CONFERENCE REPORT

VB2013: BERLIN TIME

Helen Martin

With high-tech industries, renowned universities and research facilities nestling alongside historic sites, diverse architecture, a dynamic arts scene and a lively nightlife, the vibrant city of Berlin combines the old and the new in a way that few other places manage, and it caters to all tastes and interests. The same could be said for the 23rd Virus Bulletin International Conference (VB2013) – which really did seem to have something for everyone.

The Maritim Hotel Berlin, which played host to VB2013, stands directly opposite the historic Bendlerblock building complex (which now houses the German Resistance Memorial Centre), a couple of strides away from the Tiergarten (the largest and oldest public park in Berlin), and a short walk from the ultra-modern Sony Center and Daimler complex at Potsdamer Platz. Drawing inspiration from the Golden Twenties, the hotel's marbled floors, luxurious polished wood finishes and dazzling chandeliers create a feeling of opulence and supreme comfort. The generously proportioned Hall Maritim, which was home to the Technical stream for the week, was probably the largest room a single stream of the *VB* conference has ever occupied – even making the close to 400 delegates that amassed for the conference opening seem like a relatively small gathering. The Hall Berlin, home to the Corporate stream, was somewhat cosier, but no less elegant.

This was yet another bumper year for delegate numbers – European destinations always seem to draw the crowds and Berlin was no exception, with a grand total of 390 attendees. The growth of the *VB* conference over the years has been fantastic to observe, although the swelling numbers do cause a bit of a headache in that it is becoming increasingly difficult to find venues that have enough space to accommodate us! (A good headache to have, though.)

MAKING A START

VB2013 began on Wednesday morning with the usual opening address and housekeeping notices, after which the stage was left in the capable hands of Andrew Lee, CEO of *ESET* North America. Kicking off the conference in style, Andrew delivered a passionate and provocative keynote address looking at ethics in the anti-malware business in the age of government cyber surveillance. Opening with a video montage on Snowden, the NSA and user privacy, Andrew highlighted the fact that the recent NSA leaks have created a culture of distrust. While the AV industry has spent many years building trust between vendors and among researchers, those levels of trust have been damaged – with researchers no longer sure who can be trusted and who may be disclosing information to intelligence and law enforcement agencies. Kudos to Andrew for managing to slip in quotes from George Orwell and Samuel L Jackson (as Jules Winnfield), some cat pictures and a handful of penguins, while at the same time delivering a thoroughly engaging and thought-provoking talk on a topic that has much relevance to the whole of the security community.

After the keynote address the conference took on its traditional two-stream format. Starting the presentations off in the Corporate stream, Andreas Lindh described ways in which corporations can reduce the window of exposure to zero-day threats by getting back to basics and using tools that are already available as a complement to the often prolonged or delayed patching process.

Next up, Razvan Benchea and Vlad Bordianu described how an examination of over 800,000 apps on the *Google* and *Apple* markets uncovered a worrying number with security issues. The researchers found that 0.44% of *Google Play* apps were using an unencrypted connection for authentication/registration while the same was true for 0.51% of apps in the *Apple App Store*.

Meanwhile, in the Technical stream, James Wyke detailed some of his discoveries about the ZeroAccess botnet, demonstrating its network traffic obfuscation techniques and revenue generating model – and revealing that ZeroAccess click fraud revenue is estimated at between US$90,000 and US$200,000 per day.

After lunch, Tom Cross and Holly Stewart tackled the thorny issue of vulnerability disclosure from a different angle: when

to disclose that a vulnerability is being exploited in the wild. While the knowledge that a vulnerability is being exploited can be helpful for users in prioritizing their defences, the knowledge that a vulnerability exists and that it can be targeted effectively is also useful for potential attackers – and can result in an overall increase in attack activity. Holly and Tom looked at a number of different real-world examples demonstrating both the positive and negative effects of public disclosure of exploitations and showing how the timing of disclosure can significantly affect the outcome.

Later, Joe Blackbird and Bill Pfeifer looked at the global impact of anti-malware protection state on infection rates – they used *Microsoft* statistics to show that PCs without anti-malware protection (or with inadequate anti-malware protection) are 5.6 times more likely to be infected, and a computer that runs consistently without anti-malware has a 10 times greater risk of being infected month on month than a machine with protection installed. Among other things, the pair called for anti-malware vendors to make sure that disabling options for anti-malware products are well hidden.

Wednesday afternoon saw presentations on two major cross-industry telemetry projects. Righard Zwienenberg and Thomas Wegele presented a system being developed by members of the Anti-Malware Testing Standards Organization (AMTSO) that is intended to overcome the shortcomings of the WildList. The Real Time Threat List (RTTL) should offer a more accurate and up-to-the-minute picture of the latest threats in circulation than anything currently on offer, while also providing a flexible framework for testers to make use of it in different ways. Later, Igor Muttik and Mark Kennedy spoke about another cross-industry initiative, this one developed by members of the IEEE Industry Connections Security Group (ICSG) malware research group and designed to help mitigate the issue of false positives. The IEEE-ICSG clean file metadata sharing system (CMX) provides a database that can be shared by all security vendors. Legitimate software developers can submit metadata for their products to the system, and the metadata will be relayed to all security vendors at once, thus enabling vendors to add the products to their whitelists and helping them to build clean sample sets for quality assurance.

The first day drew to a close with sponsor presentations in each stream. In the Corporate stream, *ESET*'s Stephen Cobb asked 'What can Big Data Security learn from the AV industry?', while in the Technical stream *AV-TEST*'s Andreas Marx detailed some of the testing company's expert knowledge and research.

BEER AND WINE MAKES YOU FEEL FINE

Wednesday evening saw the usual gathering of attendees for the VB2013 drinks reception – the wine, beer and canapés

Cheers! VB2013 delegates let their hair down and enjoy some valuable networking.

flowed steadily, giving delegates the chance to unwind and discuss the important issues of the day (such as who would triumph in this year's *G Data* table football tournament, whose beer consumption would top the *Avast* league table, and how on earth did the catering staff manage to superheat the inside of the mini spring rolls to a near thermonuclear degree?).

Indeed, the beer flowed freely throughout the three days of the conference at the temporary bar set up by *Avast* – and an online league table provided live updates as to the most prolific beer drinkers both individually and by company. Wednesday night also saw the lure of all sorts of weird and wonderful alcoholic beverages at *G Data*'s 'Snake Oil' party held after the *VB* drinks reception (one delegate suggesting he may actually have sampled window cleaner disguised as an alcoholic beverage). For those who had been unable to resist doing the drinks party double, Thursday morning brought a scrabbling for aspirin and coffee – and some concerns as to how their livers would stand up to the next assault on the *Avast* beer leader board.

GOING MOBILE AND LAST MINUTE

Returning to the serious stuff, on Thursday morning VB2013 went mobile with a series of presentations on various different aspects of mobile malware threats. Rowland Yu kicked things off with an in-depth look at GinMaster – a piece of *Android* malware distributed via the many third-party app markets in China and which is estimated to bring in approximately US$245,000 per month for the criminals behind it.

Samir Mody tackled the subject of *Android* malware obfuscation – as the volume of *Android* malware grows and more anti-virus vendors provide protection against it, it is likely to be only a matter of time before *Android* malware obfuscation becomes routine, as it has in *Windows* malware. Samir highlighted some of the current methods of obfuscation used in *Android* malware, and showed examples of .dex byte-code and data obfuscation techniques which are likely to be abused in the future.

Axelle Apvrille focused on the security and privacy issues of *Android* ad kits, revealing the shocking level of personal detail collected by most in-app ad kits – including information on age, gender, sexual orientation, marital status, religion, education, income and ethnicity – and concluding that the current mobile ad model is far too heavily weighted in favour of the advertiser.

On a similar theme, Vanja Svajcer looked at the issue of potentially unwanted applications in the mobile environment. The difference between malware, potentially unwanted applications and legitimate apps for mobile platforms is often much less clear than it is within the desktop world – Vanja laid out a set of common criteria that can be used by researchers and developers for detecting and determining the differences between malware and potentially undesirable apps.

Finally in the mobile-themed block, Roman Unuchek looked at the web infections that only lead to malicious redirection if the request comes from a mobile device, detailing some of the major redirection techniques.

Besides mobile-related presentations there were several other highlights on Thursday morning, including Gunter Ollmann describing how penetration testing with live malware has become a must in today's enterprise networks, and the Technical stream saw the start of the last-minute presentations.

The last-minute presentations – the section of the conference set aside for talks that are submitted and selected as close to the conference as possible – kicked off with Gabor Szappanos detailing how targeted attacks hide behind clean applications. Next up, Christy Chung took a look at the facts behind recent South Korean government DDoS attacks, and John Graham-Cumming detailed how open DNS resolvers are used to launch huge DDoS attacks against websites and DNS servers – demonstrating how frighteningly easy it is to launch a massive DDoS attack.

After lunch, the last-minute presentations also visited the topic of *Android* threats, with Adrian Ludwig explaining *Android* security from *Google*'s point of view. He revealed that fewer than an estimated 0.001% of malicious app installations on *Android* are able to evade its multi-layered defences and that, according to the company's data, users are more likely to install non-malicious rooting and SMS fraud apps than traditional types of malware such as spyware, trojans, backdoors and malicious exploits.

Ross Gibb followed with a very popular presentation detailing how he and his colleagues successfully sinkholed around 500,000 bots (roughly half) of the ZeroAccess P2P botnet, working together with ISPs and CERTs worldwide to clean up infections. Next, Robert Lipovsky and Anton Cherepanov looked at the sophisticated and extremely

Adrian Ludwig shares Google's point of view on Android security.

Life is a cabaret! Spectacular performances from German Dance Sensation.

active Hesperbot banking trojan whose activity peaked between July and September 2013.

The final last-minute presentation was given by Dennis Batchelder and Hong Jia of *Microsoft*, who described recent attacks against their and other AV vendors' automation systems via crafted files. They called for the industry to work together to share information about such crafted files and fix systems and processes before this type of attack can cause significant damage.

Two more sponsor presentations rounded off the day on Thursday, with *Avast*'s Peter Kalnai and Jaromir Horejsi asking 'Are *Linux* desktop systems threatened by trojans?' and *Qihoo 360*'s Paul Fan looking in detail at targeted attacks against Chinese online card games.

GIVE 'EM THE OLD RAZZLE DAZZLE

No *VB* conference would be complete without the glitz and glamour of the gala dinner evening – and this year's gala certainly had glitz and glamour in spades. Dance troupe German Dance Sensation opened the evening with a performance full of sequins, bling, feathers and high kicks, and continued to inject plenty of pizzazz into the evening with several revue-style dance numbers that were both colourful and impressively energetic.

The mellow sounds of Oui D'Accord.

A more mellow tone was set for the rest of the evening by musical trio Oui D'Accord who played their own unique blend of musette, tango and jazz. It was a treat to listen to live music performed by a talented group of musicians, and their smooth sounds created the perfect atmosphere for a relaxing end to the evening. (Of course, the end of the dinner wasn't the end of the evening for the dedicated party people in our midst – I hardly need to mention that *Avast*'s beer continued to flow freely and the hotel's bar was packed to the rafters long into the night.)

THE FINAL PUSH

There were a few bleary eyes on Friday morning, but most delegates who came down for the early morning sessions seemed impressively alert (perhaps in comparison with the *VB*-drinks-reception/*Avast*-bar/*G-Data*-party combo the gala dinner night had been a relatively tame one).

Bravely taking the opening slots on Friday morning were Cathal Mullaney, who presented an end-to-end analysis of the Android.Bmaster trojan in the Technical stream, and Eileen Sinnott and Raymond Roberts who looked at new security measures in *AutoCAD* in the Corporate stream. Next up, Fabio Assolini gave an energetic overview of malicious use of PAC (proxy auto-config, or as Fabio and his colleagues have dubbed them 'problem auto-config') files. Attacks using malicious PAC files have reached a level of efficiency whereby an entire bank account can be hacked with just a 1KB file. Fabio showed the evolution of the attacks, how the bad guys are bypassing detection, and some of the messages the attackers have directed at analysts – politely, and not so politely, asking to be left to continue their shady activity uninterrupted.

After a very welcome mid-morning caffeine boost, proceedings continued with Samir Patil taking a close

No, not the latest boy band on the block about to break into song, but a panel of security experts discussing collateral damage in the age of cyberwarfare (L to R: Tom Cross, Gunter Ollmann, Pedram Amini, Mikko Hyppönen and Ryan Naraine).

Thank you to all of the VB2013 speakers (including those not pictured here!).

look at Blackhole spam and how it can be blocked, and Ciprian Oprisa and George Cabau presenting an overview of ransomware. Ciprian and George showed some of the encryption methods used by various types of ransomware and warned that the amount of ransomware in the wild is on the increase.

There were two sleuthing-themed presentations on Friday afternoon: Peter Kruse focused on the investigation of a large phishing cluster operating out of Morocco, while double act Bob Burls and Graham Cluley described how members of the gang behind the SpyEye botnet were tracked down and arrested in the UK and in Estonia.

The final presentation in the Corporate stream was given by Sergey Golovanov, who discussed the reality of the business-to-government malware market and presented details of the activities of two companies: UK-based Gamma International and Italian Hacking Team – which have sold backdoors and spying tools to governments around the world. Sergey also provided one of the most captivating moments of the conference when he screened a recording of his own version of British comedian Tim Minchin's 'Song for Phil Daoust'. Sergey had re-titled the piece 'Song for John Doe' and dedicated it to the unknown creator of malware for law enforcement. Sergey managed to get an entire room of security experts tapping their feet and clapping along to the chorus of the song – a highly entertaining moment, while also being one of the most bizarre (I had to pinch myself to make sure the late night hadn't got the better of me and that I really was witnessing a security expert singalong).

Finally, rounding off the conference in a not too dissimilar vein to that in which it began, a discussion panel tackled the issue of collateral damage in the age of cyber warfare. Led by Ryan Naraine, panel members Tom Cross, Gunter Ollmann, Pedram Amini and Mikko Hyppönen made some strong points on both the definition and the nature of cyber conflict – an important and controversial subject.

UNTIL NEXT TIME...

As is ever the case, this report has barely scratched the surface of what went on over the course of the three days in Berlin. There were many more excellent presentations that I have not been able to mention, and I would like to thank all of the VB2013 speakers, session chairs and panel members for their huge contribution to the event, as well as the conference sponsors (*Avast*, *AV-Test*, *ESET*, *Qihoo 360*, *HP*, *NSS Labs*, *ThreatTrack Security*, *AV-Comparatives*, *Ikarus Software*, *OPSWAT* and *Veszprog*). My thanks also go to the whole of the *VB* team, the onsite crew and the *Cue Media* technicians for their tremendously hard work and the vital role they played in the running of the event.

Thanks to a number of delegates opting to forgo their printed copies of the VB2013 conference proceedings, a donation of £570 has been made to the conservation charity WWF (http://wwf.panda.org/).

Next year sees the conference hop back across the pond to the West coast of the US, with VB2014 taking place in Seattle, WA, from 24 to 26 September. I look forward to seeing you there.

(Photographs courtesy of: Morton Swimmer, Jeannette Jarvis, Andreas Marx, Pavel Baudis and Eddy Willems. More photographs from the event can be viewed at http://www.virusbtn.com/conference/vb2013/ photos and slides from the presentations are available at http://www.virusbtn.com/conference/vb2013/slides/index.)