CONFERENCE REPORT

THE OTTAWA RULES

Helen Martin

This year the *VB* conference returned to Canada and paid a visit to Ottawa, Canada's fourth largest city and seat of the country's federal government. The venue for this year's conference, the Westin hotel, couldn't have been in a more convenient position for exploring the city – with the Rideau canal within spitting distance, Parliament Hill and Byward Market a couple of steps away, and museums of war, nature, contemporary photography and the Royal Canadian Mint within less than a mile. But city explorations were put on hold – for three days at least – as the doors opened on the 18th Virus Bulletin conference.

IT'S ALL GEEK

The conference kicked off on Wednesday morning with *Sunbelt* CEO and blogger extraordinaire Alex Eckelberry taking to the stage after the official conference opening for his keynote address: 'The AV industry – quo vadis?'. Alex compared statistics from two surveys – one of consumers and another of enterprise customers – that explored customers' feelings towards their AV products and vendors. Overall, consumers appeared to be more satisfied with their products and to place greater trust in their vendors than enterprise users. Alex also stressed the importance of customer support in gaining consumer confidence and presented the results of a review of vendor technical support services – showing many to be lacking in various areas. A perfect start to the conference, the address was entertaining, engaging and struck a chord with pretty much everyone in the room.

After the keynote address the conference split into its usual two-stream format, with David Emm presenting an overview of the malware business, or 'the flip side of the legitimate economy', in the corporate stream, while in the technical stream Morton Swimmer posed the questions: 'How can we build an effective defence structure?', 'How can we get our products to work *together*?' and 'What models can we use for product interaction?'.

After lunch, Gunter Ollmann and Holly Stewart covered the merging of the underground markets dealing in malware and vulnerability exploits, and discussed how the competitiveness between the different market areas actually makes it easier for security vendors to detect the threats.

Kimmo Kasslin's presentation proved to be the most popular session of the conference, taking a detailed look at Mebroot, one of the most sophisticated pieces

Jeannette Jarvis shows the Ottawa Gee-Gees how it's done.

of malware seen in recent times, and characterizing it as 'commercial-grade framework'.

In his paper Matt McCormack coupled analysis of the major malware families targeted by the *Microsoft Malicious Software Removal Tool* with the telemetry it gathers, to provide a perspective on how malware authors respond to the impact on their networks after each release of the disinfection tool. Matt's observations indicate that being targeted by the tool causes significant changes in malware behaviour, including increased use of evasion and stealth techniques.

Jeff Aboud viewed the malware problem from a different angle – that of anti-malware marketing. The mass outbreaks of the 1990s created what seemed like ideal marketing conditions – a situation in which the media and prospective customers all wanted to hear what the anti-malware companies had to say. With the lack of big outbreaks in recent years Jeff argued that many vendors have found a gap in their marketing strategy. He discussed a 'threat marketing' strategy, describing how it can be implemented to help vendors keep their name in front of prospects and key stakeholders.

Following the last of the day's scheduled presentations, *ESET*'s David Harley took to the stage for the company's sponsor presentation, 'Interpreting threat data from the cloud', after which it was time to head for the bar.

Wednesday evening saw the first of the main networking events of the conference – the VB2008 welcome drinks reception. Delegates were welcomed at the door by two burly hockey players from the University of Ottawa team the Gee-Gees, providing some excellent photo opportunities and the chance for delegates to practise their bully-offs.

It was also at the drinks reception that a certain piece of distinguished head gear began its magical mystery tour – spot the real owner!

LOGIC BOMB

Day two started bright and early at 9am with Ismael Briones describing an automated classification system that uses graph theory to identify malicious files with similar internal structures. Meanwhile, Gunter Ollmann took to the stage for the second day running, this time stepping in for a colleague who was unavoidably detained and presenting an interesting paper on the security of virtualized networks.

After mid-morning coffee the schedule in the technical stream turned to anti-spam, more on which later. Meanwhile, David Perry held court in the corporate stream with a paper charting the life and death of the pattern file, followed by Oliver Auerbach, who described how *Avira* handles the never-ending flood of malicious file submissions using a tool which handles deduplication and assigns tasks to analysts according to priority and relevance.

Thursday afternoon saw the return of the last-minute technical presentations following their success at last year's conference. The proposals for these shorter-format (20-minute) presentations were submitted and selected just three weeks prior to the conference, allowing for subjects that were more up-to-the-minute than the full length papers. The fast-paced 'turbo' talks were started off by *VB*'s head of testing John Hawes, who outlined details of a new anti-malware testing methodology that *VB* is planning to introduce to supplement the information provided in the VB100 comparative reviews. Boris Lau followed, with a look at how malware authors effectively emulate the 'race to zero' contests held by other security events as they attempt to beat online scanners as a matter of course.

Spot the rightful owner!

John Hawes talks RAP testing.

Next up, Pedro Bueno provided an insight into the world of South American cybercriminals and their banking trojans, followed by Marius van Oers with a look at what can be done on the *Apple iPhone* with an SDK, and what possible new malware attack vectors could arise from it.

After a quick break for tea, Dan Hubbard presented a different take on the technology *du jour*, cloud computing, discussing how it can be used to decentralize attacks and how it opens up new opportunities and threats to security researchers. Kurt Baumgartner then presented an overview of recent rogueware, which was followed by Sorin Mustaca's presentation in which he introduced an aggregator for phishing and other malicious URLs. The final last-minute presentation was given by Nicolas Brulez, who gave a live demonstration of a malicious packer, showing how it is possible to manipulate unpacking routines.


Panel members share their views on testing.

To round off day two's presentation schedule delegates gathered in the technical stream for a panel discussion entitled 'The current state of anti-malware testing'. Led by Stuart Taylor, panel members representing an end-user, the media, testing bodies and a vendor (John Alexander of *Lockheed Martin*, Paul Roberts of the *451 Group*, Andreas Marx of *AV-Test* and *VB*'s John Hawes, and Righard Zwienenberg of *Norman*, respectively) answered questions from the floor ranging from whether the panel felt that testing is stifling innovation in detection technologies, to how panel members foresee the testing of products that use in-the-cloud technologies. As is often the case with panel discussions, the 40 minutes flew past leaving much unsaid – an indication of how much interest currently surrounds the topic of anti-malware testing.

SPAMALOT

Five years since the introduction of the *VB Spam Supplement* and four years since spam-related papers were first presented at the *VB* conference, spam continues to clutter up our inboxes and shows no sign of abating. This year's conference included five papers on the subject. On the technical side, Patrik Ostrihon and Reza Rajabiun looked at the robustness of new email authentication standards, and Andrey Bakhmutov described a method for tracking botnets sending out spam, while in the corporate stream Vipul Sharma presented a case study of non-English spam, Darya Gudkova described a view of Russian spammers and Chris Lewis reported on *Nortel*'s open-source spam filter for enterprises. A sixth spam paper was scheduled, but following the non-appearance of both the scheduled speaker and the reserve speaker, it was Martin Overton who gallantly stepped up to the mark with his paper on malware forensics. Our heartfelt thanks go to Martin for saving the day.

DATA DIDDLER

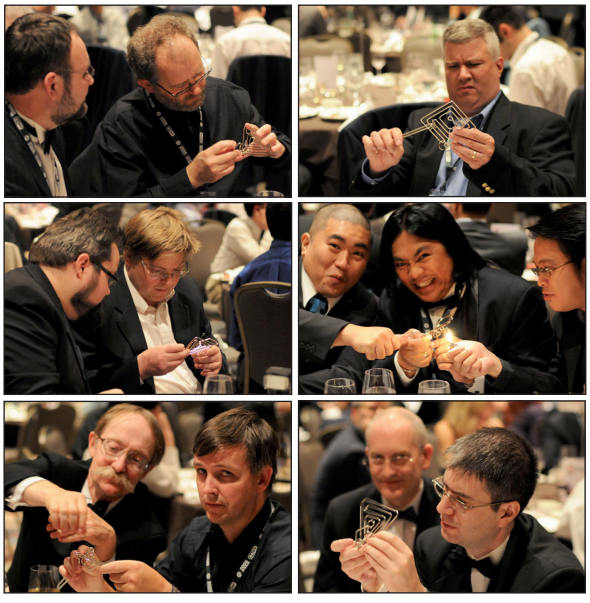

Hosts of the VB100 quiz, Graham Cluley and yours truly.

Thursday evening was, of course, gala dinner night – or was it quiz night? This year's gala entertainment was somewhat more interactive than normal – there was to be no sitting back and waiting to be entertained this year! Compèred by myself and Graham Cluley, the idea of the evening was for dinner tables to compete against each other in a battle of wit and trivia with a selection of exciting prizes on offer for the winning team.


Alex Shipp demonstrates he still pays heed to the Scouts' motto 'be prepared'.

Karen Richardson proved she was truly game for a laugh as she took to the stage in character as the joker, geeing up the audience with 'ooh's and 'aah's and being as flabbergasted as the rest of us when, on being sent on an errand with Alex Shipp, her running partner stripped down to running shorts and trainers in the middle of the dining room.

After five tough rounds of questions based loosely on the subject of malware, ranging from geek trivia to mind-bending brain teasers, just when the audience thought it was safe to sit back and relax, it was time for the final challenge. Two Chinese-style wire puzzles were given to each team, the challenge being to complete both puzzles before the final scores had been totted up. The photographs on the next page give some indication of the level of frustration caused by the 'mosquito' and 'gridlock', and congratulations go to Nick FitzGerald for being the first to complete both puzzles. Nick (and others who eventually completed the puzzles) will be pleased to know that,



'Brain power alone is the key to success.'

according the puzzles' manufacturer, 'brain power alone is the key to success'.

The eventual winners of the quiz were team 'Chop Chop', closely followed by runners-up 'The WTFs' and 'K9s'. A mention should also go to the losing team, 'Rødgrød med Flød' – who were 'rewarded' for their efforts with a very special booby prize.

Team 'Rødgrød med Flød' seemed happy with the booby prize.

Special thanks go to Graham Cluley, whose wit sparkled as brilliantly as his fuchsia pink accessories and whose skills as a quiz show host will hold him in good stead for the day the Eurovision Song Contest returns to the UK, as well as to the members of the *Cue Media* team who put such an enormous amount of work into the production of the show's graphics and its staging.

DISASSEMBLY

For those whose brains had recovered sufficiently from the previous night's mental workout, the final day of the conference began at 9.40am. In the corporate stream Randy Abrams described how a household appliance can be used as a means to teach users about bots and botnets, while in the technical stream Andrew Walenstein and Arun Lakhotia demonstrated the use of game theory to assess the strength of an AV system against evolving offences.

Two papers on anti-malware testing followed the mid-morning coffee break, with Andrew Lee questioning whether it is possible to make testers and certifying authorities more accountable for the quality of their testing methods and the accuracy of the conclusions they draw, and Igor Muttik looking at rebuilding anti-malware testing for the future.

Other highlights on Friday included Ryan Hicks' overview of rules-based analysis using *IDA Pro* and CLIPS, Richard Ford's outline of a new automated sample submission/multi-scanner service, and Peter Ször's paper exploring the possibility of malware evolving to follow Darwinian principles – while still very theoretical, the paper provided plenty of food for thought.

Rounding off the conference was a discussion forum on security in banking – this despite the fact that during the week leading up to the conference it seemed doubtful as to whether there would be any banks left to worry about security. Session chair Jan Hruska directed questions to independent researcher Nick FitzGerald, Reza Rajabiun of York University and *COMDOM Software*, and Eric Davis from *Google*. The discussion opened with a question to the audience: 'Will there be a change in phishing volumes due to the current global banking crisis?' Opinion was somewhat divided, although we now know that the rate of phishing has indeed increased over recent weeks. The discussion moved on to cover liability for phishing losses and user education. The panel session ended while there was still a sea of raised hands in the audience – but was concluded, suitably enough, with the comment 'Users are stupid and will remain stupid', from whom else but Vesselin Bontchev.

AND FINALLY...

My thanks to the VB team, Karen Richardson, the Cue Media team and students from Carleton University.

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 VB2008 speakers for their contributions, as well as to sponsors *ESET*, *ParetoLogic*, *COMDOM Software*, *OPSWAT*, *TrustPort*, *Sunbelt Software* and *K7 Computing* for their support.

Next year the VB conference lands on the shores of Lake Geneva, with the conference taking place 23–25 September 2009 at the Crowne Plaza, Geneva, Switzerland. I very much look forward to welcoming you all there.

Photographs courtesy of: Andreas Marx, Petr Odehnal, Jeannette Jarvis, Kenneth Bechtel, Joe Wells, Tjark Auerbach and Marius van Oers. For more photographs see http://www.virusbtn.com/conference/vb2008/photos.