CONFERENCE REPORT

VIVA BARCELONA!

Helen Martin

The colourful and flamboyant city of Barcelona has been world famous for its art, architecture and style since the late 19th century, and last month the Catalan capital played host to more than 360 anti-malware experts as the 21st Virus Bulletin International Conference landed in sunny Spain.

And very sunny it was too – by happy coincidence the conference was held during a week in which most of northern Europe experienced a period of unseasonably warm weather, and we were treated to soaring temperatures, glorious sunshine and balmy evenings.

Standing at 107m tall, the Hesperia Tower – the VB2011 conference venue – is one of Barcelona's tallest buildings. Designed by renowned architect Richard Rogers (whose other creations include the Pompidou Centre in Paris and the Millennium Dome in London), the Hesperia Tower is also one of the city's most stylish modern buildings. And its stylishness does not stop at the external architecture. In the hotel lobby funky low sofas, swivel chairs and brightly coloured chunky rugs contrast with the highly polished black marble floor to create an area that feels arty and elegant while also relaxed and inviting.

However, some aspects of the highly styled venue simply served to perplex: the über sleek bathrooms were adorned with so many mirrors that finding the exit became like navigating one's way around a labyrinth, while the hi-tech elevators caused excitement and consternation in equal measure – even some of the brightest minds of the anti-malware industry were stumped when faced with calling the elevator using a set of touch-screen controls.

A purpose-built auditorium served as the main conference room and home to the technical stream. While the tiered seating provided the audience with uninterrupted views of presenters and projector screens, the layout presented a challenge for the microphone runners who had to negotiate a long flight of steps to get from the back of the room to the front. Thankfully there were no casualties, but the thought of rolling down the stairs head over heels and landing in a heap at the foot of the stage haunted *VB* team members all week. Meanwhile, one floor above, a more traditional style ballroom was home to the corporate stream, offering acres of space and far less of an obstacle course for weary crew members.

EL INICIO

The conference kicked off in the auditorium on Wednesday morning with an engaging keynote address from *F-Secure*'s Mikko Hyppönen and Bob Burls from the UK's Police Central e-Crime Unit. Mikko and Bob described details of a multi-jurisdictional investigation against the m00p malware-writing group. The pair revealed the enormous amount of work that went into the several-year-long investigation as well as some of the clues that ultimately led to the arrest and conviction of two of the members of the group (including one member who embedded his social security number in his malcode, as well as having had his unique online nickname tattooed on his arm). The fascinating presentation gave delegates an insight into how much work goes into such investigations as well as some of the obstacles faced by investigators of cybercrime.

Sticking with the theme of online crime, Dmitry Bestuzhev took a look at the cybercrime ecosystem and the way it works – highlighting cybercriminals' moves, their organization and what sort of people they are. He also revealed the limitations of the legal systems used against cybercriminals in several countries – the lack of any real threat of punishment being one of the reasons why this type of crime has become rife in certain countries. He revealed, for example, that despite a new bill having been pending in congress since 2005, the current law used against cybercriminals in Brazil is 70 years old.

Dmitry's colleague Fabio Assolini followed with a presentation focusing on why Brazil has achieved worldwide notoriety as a place where cybercrime, and in particular online banking crimes, flourish. He described examples of Brazilian cybercriminals living the life of Riley – buying top-of-the-range cars and staying in luxury hotels. Interestingly, he revealed that rather than looking further afield, many banking trojans specifically target Brazilian IP addresses – with $900 million having been stolen from Brazilian banks in 2010.

Meanwhile, in the technical stream Rachit Mathur took a look at the future of stealth malware, and Pierre-Marc

VB2011 saw a special guest appearance from Kermit the frog – or was it his beer-loving Spanish cousin Gustavo?

Bureau presented an interesting look at botnets, suggesting that the same group is behind some of the most prolific bots seen over the past four years.

After a break for lunch the corporate stream saw presentations detailing malicious attacks on *Facebook* (in which an audience member stole the show by answering the question 'What's your advice for people wanting to avoid security problems on *Facebook*?' with the simple advice 'Don't log in!'), anti-malware product testing and its associated frustrations, and how much information users give away on social networks.

Meanwhile, in the technical stream Jeff Edwards explored Chinese DDoS bots, revealing that a large amount of code is re-used amongst them. Jeff described a 'typical' Chinese DDoS bot and touched on some of the targets of these attacks which have included Chinese manufacturers of ice cream and custard-making equipment as well as prominent international financial and investment companies.

After a break for tea, Onur Komili took to the podium in the technical stream to analyse the behaviour of the malware distribution networks that poison search results specifically to deliver users to web pages that install fake anti-virus software. Onur explained some of the methodologies used by those behind rogue security software and described how *Sophos* has built tools to help look for patterns that identify different distribution networks.

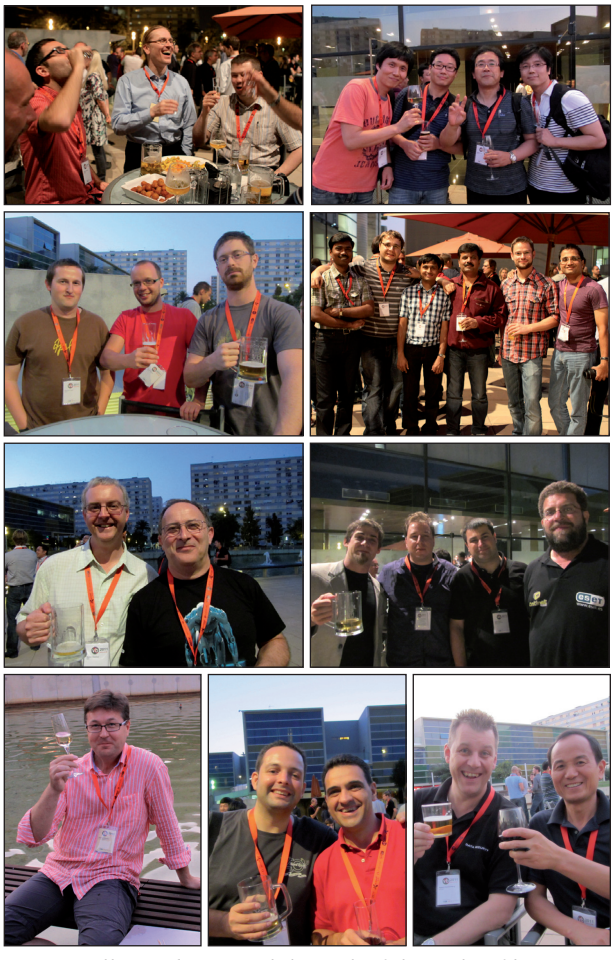
Next, Igor Muttik looked at the use of data mining in the processing of malware samples. He began by demonstrating the power of data mining in distinguishing between males and females – based on buttock circumference. Having successfully grabbed the audience's attention (thankfully not their buttocks), he went on to explain that some 250 parameters exist within the PE header of executable files, from which information can be gathered and differences can be discerned between malicious and non-malicious files. Although the data-mining method is not robust enough to be used as a sole method of detection, Igor suggested that the hit rate is good enough to be used to help prioritize malware in the sample submission queue.

MUCHA CERVEZA

As usual, the opening day of the conference ended with a drinks reception. Thanks to the glorious weather, delegates were able to spill out onto the hotel's outdoor terrace and, with the melodious tones of a Spanish guitar duo drifting out through the doors, it was easy to imagine that we were enjoying a warm summer's evening rather than hurtling towards the end of the year in the first week of October.

A note must be made at this point about the accessory of choice at this year's event: the *Avast!* beer mug. These were distributed from the *Avast!* exhibition booth and could be filled (and re-filled) with beer free of charge. Delegates were spotted wandering around the conference with their mugs clutched to their chests – reluctant to let them out of their sight lest they lose their precious 'bottomless' receptacles. (Regrettably, it appears that the mugs' beer-filling/refilling qualities do not extend beyond the *VB* conference – the *VB* team has checked.)

Avast! also sponsored the beer served at the event's drink receptions and gala dinner – and judging by the popularity of this act of generosity (marketing), one cannot but hope that the beer bill didn't bankrupt the company's marketing director at the end of the three days!



Beer all round. Meanwhile (sick of the sight of beer?), Avast!'s marketing director Milos Korenko raises a glass of wine.

DIAS EL NÚMERO DOS

With so much free-flowing beer, Wednesday's festivities went on perhaps a little later than usual and delegates were noticeably thin on the ground at breakfast the next morning. Thankfully, the promise of an excellent set of presentations was enough to lure sleepy heads away from their pillows, and after a couple of servings of coffee audience numbers returned to full strength.

Axelle Apvrille kicked off in the technical stream with a popular talk on how to replicate mobile malware in a secure environment with a fake GSM network built using OpenBTS.

Andrea Lelli presented the first of the last-minute presentations in the technical stream with an overview of reversing the Xpaj virus – revealing that the authors of the click fraud polymorphic infector earned $46,000 in a year.

Other last-minute presenters included Eugene Rodionov, who presented an overview of the evolution of rootkit installation; Stefan Tanase, who shared his experience of attempting to clean up 100 infected websites in the least amount of time possible (see p.2); and Vicente Diaz who detailed a recently discovered *Twitter* fraud campaign.

Meanwhile, in the corporate stream, Rainer Link and David Sancho shared their experience of sinkholing botnets – a method that aims to redirect the traffic intended for the malicious server to an analysis server – and revealed some of the problems they have encountered using the technique.

Also in the corporate stream, Martin Lee talked about mapping targeted attacks, Brett Cove described the oft-ignored snowshoe spam and Methusela Ferrer delivered the message that *Mac OS X* and *iOS* users are very much the target of cyber attacks right now, and that running a *Mac* anti-malware solution is essential.

Thursday morning also saw *VB*'s first 'stealth presenter'. Denis Maslennikov and Tim Armstrong had been scheduled to present a paper together on *Android* malware, but due to an unfortunate clerical error, Tim was unable to attend the conference at the last minute. The organizers hastily arranged for 'virtual Tim' to grace the stage, and thanks to the wonders of *Skype* the pair were able to co-present from separate continents.

The day ended with a presentation by platinum sponsor *comScore* on its digital market research services, while in the auditorium a panel of experts discussed the sharing of information and collaboration (or lack thereof) within the anti-malware industry.

LA FIESTA

Of course, no *VB* conference would be complete without the glitz and glamour of the traditional gala dinner evening – and this year we were treated to some truly spectacular entertainment to liven up the breaks between courses.

The deafening sounds of Batek.

As soon as everyone was seated, Brazilian percussion group Batek burst into the room beating out their infectious rhythms. The group raised the roof with their high-energy routines (and probably deafened a few diners in the process).

The Evna Barcelona dancers bring the dinner to a close with a true Spanish flavour.

Later in the evening we reverted to Spanish rhythms with a stunning performance by the Evna Barcelona flamenco dancers and musicians. The dancers' speed, agility and artistry was awe inspiring and their expressive performance made for a suitably colourful and upbeat finish to the official part of the evening. (Of course, thanks to *Avast!*, the beer continued to flow long after the end of the dinner.)

EL FINAL

Early risers on Friday morning were treated to Gunter Ollmann discussing various reputation systems and their strengths and weaknesses, followed by Denis Maslennikov who took to the stage again (this time without his 'virtual' colleague) to explore the problem of cell phone money laundering in Russia. Meanwhile, the technical stream saw Aditya Sood detailing browser exploit packs and Zheng Zhang analysing fake anti-virus packers.

After a quick caffeine boost it was show time in the corporate stream. Maybe one year Terry Zink and David Perry will combine their talents and put on a double act, but for now the two magicians in the pack remain solo artists. Terry began his presentation on practical cybersecurity with a trick involving session chairman Per Hellqvist. Per was asked to splay his hand on a table then choose one of two identical bags, the contents of which would be emptied onto his splayed hand. Per made his choice and a small piece of paper fluttered out onto his hand – Terry then upturned the second bag and, to the audience's delight, a large rock came crashing to the (now empty) table. Terry then proceeded to describe

The VB2011 speakers.

how the human brain works when it learns and retains new information, and how successful teaching techniques can be applied to help teach people about cybersecurity. Not to be out-magicked, David Perry managed to slot two tricks into his presentation, including producing a six-foot drinking straw seemingly from thin air and a mind-boggling box trick.

After lunch, Holly Stewart gave an overview of the top exploits of 2011, revealing that the top OS vulnerability seen by *Microsoft* this year has been CplLnk, the Windows Shell shortcut vulnerability used by Stuxnet as a form of propagation. She also revealed that as far as documents are concerned, exploits hidden in *Adobe* PDFs represented 96% of all document-related exploits affecting systems at the start of 2011, while exploits in *Office* documents represented just 4% of exploits.

Maksym Schipka concluded proceedings in the corporate stream with a look to the future. He predicted that the security industry will move away from protecting endpoint devices to concentrate on protecting the backend and its associated (cloud) services, as traditional endpoints are replaced by thin clients that purely access remote applications and data.

Drawing the conference to a close in a combined final session a panel of experts shared their opinions on and experiences with tackling botnets. They asked who is responsible for fixing the botnet problem – the owner of the computer which became a bot, the owners of the infection vectors (e.g. websites, producers of vulnerable applications which get exploited), or the ISPs which can control their end points' access to the Internet? The topic is a complex one involving lots of legal and technical issues and, as with many of these discussion sessions, more questions were raised than answered.

LOS INDESEABLES

It was often the case in years gone by that a new virus or variant would be released during the *VB* conference – possibly in the hope that the industry's top experts would be otherwise engaged giving or listening to presentations and sharing tips in a hotel bar, thus allowing the malware to stay under the radar for as long as possible.

Although this hasn't been the case for a couple of years, this year's conference did attract some unwanted attention. Within the last couple of years it has become the norm to see delegates sitting in sessions with their laptops or mobile devices, busily tweeting their thoughts and comments on the papers or interesting facts gleaned from the presenters. This year, however, a rogue tweet appeared using the '#vb2011' hashtag and promising 'news from the VB conference'. *BitDefender* researchers determined that the shortened URL in the post actually downloaded a file named VB2011.exe which, once executed, injected a *Windows* process and downloaded an installer, resulting in a slew of adware, gameware and adult content opened in a web browser. The incident was a good illustration of the fact that even links that seem related to a trusted security event may not be all they seem.

MUCHAS GRACIAS

The hard working VB crew.

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 VB2011 speakers for their contributions, as well as to the sponsors of the event: *AVAST Software*, *comScore*, *ESET*, *Ikarus Security Software*, *Qihoo 360*, *Total Defense*, *ArcaBit*, *GFI Software*, *OPSWAT* and *TrustPort*. My thanks also go to all of the on-site crew for working so hard to ensure the event ran smoothly.

Thanks to a number of delegates opting to forego their printed copies of the VB2011 conference proceedings a donation of £260 has been made to the WWF. A similar opt-out scheme will be run again next year.

HASTA LA VISTA!

Next year the conference lands in Dallas, TX, USA with the event taking place 26–28 September 2012 at the Fairmont Dallas. And we will be returning to Europe for VB2013 which will be held 2–4 October 2013 in Berlin, Germany. I very much look forward to welcoming you all to both events.

Photographs courtesy of: John Alexander, Pavel Baudis, Filip Chytry, Jeannette Jarvis, Andreas Marx, Michael Neitzel, Morton Swimmer and Eddy Willems. More photographs can be viewed at http://www.virusbtn.com/conference/vb2011/photos and slides from the presentations are available at http://www.virusbtn.com/conference/vb2011/slides/.