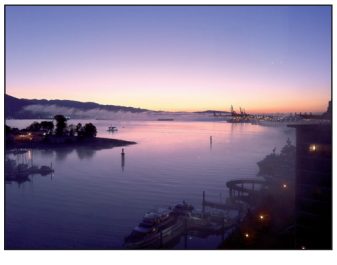
CONFERENCE REPORT

VANCOUVER EXPEDITION

Helen Martin

Last month saw the conclusion of VB2010 – marking the 20th anniversary of the Virus Bulletin conference – in Vancouver, Canada. It was *VB*'s second visit to Vancouver, the last sojourn having been for the ninth *VB* conference, in 1999. The vibrant, multicultural city of Vancouver, with its spectacular natural surroundings, frequently tops the charts as one of the best places to visit in North America, has been ranked among the top ten restaurant cities in the world, and has often been voted as one of the world's most liveable cities. With all that under its belt it's a wonder it took us 11 years to return!



The Westin Bayshore hotel provided the perfect setting for the anniversary celebrations, with stunning views across the bay to North Vancouver and along the seawall to Stanley Park. Even the weather gods smiled on the 20th birthday of the conference, generously giving us some beautiful Indian summer weather in late September (not that the conference team got to experience it, but the outside world looked nice as we peeked through the windows).

Whether it was the appeal of the beautiful city of Vancouver, the buzz surrounding Stuxnet, or simply the industry's recognition of the importance of getting together to share insight and knowledge, this year's conference exceeded all expectations in terms of delegate numbers, with a turnout of more than 360. In a period in which budgets are still tight as world economies begin the slow process of recovery we were thrilled to see such a large turnout – although the credit is surely due to the presenters and the papers on the schedule for creating such a draw.

THE OPENER

The conference kicked off on Wednesday morning with a keynote address by *Facebook* malware researcher Nick Biologorskiy. Nick revealed that the six-year-old social networking site – which has only been available to the public for the last three years – has over half a billion active users worldwide, and that 56% of these log into the site every day. With such a large user base and high profile, the site is a prime target for attackers and security is a high priority for the company. Nick detailed some of the many different types of attack targeting the site, and explained how the company's security team works to shut them down – revealing that the majority of attacks are unsuccessful thanks to behind-the-scenes security, and the ones the public sees are a very small percentage of what the security team deals with. He also described some specific attacks – disclosing that in 2009, the authors of the *Facebook*-targeting Koobface worm made around $1.8 million through their botnet and that, through their research, the *Facebook* security team has managed to uncover their identities (and pass that information on to the authorities).

Following the keynote address the conference programme split into its traditional two-stream format, with papers in both streams relating to bringing the perpetrators of cybercrime to justice. In the corporate stream Raymond Pompon – former undercover FBI agent – looked at some successes and failures in tracking down malware authors, highlighting some of the key problems and the methods that are used to investigate and prosecute them. Meanwhile, in the technical stream, *Panda Security*'s Pedro Bustamante spoke about the takedown of the Mariposa botnet and the arrest of its operators. *Panda Security* was part of the Mariposa Working Group, which was instrumental in the takedown of the botnet and the subsequent arrests. Pedro explained how the botnet was being operated, how its operators were so successful in turning it into one of the biggest botnets ever – at one point controlling close to 13 million computers and netting more than 20,000 euros per month – and how the investigation was carried out. However, he also highlighted the fact that insufficient cybercrime laws in the countries from which the botnet was operated may make it difficult to achieve successful prosecutions.

Kaspersky's Dmitry Bestuzhev posed the question 'How much do you cost?', referring to the black market price of digital data. Following a quick series of questions to the audience he calculated that, once infected, the details of

The VB conference wasn't the only one celebrating an anniversary – both Microsoft and G DATA also celebrated landmark birthdays.

the average *VB* conference attendee – email address, IM account, *Facebook* account, *PayPal* account, bank account and so on – would be worth $7,810.

Paul Baccas spoke about the heuristic detection of malicious PDFs, revealing that *SophosLabs* has seen an exponential rise in malicious use of PDFs, with nearly all drive-by web attacks containing a PDF component and a lot of infected PDFs also being emailed. Paul conducted a poll of the audience, asking whether PDF should be replaced with a safer format. An overwhelming majority of the audience agreed that it was time to retire the PDF. Paul also urged *Adobe* to remove JavaScript support from the format based on the results of his research.

Later in the technical stream, Donald DeBolt discussed the technical details behind black hat SEO attacks, explaining their logic flow, the abuse of *Google Trends* keywords, and identifying the technologies exploited. Dan Hubbard then drew the day to a close with a demonstration of how easy it is for criminals to contaminate real-time search results.

CHILD'S PLAY

The drinks reception at the end of the first day provided ample opportunity for delegates to relax and unwind – while several also took up the opportunity to regress into childhood. This year's drinks reception was dubbed the 'VB games night' as delegates were invited to roll back the years and rediscover their inner child with games ranging from the intellectual to the plain silly. Delegates were seen getting competitive over *Hungry Hippos*, *Operation*, *Buckaroo* and *Connect 4*, among others, while the intellectuals could be seen deep in concentration over a chess board or mastering *Othello*.

All the games used at the drinks reception were donated after the conference to a community project operating childcare programmes in the inner-city area of Vancouver.

Serious stuff – delegates show their competitive streak at the VB drinks reception and games night.

IN THE MIDDLE

On Thursday morning in the corporate stream, Gunter Ollmann discussed the limitations of current methods for measuring botnets and their associated malware components – highlighting the fact that botnet numbers are often overinflated.

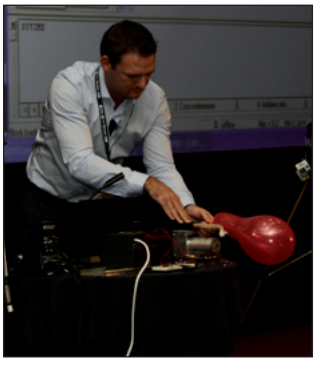
Next, Stefan Tanase investigated the role of social networks in automated targeted attacks, describing how criminals are using such attacks to get their foot in the door and go deep inside corporate networks by targeting a small number of specific employees using information gleaned from social networks.

After lunch, Carey Nachenberg and Vijay Seshadri analysed the real-world effectiveness of reputation-based security in detecting new malware. Having outlined the definition of reputation-based security and highlighted the differences between such an approach and cloud-based fingerprinting, they described *Symantec*'s reputation-based system and took delegates through an evaluation of the system, concluding that the reputation-based security approach provides a substantial independent layer of protection.

STUXNET, STUXNET, STUXNET

Most of the technical stream on Thursday was devoted to the last-minute papers – papers that had been submitted and selected just a couple of weeks before the start of the conference in order to allow up-to-the-minute content to be presented. This year's crop of last-minute papers were very strong, including presentations on smartphone dialers, ATM malware defences, exploit packs and the first 64-bit rootkit – but undeniably, the buzzword of the conference was Stuxnet.

Two last-minute presentations were devoted to the piece of malware everyone was talking about. First up, Liam O'Murchu disclosed some of the details he and the *Symantec* team have uncovered about the highly complex malcode that targets SCADA systems. To add drama to the proceedings he demonstrated, with the aid of an air pump and a confetti-filled balloon, how a Stuxnet-like piece of proof-of-concept code can override a programmable logic controller (PLC) to take control of a piece of



Liam O'Murchu demonstrates the world's most expensive balloon pump.

machinery. Liam hooked the PLC up to the air pump and programmed it to inflate the balloon for just five seconds. He then infected the PLC with his proof-of-concept code and set it to run again – but this time, rather than stopping after five seconds, the air pump continued inflating the balloon until eventually it burst, showering the front row of the audience with confetti and generating an excited round of applause. He suggested that, had the PLC been connected to, say, an oil pipeline, one could imagine how the results could have been significantly more destructive.

Next, a combined presentation from *Microsoft*'s Peter Ferrie and Holly Stewart and *Kaspersky Lab*'s Costin Raiu provided a discovery timeline for the malware – revealing that there is evidence that Stuxnet code dates back as far as January 2009 – as well as full details of the four zero-day vulnerabilities it uses.

In a break from tradition, a 50-minute panel-style question-and-answer session took place with the presenters of both talks after the two presentations. Even with the extension of the Q&A session, there wasn't enough time for all the questions the audience wanted to ask. The Stuxnet presenters also attracted much media attention, with interviews taking place in the press room almost every minute of the day, and film crews from both the CBC and the BBC attending to get the latest updates on the subject.

SONG, DANCE AND BIRTHDAY AWARDS

No *VB* conference would be complete without the traditional gala dinner evening and, in celebration of the 20th anniversary of the conference, this year's gala evening saw a special addition in the form of the VB2010 awards ceremony.

Chor Leoni and the Lorita Leung dancers add a little Canadian culture and colour to the evening.

And the winners are... (clockwise from top left): Peter Ferrie, the Spamhaus team, Andrew Lee presenting the best educator award to Mikko Hyppönen, and Righard Zwienenberg.

Diners entered the ballroom to the melodic tones of Chor Leoni men's choir who performed a selection of traditional Canadian folk songs dressed in their all-Canadian hockey shirts. Later we were treated to a visual feast in the form of a performance by the Lorita Leung dance company – North America's leading Chinese dance troupe.

After the singing, dancing and dining it was on to the awards ceremony. Ten years ago, at VB2000 in Orlando, an award was given to the individual considered to have contributed the most to the AV industry in the first ten years of the *VB* conference. To celebrate the 20th anniversary of the conference, the organizers decided to revive that award, along with five new awards that recognize the tremendous work and achievements of individuals in the industry.

The nominations were all made by visitors to the *VB* website and conference delegates voted during the first two days of the conference to decide the winners in each category. The winners were as follows:

Greatest contribution to the anti-malware industry in the last ten years – *Peter Ferrie*

Greatest contribution to the anti-spam industry in the last ten years – *The Spamhaus Project*

Best newcomer to the anti-malware industry in the last ten years – *Pierre-Marc Bureau*

Best educator in the anti-malware industry – *Mikko Hyppönen*

Most innovative idea in the anti-malware/spam arena in the last ten years – *Righard Zwienenberg*

Lifetime achievement award for services to the anti-malware industry – *Eugene Kaspersky*

Without exception the winners were very popular choices with the audience. Although there wasn't enough time for speeches from all the award winners, Righard Zwienenberg (winner of the award for most innovative idea, for *Norman*'s *Sandbox*) made a special request to say a few words in acknowledgement of Kurt Natvig's enormous contribution to the development of the *Sandbox*. Our best wishes go to Kurt, who wasn't able to attend the conference.

My thanks go to Eddy Willems, Paul Baccas, Randy Abrams, Andrew Lee, Richard Ford and Paul Ducklin for their help in introducing and presenting the awards. Each of them did such a professional job that you'd think they were regulars at red carpet events.

THE END IN SIGHT

Terry Zink kicked off the final morning of the conference in the corporate stream with a look at the psychology of spamming, looking at the role our emotions play when evaluating the content of a spam message and how this works to the advantage of the spammer. David Koconis of *ICSA Labs* then presented an overview of the certification body's anti-spam test methodology, highlighting some of the differences between its methodology and that of other anti-spam tests.

The technical stream saw Thomas Dullien challenging conventional wisdom on byte signatures – arguing that byte signatures are not inherently bad – and Catalin Cosoi discussing the benefits and the downsides of scanning URLs in the cloud.

Later in the afternoon, Pierre-Marc Bureau and Joan Calvet described a Canadian government-funded collaboration between academic researchers and *ESET* to conduct a large-scale malware experiment. The researchers used a computer cluster to boot virtual machines, infect them with malware and let them connect together as a botnet, which they were then able to study and experiment with.

To round off proceedings on Friday afternoon a panel of experts – Lysa Myers, Andrew Lee, Catalin Cosoi, David Perry and Nick Bilogorskiy – were led by Mikko Hyppönen in a discussion of social networking and computer security.

Setting the scene for the discussion, Mikko set up a *Twitter* wall using the hashtag #vb2010 so that, as the discussion progressed, tweeted comments and questions from the audience (both present and remote) would appear live on screen. (Thankfully this was a few days before Mikko was banned from *Twitter*!) Several serious topics were addressed, including the issue of compromised and fake accounts – with perfect illustration of how easy it is to impersonate others online provided by onscreen tweets from 'VesselinBontche' and a Barack Obama impersonator. While the first tweet from the Vesselin impersonator – 'firstly, social networks are for idiots' – had the audience wondering if we had been joined remotely by the great man himself, subsequent tweets had a distinctly more fishy ring to them. At the end of the session Mikko concluded that 1. you can't trust anything on the Internet, and 2. social networks can be awfully distracting – he also warned that since social networks seem to be very much here to stay, the security industry must be prepared for more attacks.

At the cutting edge: the VB2010 speakers.

THANK YOUS

There is never enough space in these reports to mention more than a small selection of the speakers and presentations at the conference, and I would like to extend my warmest thanks to all of the VB2010 speakers for their contributions, as well as to the sponsors of the event: *Avast Software*, *ESET*, *K7 Computing*, *CA*, *Kingsoft*, *Microsoft*, *MX Tools*, *ArcaBit*, *OPSWAT*, *Sunbelt Software*, *TrustPort*, *Beijing Rising* and *AVIEN*.

Next year the conference lands in sunny Spain with the event taking place 5–7 October 2011 at the Hesperia Tower hotel in Barcelona. I very much look forward to welcoming you all there.

Photographs courtesy of: Andreas Marx, Eddy Willems, Pavel Baudis, Tiffini Schwarzkopf and Tjark Auerbach. More photographs can be viewed at http://www.virusbtn.com/conference/vb2010/photos/ and slides from the presentations are available at http://www.virusbtn.com/conference/vb2010/slides/.