CONFERENCE REPORT 1

GENEVA CONVENTION

Helen Martin

This year the *VB* conference landed on the shores of Lake Geneva – or, perhaps more accurately, at the end of the runway of Geneva International Airport. The Crowne Plaza hotel, a mere 0.5km from the airport terminal, is a haven for plane spotters, boasting uninterrupted views of the runway from one end of the building, yet internally free from the slightest sound of a jet engine thanks to the wonders of modern glazing technology.

A free tourist bus pass made the venue's distance from the centre of town seem significantly shorter, with the 10-minute ride into the city taking in such sites of international significance as the UN European HQ and the High Commission for Refugees before arriving in the centre of Geneva, where the crystal waters of Lake Geneva sparkled against their backdrop of majestic mountains (when they appeared from the mist that is).

The run-up to this year's event was surrounded by a certain amount of uncertainty – as will have been the case for many businesses, we waited anxiously to see what the effects of the global economic downturn would be. Having heard rumours of travel budgets having been slashed in this company and that, we braced ourselves for a slightly more modest turnout than in recent years. However, we were thrilled by an even stronger turnout than last year, with the final number of attendees just a handful short of *VB*'s largest conference to date. The number of delegates in attendance this year and the level of support from sponsoring organizations are, I think, a testament to the industry's recognition of the importance of sharing insight and knowledge, debating and challenging ideas, and encouraging coordinated global efforts to combat cybercrime.

IN THE BEGINNING

The conference kicked off on Wednesday morning with a presentation by Eric Davis, head of *Google*'s Anti-Malvertizing team, who called for industry-wide cooperation in an effort to help combat malicious web advertising – a serious problem not only for *Google* and other search sites but also for the sites that rely on ad syndication networks, and for users of the web in general.

The conference then split into its usual two-stream format, with Pascal Lointier looking at incident response from a financial perspective, while *Microsoft* trio Elda Dimakiling, Scott Wu and Francis Allan Tan Seng unravelled the various malware attacks linked to the MS08-067 vulnerability – looking not only at Conficker but at a number of other malware families that use the MS08-067 exploit to spread.

Next, Juraj Malcho asked 'Is there a lawyer in the lab?' as he explored the boundaries between legitimate and illegitimate applications and the minefield that exists for vendors in making a decision regarding an executable's intentions (and thus whether or not to include detection for it). He highlighted the increasing frequency with which labs are forced to consult with legal teams regarding applications that are sufficiently dubious to warrant detection, yet which proclaim just enough legitimacy to potentially cause problems for a vendor that detects them.

Later in the afternoon another *Microsoft* researcher, Chun Feng, provided a fascinating look at five generations of Dogrobot – a family of malware that has caused more than $1.2 billion in losses from Chinese Internet cafés using a novel rootkit technique to hijack System Restore on *Windows*. Meanwhile, Guillaume Lovet gave a comprehensive overview of the technical, juridical and ethical challenges of fighting cybercrime.

EAR PLUGS ANYONE?

Wednesday evening saw the first of the main networking events of the conference – the VB2009 drinks reception. Delegates were greeted at the entrance to the reception by two magnificent St Bernards. Each weighing in at around 65kg, both Beetoo and Caspar proved to be gentle giants and took the hustle and bustle of the crowd and the non-stop paparazzi-style photography in their (very large) stride. Of course, for Beetoo (formal name Beethoven), the glitz and glamour lifestyle is in the genes as his owners proudly revealed that he is a direct descendant of the canine star of the 1992 film *Beethoven*.

Some VB delegates brought their own supplies in case the free drinks ran out...

...while for others, the drinks reception was too much to handle.

At the opposite end of the bar from our canine guests an altogether more raucous form of entertainment was on offer (if I'm honest, it was a little difficult to ignore). Yodeller extraordinaire Barbara Klossner and her group of musicians, Les Amies du Lac Léman, began by providing a rousing demonstration of traditional Swiss yodelling. The mantle was then passed over to the audience for *VB*'s first (and hopefully last) yodelling competition.

Compère Jan Hruska started proceedings with a quick demonstration of his own yodelling skills (or lack thereof) to the tune of 'Happy Birthday' and then threw the competition open to the floor. A steady stream of would-be yodellers lined up to take the mic. At one point concern was expressed for the distinct possibility that all the wine glasses in the room might shatter around us, but mercifully 'Happy Birthday' proved to be just brief enough to save the glassware. A three-strong judging panel awarded marks out of five for each contestant, eventually declaring Björg Olafsdottir the undisputed winner.

IN THE MIDDLE

Thursday morning kicked off with a presentation by Raoul Chiesa, a former hacker who is now Technical Liaison Officer on Cybercrime Issues at the United Nations Interregional Crime and Justice Research Institute (UNICRI). Raoul provided a fascinating insight into the Hackers Profiling Project, the first project to be dedicated to the criminal profiling of hackers. Meanwhile, Maik Morgenstern and Andreas Marx of *AV-Test.org* discussed the limitations of current in-the-cloud security solutions, highlighting privacy, security, reliability and fault tolerance issues.

Next to take to the podium was *Sophos* researcher Dmitry Samosseiko who took a detailed look at the Russian partnerka – the hundreds of well-organized affiliate networks and webmasters that make millions of dollars of profit each year through the online sales of unlicensed prescription medicine, fake designer goods, fake anti-virus, and so on. Dmitry exposed their economic model, revealing statistics and information including the typical amount of money a partnerka webmaster could expect to earn each day, as well as highlighting some of the tools and techniques of the 'trade'.

VB delegates show off their yodelling skills while the judging panel keep smiling through the pain.

After a break for mid-morning coffee and pastries, Bryan Lu took to the stage for a look at the different ways in which security companies display threat levels. He called for standardization of the way in which computer and Internet threat levels are assigned in order for these to be useful and have any meaning.

Righard Zwienenberg followed, with an update on the current state of the Anti-Malware Testing Standards Organization (AMTSO) and on the progress the group has made since its early beginnings in 2007.

The first of this year's anti-spam papers came after lunch on Thursday, with *Kaspersky* team Darya Bronnikova and Anna Volodina presenting a detailed look at SMS fraud – a criminal activity that is common in Russia and the former Soviet countries but rare in Western countries, the discrepancy largely being due to the fact that Russian mobile network providers do little to prevent fraudulent activities, while in the West the risks of being caught are significantly greater. *Microsoft*'s Terry Zink was next up with an interesting look at how *Microsoft*'s *Exchange Hosted Services* mitigated the problem of outbound spam – not only that, but the multi-talented Terry also delighted the audience with a card trick and by making a coin vanish into thin air (although on reflection, given the astronomical bar prices at the venue, the crowd might have been more impressed had he made coins appear out of thin air). Finally, another *Kaspersky* duo, Darya Gudkova and Andrey Nikishin, presented a round-up of different anti-spam legislation across the world, looking at where it is effective and what additional legislation is needed to help the global fight against spammers.

Later in the afternoon Methusela Ferrer highlighted the issue of Mac security, looking at malware threats on *Mac OS X*. Methusela outlined the underlying motives and methods used by a number of Mac threats. Despite a small technical hitch, the presentation was one of the most popular of the conference – demonstrating that Mac security is very much being taken seriously by the industry's top researchers.

Thursday also saw this year's selection of last-minute presentations – eight shorter papers that were submitted and selected just three weeks prior to the conference in order to allow more up-to-date material than the rest of the papers which take several months to produce.

Dmitry Bestuzhev kicked off the last-minute papers with a colourful presentation on the thriving Brazilian banking trojan scene. With close to 23 million users of the major online banks in Brazil, combined with the fact that the country is the largest source of banking trojans in the world, banks have a tough challenge in fighting the problem. If nothing else, most delegates came away from the presentation with a sense of relief that they don't bank in Brazil.

Researchers from *Trend Micro* and *Kaspersky* focused on social-network-aware threats. Ivan Macalintal from *Trend* presented research carried out by his colleagues on the Koobface worm – the first piece of malware to successfully and continuously propagate through social networks. Ivan described what Koobface does, what makes it successful and how cybercriminals are monetizing it – concluding that the worm is still a work in progress and more developments are likely. Afterwards, *Kaspersky*'s Costin Raiu and *Trend Micro*'s Morton Swimmer collaborated on a presentation that focused on *Twitter* attacks – both researchers are working on separate projects analysing the volume and nature of *Twitter*-related threats and exploring patterns of abuse. The pair revealed that AV firms currently scan around half a million unique URLs posted to *Twitter* every day in their search for malicious code.

Other last-minute highlights included Igor Muttik discussing the Industry Connection Security Group's XML schema for sharing samples and information among vendors and testers and Erik Wu's presentation of the results of a three-month case study of more than 600 real-world botnets.

FUN AND FROLICS

Of course, no *VB* conference would be complete without the traditional gala dinner evening. As usual, members of the AV industry turned out in all their finery and elegance – I have to say that, as a crowd, the AV industry scrubs up pretty well!

The dinner was accompanied initially by the mellow and melodious tones of a trio of alphorns, and towards the end of the meal we were treated to a charming performance by Swiss mime trio Due piu Uno. Their repertoire was witty, touching, energetic and delightfully entertaining, with a mixture of slapstick comedy, music and acrobatic feats, all timed to perfection.

IN THE END

The final morning started off bright and early at 9am with a presentation by *Kaspersky*'s Stefan Tanase taking a look at the evolution of Web 2.0 threats and at the likely direction in which they will develop in the future, while *BitDefender*'s Claudiu Musat described a system for extracting novelty from an unsorted spam flow. *VB*'s own Martijn Grooten followed with a presentation outlining the essentials of anti-spam testing, while another *BitDefender* researcher, Catalin Cosoi, returned once again to the topic of Web 2.0 as he described a fractal approach to the detection of social network spam.

Fun and frolics with Due piu Uno.

The most popular presentation of the conference took place later on Friday as John Graham-Cumming described JavaScript security as 'the elephant in your browser', pointing out that the security situation with JavaScript is so poor that the only solution is to kill it.

The conference concluded with a panel discussion led by Paul Ducklin, in which two 'teams' (*Sophos*'s Graham Cluley and *West Coast Labs*' Lysa Myers, facing *McAfee*'s Greg Day and *Lockheed Martin*'s John Alexander) debated the virtues of free anti-virus versus paid for anti-virus and the issue of rogue anti-virus products. Aside from the entertaining debate, the award for the best moment of the conference must surely go to Mikko Hyppönen, who was called upon to ask a question in the style of Vesselin Bontchev – all I can say is that it was as if the great man himself was in the room.

AND FINALLY...

There has not been enough space to mention more than a small selection of the speakers and presentations here, but I would like to extend my warmest thanks to all of the VB2009 speakers for their contributions, as well as to sponsors *CA*, *ESET*, *K7 Computing*, *IKARUS Software*, *Kaspersky Lab*, *Kingsoft*, *Lavasoft*, *eScan*, *OPSWAT*, *Sunbelt Software*, *TrustPort* and *Beijing Rising* for their support.

Next year the *VB* conference makes a return visit to the stunning city of Vancouver for its 20th birthday, with the conference taking place 29 September to 1 October 2010 at the Westin Bayshore, Vancouver, Canada. I very much look forward to welcoming you all there.

Photographs courtesy of: Pavel Baudis, Jeannette Jarvis and Tjark Auerbach. More photographs will be available soon at http://www.virusbtn.com/conference/vb2009/photos.