CONFERENCE REPORT

OH, VIENNA!

Helen Martin

This year the *VB* conference returned to European soils, landing in the majestic city of Vienna, Austria. Boasting dancing horses, imperial palaces, grandiose opera houses, macabre catacombs, white knuckle rides in the Prater Park, sedate fiaker rides around the historical city centre, classical concerts and operettas, river trips and more, it's a wonder that the 340 conference delegates turned up to each day of the conference instead of spending their time exploring the delightful city. But, thanks to a programme of exceptional presentations, the *VB* conference halls were full to the seams on each of the three days of the conference.

Modern chic... or modern chick?

In contrast to the rest of the city the conference venue, the Hilton Vienna, oozed modern chic, with contemporary sculptures on every corner. The Hilton's newly built congress centre couldn't have been more suited to our needs, with congress halls 1 and 2 right next door to each other and a small, but perfectly formed exhibition area in which the nine conference sponsors set up camp with their exhibition booths.

OVERTURE

The conference kicked off on Wednesday morning and went straight from the opening address into the traditional two-stream format. Opening the conference programme in the technical stream was Maksym Schipka, who took a fascinating look at automation methods for malware generation, concentrating in particular on the story of Warezov and demonstrating how offline polymorphism is likely to become an increasingly powerful tool for blackhats – as well as an increasingly complex challenge for the anti-malware industry. Meanwhile, Sami Rautiainen started proceedings in the corporate stream with a detailed look at malicious web-based scripting.

After lunch, the corporate stream saw two papers on an up-and-coming area of interest for malware authors: the world of online gaming and virtual universes. Hannah Mariner and Amir Fouda co-presented an overview of game-targeting malicious software, highlighting the motivations of malware authors who target users of Massively Multiplayer Online Role-Playing Games (MMORPGs), taking a closer look at some of the malicious programs themselves, and looking at possible future trends. The question everyone in the audience seemed to want answered was whether the presenters had spent much time playing the games themselves. Hannah and Amir admitted that they had indeed spent 'some time' playing the games – all in the name of research, of course. In the following presentation, Morton Swimmer took a look at security in the fascinating realm of virtual universes – which have long been the domain of gamers, but which have now started to infiltrate the corporate world. Morton urged the security industry to think hard, while virtual universes are still in their relative infancy, about how security and privacy need to work in this area.

Later in the technical stream, Aleksander Czarnowski presented a follow-up to his VB2006 presentation on rootkits and anti-rootkit safeguards, this time presenting updated information relating to *Windows Vista* (which was yet to be released this time last year). Alex pointed out a number of vulnerabilities and weaknesses that could be exploited by *Vista* kernel rootkits and concluded that even without breaking any of the new layers of defence introduced by *Vista*, the operating system will never be immune to kernel rootkits since it will always be possible to trick a user with high-level privileges into installing one.

Afterwards, Alex Hinchliffe asked whether patching is always with the best intentions. He described the new trend among malware of patching applications and libraries on disk in order to launch attacks, using two pieces of recent malware, PWS-Goldun.dr and W32/Crimea, as examples.

Wednesday evening saw the first two of the three sponsor presentations from this year's platinum sponsors (*ESET*, *Grisoft* and *Microsoft*). To start, *Grisoft*'s Larry Bridwell presented a lively and entertaining talk entitled 'Surfing in a hurricane', which was followed by *ESET*'s Randy Abrams and Pierre-Marc Bureau. Randy and Pierre-Marc refuted recent claims that anti-virus is dead, and demonstrated that far from having died out, anti-virus technology is alive and evolving. In the final sponsor presentation, on Thursday evening, *Microsoft*'s Vinny Gullotto enlightened the audience on 'Malware research and response today at *Microsoft*'. At times over the past 12 months it has seemed as if barely a week has gone by without news of another handful of names in the anti-virus industry making the move to Redmond (or one of the company's other main virus research centres) and in his presentation, Vinny provided a light-hearted, yet informative glimpse into how *Microsoft* is organizing its security team, the company's intentions in the security field and what changes may be ahead.

Back to Wednesday evening, and the VB2007 welcome drinks reception was held in the hotel's Klimt Gallery, overlooking the lobby at the Hilton Vienna. An informal affair, a string ensemble provided tasteful background music, while delegates caught up with old acquaintances and networked with new ones over a glass (or two) of the local brew.

A hard evening's networking at the VB2007 welcome drinks reception.

FIRST MOVEMENT

Thursday morning kicked off bright and early at 9am with a demonstration of a spyware-resistant virtual keyboard by Richard Ford in the technical stream, and something of a trip down memory lane in the corporate stream. Martin Overton looked back at 'the journey so far' in the anti-virus world, presenting graphs and statistics of the trends in malware growth since the start of the malware problem on DOS and *Windows*. (An updated version of Martin's paper – modified following feedback from members of the audience – can be found at http://momusings.com/papers/VB2007-The-Journey-So-Far-1.02.pdf.)

Dmitry Gryaznov and Joe Telafici next proposed some solutions for the strain on storage, bandwidth, processes and personnel suffered by vendors as a result of an enormous number of incoming malware samples. Following analysis of the source, timing and frequency of incoming submissions, they concluded that the AV industry is effectively DoS-ing itself by continually resending the same samples over and again. They suggested the implementation of a centralized database of sample hashes, accessible to multiple vendors, against which new samples can be checked prior to being sent on, thus avoiding resending the same samples time and again.

After morning coffee, Andreas Marx and Frank Dessmann took to the stage in the corporate stream. Such was the interest (and controversy) surrounding their presentation that there was standing room only at the back of the conference hall. Their talk focused on what they (and others) perceive to be the current problems with the WildList, and on what can be done to turn it back into a useful metric. Andreas condemned the current WildList for having too few active reporters of new samples (meaning that the number of malicious programs on the list is several orders of magnitude lower than the actual number of malicious programs circulating), for the fact that copies of the list are issued only monthly, and for the fact that the list reports only self-replicating malware – which represents the minority of the threats seen by vendors every day.

Andreas Marx survived his presentation relatively unscathed.

However, the room was not without a number of vehement supporters of the WildList, who argued that the current system of requiring each sample to be verified by skilled reporters ensures that the quality of samples is very high, and that the automated systems and processes proposed by Marx and Dessmann to improve the WildList could actually have the converse effect, making it difficult to verify whether all samples are actually malicious. The session concluded with a fairly heated debate, but thankfully no weapons were drawn.

Meanwhile, in the technical stream the first of this year's anti-spam papers were being presented, with Vipul Sharma looking at continual feature selection as a means to enhance the efficiency of corporate anti-spam solutions, Tim Ebringer presenting a paper looking at the crossover between malware and spam, and Sándor Antal describing methods for detecting spam images using statistical features.

Thursday afternoon saw the introduction of a brand new feature in the technical stream. After considering all the feedback from VB2006 delegates, it was decided that a slightly different format was required for technical papers that would allow more up-to-the-minute topics to be presented. The 'last-minute' presentations were the result.

A call for last-minute papers was put out a few weeks prior to the conference, with would-be speakers being warned that they would only have 10 days in which to prepare their presentations if selected. After a good response to the call for papers, eight were selected and their eager presenters took to the stage on Thursday afternoon. The 20-minute 'turbo' talk format proved to be very successful, with the presentation topics covering: high-speed image part recognition in spam filters; novel code obfuscation using COM; the challenges associated with terminating hidden processes; a practical guide to the advantages of using an advanced automated threat analysis system; phylogenetic comparisons of malware; a detailed description of a targeted banking trojan attack; and a detailed look at the ongoing Storm threat. With such an overwhelmingly positive response to the last-minute sessions, delegates can expect to see a return of the format next year.

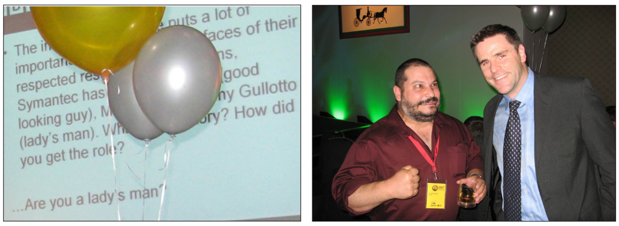
Meanwhile, Thursday afternoon in the corporate stream saw Jeannette Jarvis proposing to transform victims into cyber-border guards; Andrew Lee and David Harley questioning the effectiveness of certain types of phishing education; and some more anti-spam papers, including a fascinating look at stock spam and pump-and-dump scams. Dmitri Alperovitch demonstrated that, using stolen brokerage account data to buy a company's stock and increase its value, fraudsters can easily make up to $40,000 profit in just half an hour.

INTERVAL

Of course, no *VB* conference would be complete without the traditional *VB* gala dinner evening. This year the gala evening began with a slightly unusual form of entertainment – otherwise known as a stitch-up.

It had come to the attention of a small number of delegates that a particularly well known face in the AV industry, one Mr Joe Telafici, was due to celebrate a special birthday the following day. His 'friends' consequently set about actioning an elaborate plan with which to well and truly stitch him up.

In cahoots with the *VB* organizers, it was arranged for a 'journalist from the BBC' (otherwise known as *VB* crew member Jonathan Clarke – whose disguise consisted of swapping his crew T-shirt for suit and tie) to come and record a somewhat tricky interview with Joe. Later that evening, as delegates took their places at the dinner tables the 'renowned, and highly respected BBC journalist' Jonathan Clarke took to the stage to provide an insight into his unique interviewing technique, using a playback of his earlier interview with Joe as a demonstration. Questions that must have made Joe squirm earlier in the day had the audience in fits of laughter (my favourite has to be 'Are you a ladies' man?' – a question which, like many of the others, Joe handled admirably) and by the end of the brief presentation Joe was left in no doubt that he had been well and truly stitched up.



Birthday boy Joe Telafici 'congratulates' Jonathan Clarke on his new-found journalistic talents.

Joe must be congratulated for coping with a difficult interview so well and for taking the joke in such good humour, and Jonathan must be congratulated on playing it straight the whole way through – not to mention for having the nerve to stand in front of an audience of 340+ with neither a shadow of a nerve nor a waver from his journalist persona.

The grace and elegance of a bygone era.

Pranks out of the way, it was time for the evening's scheduled entertainment and the audience was wowed by the grace and elegance of two couples recreating the atmosphere of a traditional Viennese ball, performing the Fächer polonaise, the Blue Danube waltz, the Fledermaus quadrille and the Radetzky march.

Later in the evening, as the sumptuous four-course meal drew to a close the *VB Gala Casino* opened its doors for business, with delegates trying their luck at the tables in the hopes of being the night's first, second or third place winner – for which suitably silly prizes were awarded.

SECOND MOVEMENT

Back to the serious stuff and despite a late finish on Thursday night, Friday morning kicked off with remarkably full sessions in both streams – such was the draw of the presentation topics in the early morning slots. In the

Place your bets! Delegates compete for a USB piano keyboard, a remote-controlled helicopter and an iPod Shuffle.

High jinks and capers at the VB gala dinner.

technical stream Eric Filiol put forward a formal model proposal for malware stealth, while in the corporate stream, the über-cool Guillaume Lovet presented a follow-up to his VB2006 presentation on the business models of cyber criminals – this time delving deeper underground, and shedding light on new and anticipated business models as the borders between crime and cybercrime become ever thinner.

After a break for coffee, icon of the AV industry Vesselin Bontchev presented a paper on the virusability of modern mobile environments – explaining why some of the newer versions of mobile operating systems are less vulnerable to self-replicating malware than their previous incarnations. On a similar theme, Nicolas Brulez took a look at unpacking PE files on *Windows Mobile*, and Marius van Oers examined the security of *Apple* media files and the *iPhone*.

Meanwhile in the corporate stream, David Perry insisted that, unlike what we can usually expect from a David Perry production, his presentation would contain no jokes or amusing anecdotes, sticking instead to the serious subject matter of the paper. While he was true to his word – presenting a very interesting look at malware classification from the point of view of economically motivated threats – his presentation was certainly no less engaging than usual.

The first session after lunch saw another standing-room-only situation in the corporate stream as Alex Shipp spoke about his involvement with the analysis of evidence from the trial of US substitute teacher Julie Amero. Julie was convicted in January this year on four counts of risk of injury to a minor for allegedly surfing pornographic websites while in charge of classes of school children. Alex and most of the AV industry argue that Julie was in fact the computer-illiterate victim of an adware-infected machine serving pop-ups. Alex's presentation was fascinating, yet it was ultimately frustrating to hear that the case has not yet been resolved and to realize that much of Julie's suffering could have been avoided with a better argued defence case.

FINALE

Rounding off this year's conference we were delighted to welcome representatives of the FBI and other international law enforcement agencies for a panel session providing an insight into their work in the fight against online organized crime. Led by David Thomas of the FBI, panel members Stacy Arruda, also from the FBI, Mark Oram of the UK's CPNI, and Kevin Zuccatto from the Australian Federal Police gave a short presentation about their ongoing work before taking questions from the floor. In what must have been the most popular *VB* panel discussion in recent years, it was impossible to find time for the panel to answer everyone's questions. There emerged from the session a certain level of frustration, with both law enforcement and AV vendors seemingly wanting to help one another, but without a clearly defined way in which to do so. Discussions continued afterwards and there was also talk of making law enforcement panels a more regular feature at *VB* conferences in the future.

A motley crew – my thanks to the very hard-working VB team, helpers from TU Wien and the Cue Media crew.

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 VB2007 speakers for their contributions – this year's presentations were an exceptionally good selection.

In particular I'd like to thank Mario Vuksan and Peter Eicher for stepping in at the last minute to replace speakers who had to withdraw from the conference at short notice. Some of the presentation slides are now available to download at http://www.virusbtn.com/conference/vb2007/ and a selection of photographs will also be available shortly.

VB2008 OTTAWA: 1–3 OCTOBER 2008

Next year we hop back across the Atlantic to Canada, with VB2008 taking place 1–3 October 2008 at the Westin in Ottawa. I very much look forward to welcoming you all there.

Photographs courtesy of: Randy Abrams, John Alexander, Jeannette Jarvis, Andrew Lee, Andreas Marx, Alex Shipp and Eddy Willems.