CONFERENCE REPORT

SIX FLAGS OVER TEXAS

Helen Martin

The *VB* team arrived at the Fairmont Dallas in sweltering temperatures – quite a shock for those of us more used to a chilly climate at this time of year. I am told that the sunshine and searing heat persisted for the duration of the conference week, but the next time any of the *VB* team ventured past the threshold of the hotel some much more familiar weather had settled in – heavy rain started to fall almost from the minute the conference ended (notably the first time there has been bad weather at the end of the *VB* conference for at least 11 years!).

After the sleek modernism of last year's hotel in Barcelona, the Fairmont Dallas was a much more classic but no less stylish venue, conveniently located at the heart of the Dallas Arts District with several attractions within walking distance and both the antique M-Line trolley and the ultra modern DART services close by for anyone wanting to venture further afield.

The Fairmont did its best during the week to disguise the fact that temperatures outside were reaching the high-80s to 90s by chilling the conference rooms down to such an extent that many delegates were forced to rummage in their suitcases for extra jumpers and jackets. On requesting slightly less aggressive cooling of the rooms we were informed that the air conditioning had two settings: on and off – so we shivered on, grateful for the hot cups of coffee between sessions.

We were delighted with delegate numbers this year – knowing that Dallas has neither the natural beauty of Vancouver (VB2010) nor the colourful flamboyance of Barcelona (VB2011), we fully expected a downturn in delegate numbers, but the final total came in only slightly lower than the last couple of years and exceeded our expectations by some way.

CONFERENCE OPENER

The conference kicked off on Wednesday morning with a thought-provoking keynote address by Christopher Soghoian of the American Civil Liberties Union who spoke about the trade in security exploits. He described several examples of bugs being sold for seriously big money (e.g. to the US government) rather than being passed on to the companies whose software was at risk. Despite the questionable ethics and cloak-and-dagger business practices of some of the middlemen, the selling of exploits to third parties is not illegal, but it certainly sails close to murky waters. Soghoian left the audience considering whether self-regulation of the exploit trading industry is possible.

After the keynote address the conference split into its traditional two-stream format. Starting proceedings off in the Corporate stream, John Graham-Cumming took a fascinating look into Internet background radiation. Website security firm *CloudFlare* handles around 64 billion page views per month, making it ideally placed to track and observe attacks against everything from gambling sites to blogs and newspapers, governments and large corporations. John revealed that the company sees a layer 4 DDoS attack 40% of the time and a layer 7 DDoS attack 95.5% of the time. His statistics also revealed significant drops in denial-of-service attacks observed at certain points in the year, which may be attributable to events such as Earth Day, Memorial Day weekend, Chinese New Year and other festivities which likely saw many computer users switch their machines off.

A presentation by Righard Zwienenberg followed, looking into the pros and cons of the increasingly popular Bring Your Own Device (BYOD) trend. While the advantages of BYOD include cost savings and ease of use of devices, there are several disadvantages that businesses need to consider, including personal devices being difficult to update and protect. Since the trend is already well established, Righard suggested a new strategy along with a new acronym: C(hoose)YOD – where businesses select which devices they can manage, update and provide effective protection for, and employees choose which of those devices they use.

Vicente Diaz spoke about privacy issues – highlighting the fact that in visiting a single popular newspaper we make an average of 11.3 requests to different tracking sites, and that 93% of the top 100 most popular sites include at least one request to a tracking site. Vicente warned that, with the enormous amount of data being collected and sold to third parties, there is a bigger concentration of knowledge about the global population than there has ever been – and that while big companies currently use the information for advertising, they may figure out other ways to use it in the future.

Later in the afternoon, José Fernandez described how he and colleagues at the École Polytechnique de Montréal

and Carlton University conducted an evaluation of an anti-malware product in the form of a 'clinical trial' – involving real users. The study yielded some interesting findings regarding user behaviour (such as the fact that more browsing equates to a higher risk of infection) and demographics (such as the fact that the 25-to-30-year-old age group was more prone to infection than the younger 18-24 group, or even the population at large), but more pertinently it gave a very realistic picture of product performance. The researchers hope next to perform a larger-scale study – with greater statistical significance – which could be used for comparative AV testing. José ended his presentation asking vendors to volunteer their products for the team's next study.

Also on the theme of testing, *VB*'s own Martijn Grooten set forth his ideas for the setting up of a test that will evaluate products that filter malicious web traffic, while in the technical stream, Hendrik Pilz described how *AV-TEST* set up a test environment and new methodologies for conducting *Android* anti-malware tests – now that there are more than 40 commercially available anti-malware products for the mobile platform.

Other highlights in the technical stream included *ESET*'s Eugene Rodionov and Aleksandr Matrosov who described the techniques used by a number of modern complex threats to counteract forensic analysis and who introduced a free public tool, *HiddenFsReader*, which makes it possible to retrieve the contents of the most commonly encountered hidden file systems. Candid Wüest took a look at where we stand with banking trojans today – indicating that they have not changed a great deal over the past ten years because the same techniques continue to work, but that there has been an increase in the use of stealth and obfuscation techniques, more automation, and more social engineering.

Wei Xu presented details of a malicious PDF filter, developed with his colleagues at *Palo Alto Networks*, which uses a set of predictive features to detect malicious PDFs. A high detection rate and low false positive rate were recorded in evaluation tests.

The first day drew to a close with sponsor presentations in both streams – in the Corporate stream, *ESET*'s Steven Cobb asked 'What do consumers really know about malware?', while in the Technical stream *AVAST*'s Milos Korenko explained the success of the company's 'freemium' business model – then directed delegates to the bar to claim their free (courtesy of *AVAST*) beer...

RIDE 'EM COWBOY!

This year's informal drinks reception on Wednesday night went one step further in encouraging delegates to let their hair down (and take their shoes off) with the presence of two mechanical bulls, a roll-a-roper and a team of quickdraw gunfighters.

Much hilarity was had over delegates (and *VB* crew) clinging onto the mechanical bull for dear life only to eventually be hurled off and land in a crumpled heap, beaten by the red-eyed beast.

VB2012 delegates and crew practise their cowboy skills.

In another corner of the room delegates were invited to sit astride a 'horse' and try out their roping skills by attempting to lasso what was apparently intended to represent a calf (on wheels), but which I heard one would-be cowboy describe as more like a cross between a dog and a sheep.

The noisiest corner of the room meanwhile was taken over by two gunfighters who invited delegates to test the speed of their trigger fingers both against each other and against the 'professionals'. Not an activity for the faint-hearted!

MIDDLE OF THE PACK

Thursday morning kicked off bright and early in the Corporate stream with Amir Fouda taking a look at the various malware families that target the increasingly popular digital *Bitcoin* currency, while in the Technical stream Broderick Aquilino presented a technical analysis of Flashback – the most advanced *OS X* malware seen to date.

Next up in the Technical stream was a specially extended session as David Jacoby took to the stage to discuss the use of *nix servers by cybercriminals for the distribution of malware and in the set-up of their malicious infrastructure. David asked 'Why am I talking about [a problem that's] 10 years old?', answering his own question: 'Because we have done nothing [about it]!'. He followed his discussion with a 30-minute live demonstration in which he invited four members of the audience to help identify vulnerabilities and exploit them using the same techniques as those used by attackers.

Meanwhile, in the Corporate stream, Peter Kruse presented a summary of the investigation that led to the arrest by Russian authorities of the Carberp C&C administrator. The investigation was the first for the European Cyber Security Federation (ECyFed), which includes *Group-IB*, *CyberDefcon* and *CSIS*, and involved placing a GPS transponder in goods (purchased using stolen credit card details) that were being reshipped to the criminal gang. The trail led investigators to a small border town in Poland and from there into Ukraine before ending in downtown Moscow.

Next, Fabio Assolini took to the stage and described how criminals in Brazil managed to compromise 4.5 million DSL routers, going unnoticed for months. More than 50% of the users of some Brazilian ISPs were reported to have been affected by the attack. During their research, the *Kaspersky Lab* team came across an IRC chat between some of the hackers involved – during the exchange it was revealed that one of them earned approximately $50,000 and spent his loot on taking trips to Rio de Janeiro to visit prostitutes. Fabio concluded that there is little that users can do to avoid this kind of attack beyond using strong

passwords and tight security settings, and updating firmware when patches become available. He urged security researchers to be more proactive in reporting flaws related to routers, ADSL modems and other network devices, and urged manufacturers to be more responsive in securing their products.

The rest of the day's sessions in the technical stream were devoted to last-minute papers – which had been submitted and selected just three weeks prior to the conference in order to present the freshest material possible.

Tyler Moore was first up, with an overview of a piece of collaborative academic research on the real cost of cybercrime. The researchers found that, in fact, the amount spent on protecting against cybercrime far outweighs the losses attributable to it. The figures revealed by the study suggest that we ought to be spending less in anticipation of cybercrime (i.e. on anti-virus, firewalls, etc.) and instead be focusing our resources on tracking down and prosecuting cybercriminals.

Loucif Kharouni followed with a discussion of the increasing prevalence of police ransomware in Europe. His presentation certainly provided enough facts to convince the audience of the existence of the problem, but if anyone was left in any doubt, the point was beautifully illustrated by the discovery of said police ransomware on the personal laptop of one of the AV crew. (If you're going to run into trouble with malware on your machine, what better place for it to happen than at an event with more than 300 anti-malware experts on hand to help? A remarkable piece of serendipity!)

After lunch, Robert Lipovsky and Sebastian Bortnik presented the details of an industrial espionage attack in Latin America which focuses on stealing *AutoCAD* drawings – their investigation of ACAD/Medre revealed that more than 10,000 *AutoCAD* drawings had been leaked over the last two years.

Next, Neil Schwartzman and Paul Kincaid-Smith described the collaborative efforts of a working group consisting of victims of the Adober gang (including colleges, universities and ESPs), security researchers, DNSBL operators and law enforcement. The Adober gang used malware and social engineering techniques to compromise ESP subscriber accounts and steal lists of tens of millions of end-user email addresses. They then generated revenues by spamming

millions of addresses – typically selling freeware such as *Adobe Reader* or *Skype*. The Adober Working Group combined their efforts to blacklist new URLs registered by the hackers in an attempt to get ahead of the criminals and put a stop to the damage.

In the Corporate stream, Grayson Milbourne and Armando Orozco took an in-depth look at the evolution of *Android* malware, looking at risks, threat vectors, real-world examples and finishing with some tips on how to keep your *Android* device clean.

Later on, John Alexander posed the interesting question: 'Has the time come for anti-malware vendors to allow customers to write their own anti-malware signatures?'. He detailed how customer needs do not always align with anti-malware vendor needs and suggested that if anti-malware vendors were to adopt a more open model, they could empower customers to protect themselves better.

Randy Abrams gave a fascinating presentation on habit and security education – looking at ways in which we need to move consumer security education forward. He pointed out that there is a difference between bad habits and ignorance, and the two cannot be treated in the same way.

Drawing the second day to a close, *Qihoo 360*'s Royce Lu gave the third and final sponsor presentation, taking an interesting look at malware attacks on online shoppers in China.

DALLAS COWBOYS

The Western theme begun at the Wednesday night drinks reception continued through to the gala dinner on Thursday evening. Once safely seated and when starters had been dispatched, delegates were treated to an impressive

Boots, chaps and cowboy hats...

Place your bets!

demonstration of roping tricks from 'Joe Hub Baker, The Texas Kid' – who, we were reliably informed, also puts his skills to good use on his ranch in his day job.

After the main course we were entertained by 'The Gunfighters' who enacted a short Western-style skit, ending (predictably enough) in the dramatic shooting of one of the characters.

Once the (unfathomably sweet) desert had been finished, the VB2012 casino was opened for business – delegates whiled away the rest of the evening playing black jack, craps, roulette and of course Texas hold'em, with prizes at stake for the three players with the most chips left at the end of the night.

FREQUENT FLIERS

Over its 22-year history, the *VB* conference has developed a group of loyal and dependable supporters.

Aside from the presentations, the *VB* delegates are what makes the conference special – a group of individuals who seem to be able to play as hard as they work and to be as much fun as they can be serious business professionals – and I'm sure I speak on behalf of the whole *VB* team when I say that their support of the conference is part of what makes all the hard work worthwhile.

As a small token of our thanks, this year saw the introduction of long service awards for delegates who have been supporting the conference for 10, 15 and 20 years.

After announcing the awards at the start of the gala dinner, those whose names had appeared in a roll call on screen were invited to come and collect their pin badges. A total

Proud VB conference veterans.

of 40 badges were given out – four of which were given to *VB* veterans of 20 years, 16 to those who have been coming to the conference for 15 years or more, and 20 to those who have been supporting the event for 10 years or more.

It was gratifying to see delegates wearing their badges with pride.

FINAL PUSH

A slightly later start on Friday morning (alongside the energy drinks thoughtfully provided on the *Bitdefender* exhibition stand) gave everyone a chance to recover from Thursday's late night.

First up in the corporate stream were Heather Goudey and Hermineh Tchagatzbanian describing a technique for generating automatic malware descriptions that are comparable to manually produced descriptions. Meanwhile, in the technical stream Andrey Bakhmutov started the day's proceedings with a look at clustering techniques for the detection and mitigation of spam distributions.

One of the most popular presentations of the conference was Ivan Teblin's dissection of the Duqu exploit. The malware arrives on the victim's system as a *Word* email attachment and is activated by a specially crafted OpenType font embedded into the OLE2 file. Ivan noted that his team's investigations and proof-of-concept experiments indicate that OpenType content presents similar levels of danger to other active content, such as scripts or executable code, and he predicted that the format will continue to gain popularity among malware writers.

Later, John Morris described how *Kindsight* researchers cracked the encryption algorithm and decoded the command and control protocol of the ZeroAccess P2P botnet, providing a detailed analysis of how it maintains contact with its peers.

Another popular presentation was Andrew Lee's probing assessment of whether the use of the term 'cyberwar' is justified. He called for a stop to the use of inflammatory language – saying that the AV industry should take every opportunity to reduce hype and increase knowledge among end-users.

The final presentation of the day in the Corporate stream was given by Martin Lee, who showed that it may be possible to identify specific risk factors that are associated with individuals subjected to targeted attack, by considering the threat akin to a public health issue. Such risk factors can be used to identify, inform and protect those at risk of future targeted attacks.

Meanwhile, in the Technical stream, Abhijit Kulkarni and Prakash Jagdale looked at the Early Launch Anti-Malware (ELAM) driver feature of *Windows 8* and discussed the features that could be added in future versions of ELAM in order to make it really beneficial to anti-malware vendors.

Rounding off the conference in a final combined session was a panel discussion on offensive security research. Chaired by *ZDNet*'s Ryan Naraine, a panel consisting of Adrian Stone (*RIM*), Josh Shaul (*Application Security Inc.*) and Alain Zidouemba (*Sourcefire*) entered into a lively discussion of the merits and dangers of exploit disclosure.

UNTIL NEXT TIME...

There is never enough space in these reports to mention more than a small selection of the speakers and presentations and I would like to thank all of the VB2012 speakers, panel members and session chairs for their contribution to the event, as well as all of the VB2012 sponsors for their generous support: *Avast*, *ESET*, *Qihoo 360*, *Microsoft*, *Bitdefender*, *GFI Software*, *Max Secure* and *OPSWAT*. My thanks also go to the members of the *VB* team and all of the onsite crew for their extremely hard work in the running of the event.

Thanks to a number of delegates opting to forego their printed copies of the VB2012 conference proceedings, a donation of £290 has been made to the WWF. A similar opt-out scheme will be run again next year.

Next year we return to Europe, with the conference taking place at the Maritim Hotel, Berlin from 2–4 October 2013. I look forward to welcoming you there.

(Photographs courtesy of: John Alexander, Pavel Baudis, Jeannette Jarvis, Andreas Marx, Morton Swimmer and Eddy Willems. More photographs can be viewed at http://www.virusbtn.com/conference/vb2012/photos/ and slides from the presentations are available at http://www.virusbtn.com/conference/vb2012/slides/.)