the information is presented in an appropriate manner. Peter illustrated a variety of different learning styles and gave examples of how information can be presented to cater to each, thus maximising the amount of information users process and take away with them. Peter was unlucky enough to suffer from hardware failure during his presentation, when his Mac laptop unexpectedly shut down. The mishap couldn't have been more brilliantly timed however, since his very next slide (once re-booted) advised 'be memorable' – raising a round of applause and laughter from the audience and leaving many wondering whether the hardware failure had been a deliberate stunt. (We are assured that it was merely a fluke.)

The serious business of day one was rounded off at the end of the afternoon with sponsor presentations from the two platinum sponsors of the conference. *ESET*'s Andrew Lee and *BitDefender*'s Beau Roberts both presented papers looking at heuristic detection, with both sessions being well attended.

Of course, at the end of day one that only left the *other* serious business: the VB2006 drinks reception. Four of Montréal's most talented caricaturists set up their easels in the hotel's Hochelaga rooms and were soon frantically sketching the night away as delegates lined up for their turn to be depicted in amusing situations, cartoon style. Some of the results can be seen above.

IN THE MIDDLE

Day two of the conference kicked off bright and early with presentations by Jeff Williams and Roel Schouwenberg in the corporate stream, and Jim Wu and Aleksander Czarnowski in the technical stream. Aleksander's presentation – which took an in-depth look at rootkits and anti-rootkit safeguards – was the subject of much discussion and media attention as he indicated that features of *Microsoft*'s imminent *Vista* release will likely be abused by hackers and malicious code writers within several months of its release.

Alex Shipp presented a paper on targeted trojan attacks, revealing that of the three million pieces of malware *MessageLabs* sees each day, an average of only seven will represent targeted trojan attacks. Alex illustrated the ease with which such attacks can slip under the radar with an example of one targeted trojan, identified months previously, for which just four anti-virus products included detection. Alex concluded that, while the good news is that the probability of a company being attacked successfully is extremely low, the bad news is that the potential cost of such an attack is very high indeed.

Later in the corporate stream, Guillaume Lovet's presentation – illustrating the business models of cybercriminals – raised some eyebrows in shock when he indicated that phishing attacks could be more profitable (as well as significantly less risky) than the manufacture and sale of hard drugs.

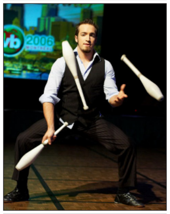
Thursday afternoon was dedicated to papers covering corporate and technical aspects of spam and phishing, amongst which birthday boy Dmitry Samosseiko and his colleague Ross Thomas provided an analysis of modern spam techniques, and Dmitri Alperovitch revealed how easy it has become to create customized phishing trojans. With do-it-yourself trojan creation kits ranging from approximately $100 to $5,500, it's a sobering thought that even the most technically inept criminal can create trojans that will go undetected by most AV engines.

In the technical track Vipul Sharma revealed how spammers' obfuscation tactics can be exploited to improve spam filtering and showed how *Proofpoint* had constructed a custom classifier for 800 commonly obfuscated words.

Thursday afternoon's programme culminated with a discussion of the work past, present and future of the Anti-Spyware Coalition. This was followed by an off-schedule birds of a feather (BoF) session organized by John Graham-Cumming on the subject of image spam – which John reports was well attended with some interesting discussions.

CIRQUE DE VB

Of course, no *VB* conference would be complete without the annual *VB* gala dinner and cabaret. Every year *VB* invites delegates to dress formally for the occasion – while equally warmly welcoming those who prefer not to, of course – and every year *VB* is delighted by the turnout of beautifully preened delegates. This time was no exception as the photographs below testify. Entertainment for the evening was provided by three jaw-dropping cirque-style acts followed by the beautiful music of the François Dufresne jazz band.



Starting the evening off was Sam Alvarez who wowed the room as he demonstrated a stunning combination of grace, strength and flexibility in his aerial tissue performance. Next up was Throw 2 Catch, a highly entertaining juggling duo whose energetic act made juggling with nine batons look easy. Finally, all eyes were on Genevieve Bessette's dizzying aerial hoop performance high above the stage. After dinner the dulcet tones of the François Dufresne jazz band provided the

perfect background for relaxed after-dinner conversation as the evening came to a close.

UNLUCKY FOR SOME ...

Day three of this year's conference fell on Friday 13th. While the *VB* conference organizers try to avoid superstition where possible, when taking into consideration the catalogue of disasters that have befallen *Virus Bulletin* conferences over the past 16 years we couldn't help but feel a little apprehensive waking up on the morning of Friday 13th. Happily, however, our fears were allayed when the final day of the conference went without a hitch.

Adam O'Donnell and Masaki Suenaga should be congratulated for braving the early morning shift on the morning after the night before. In the event, both presentations drew respectably sized audiences and the number of bleary eyes spotted was minimal.

After coffee John Morris and Eric Kedrosky showed how their forensic tool, 'the inspector', has resulted in a fivefold reduction in the number of infections seen on systems in their organization. As an aside, John revealed to the audience in the corporate stream that he uses *Linux* because he believes it currently to be less vulnerable to viruses than *Windows* – confessing that he only said so because he felt safe in the knowledge that all those with a strong 'belief' in Unix viruses were likely to be next door. Which indeed they were – listening to presentations by Patrick Knight, Jakub Kaminski and Marius van Oers on Unix malware, *Linux* threats and Macintosh OSX binary malware, respectively.

Paul Ducklin started his presentation with some audience participation. Paul asked all those with laptops in the audience to follow his directions and delete notepad.exe – then revealed that we had just witnessed the recreation of a little piece of malware history, it being 19 years to the day (Friday 13th) since the payload of the Jerusalem virus first activated. Paul's presentation itself was less historical and was based around the question: 'Can strong authentication sort out phishing and fraud?'. Thankfully Paul resisted the temptation to provide a single-slide, one-word answer to the question and instead gave a lively and informative presentation.

The highlight of the conference for many was Randy Abrams' presentation. With a title as provocative as 'Microsoft AntiVirus – extortion, expedience or the extinction of the AV industry?' it was little surprise when delegate after delegate filed in for this potential showdown from the former *Microsoft* employee. Recognising the potential for some lively discussion and controversy from this particular presentation, session chair Jan Hruska began the session by dashing off stage only to return seconds later to the tune of *Ride of the Valkyries* and wearing protective headgear. As the delighted audience snapped away with their cameras at the tomfoolery, Randy himself seemed a little concerned, saying 'It's a sobering thought to think that the last living picture of me could be with him in it!' After that it was down to the serious business of the presentation. Randy's presentation was entertaining and informative and he gave a balanced and considered opinion on what *Microsoft*'s entry into the AV market will mean for the rest of the industry. He was a little less kind to other AV giants, most notably *Symantec*, and although the majority of attendees took his comments in good humour, a letter from Randy is published in this issue (at his request) as an addendum to his presentation.

The closing panel session saw the 'Internet Strike Force' (David Perry, Righard Zwienenberg, Alex Shipp, Stacy Arruda, Jeannette Jarvis and Larry Bridwell) discuss different aspects of fighting international cybercrime. Strangely no one came forward when the panel challenged 'If anyone in the audience is a member of organized crime, please raise your hand.' As is often the case with these panel sessions, the discussion could have gone on long into the evening, but had to be cut short as the conference came to a close. No doubt it is a topic that we will return to time and again in the future.

While there has not been enough room here to mention more than a small selection of the presentations, I would like to extend my thanks to all of the VB2006 speakers (and the reserve speakers who stood on standby with their papers but were not needed this time) for the contributions they made to the conference. Some of the slides from their presentations, as well as more photographs of the event will be available soon at http://www.virusbtn.com/conference/vb2006/.

VIENNA WAITS FOR YOU

As always, the organizers of the *VB* conference appreciate the feedback delegates provide (we do read *all* of the assessment forms). It is clear from this year's feedback that the inclusion of a good deal more technically focused material is in order for next year. A call for papers for VB2007 will be issued next month, so if you think you are up to the job, start preparing your submission now!

VB2007 will be held 19–21 September 2007 in the beautiful historic city of Vienna, Austria. I look forward to seeing you there.

Photographs courtesy of: John Alexander, Jeannette Jarvis, Andrew Lee, Petr Odehnal, Martin Overton and Eddy Willems.