virus BULLETIN Covering the global threat landscape

CONFERENCE REPORT: VB2014

Martijn Grooten
Virus Bulletin, UK

There is a Dutch expression that says that you shouldn't trust a butcher who judges his own meat. Perhaps then, when the *Virus Bulletin* Editor says that the *Virus Bulletin* conference was really good, you should take these words with a pinch of salt.

But it *was* really good.

As one of the oldest security conferences in the world, *Virus Bulletin* has earned a solid reputation in the industry, and it was thanks to this reputation – and an exciting programme of events – that we saw a record number of delegates descend on Seattle for the 24th edition of the conference. While pessimists might suggest that the record attendance figures are simply an indication of how many things still need to be fixed in the world of security, realists will point out that it also shows that the content is more relevant than ever.

FROM THE CONFERENCE TO THE WILD

Indeed, several of the presentations given at VB2014 have since become news, either because predictions made in those presentations have become true, or because attacks described in them have been discovered in the wild.

Vadim Kotov's paper on how easy it is for malware authors to use advertisements to spread malware predicted a rise in such attacks – as has been seen in recent months. In his presentation on 'BlackEnergy', Robert Lipovsky spoke about what would later become known as the 'SandWorm' attack – and even discussed the related zero-day that *iSIGHT Partners* would later discover independently. Tao Wei and Hui Xue spoke about how *Apple*'s Enterprise Provisioning Program could be abused to install malware on *iOS* devices – something the WireLurker malware subsequently did.

Most of all, though, I think that what made the programme so good was that it covered so many different aspects of IT security – from DNSSEC to malware engaged in click-fraud, and from hacking a smart TV to using TCP/IP packet sizes to detect spam. Not only does the diversity in topics show that *VB* has long stopped being *solely* 'the anti-virus conference', but more importantly, it shows how different aspects of security have increasingly become intertwined.

VULNERABILITIES

2014 has been the year of the vulnerability, and for that reason we asked Katie Moussouris (*HackerOne*) to give a keynote address on the subject. Few people know more about vulnerabilities than Katie, but rather than force her opinion upon the audience, Katie's keynote was interactive and gave the audience the opportunity to engage in a debate on vulnerabilities and bug bounties.

One vulnerability that wasn't discussed during the keynote was 'Shellshock', which wouldn't become publicly known until later the same day. Of course, there had been plenty of buzz around the Shellshock vulnerability by the time the closing panel came around – in which Chester Wisniewski, David Jacoby, Nick Sullivan and Daniel Schwalbe discussed how vulnerabilities should be disclosed when they are so big that just about everyone seems affected, as was the case with Heartbleed and, indeed, Shellshock.

Of course, vulnerabilities exist everywhere, and in their presentations David Jacoby and Jeongwook Oh both showed how they could hack into home devices – Jeongwook even performed a live demonstration of exactly how he had hacked into his own smart TV.

Jeongwook Oh wasn't alone in including a demonstration in his presentation: Hong Kei Chan and Liang Huang showed how point-of-sale malware works, and Candid Wüest made a point about the insecurity of wearable devices by showing that he could count how many of the people who had been at the drinks reception on Wednesday evening had missed breakfast the next morning.

LINUX, OS X, IOS, ANDROID, TIZEN… AND A BIT OF WINDOWS TOO

Never has the *Virus Bulletin* conference been held at such close proximity to *Microsoft*'s headquarters, yet never have there been so many talks dedicated to non-*Microsoft* operating systems.

Evgeny Sidorov (*Yandex*) and Pierre-Marc Bureau (*ESET*) shared the stage to describe the research their respective companies had conducted on the 'Ebury' and 'CDorked' malware families that target *Linux* servers, while *Symantec* researchers Cathal Mullaney and Sayali Kulkarni looked at other families targeting those same servers.

No fewer than three presentations looked at various aspects of malicious *Android* apps, while Irfan Asrar looked at the lesser known *Tizen* mobile operating system.

Apple's devices remain popular among security experts, and they tend to have a pretty good reputation when it comes to their security, but that doesn't mean there are no issues. Apart from the aforementioned paper on *Apple*'s Enterprise Provisioning Program that showed a surprisingly large infection vector for *iOS*, Patrick Wardle showed that there are many ways for malware to maintain persistence on an *OS X* device.

Of course, many presenters talked either implicitly or explicitly about threats faced by *Windows* users: Micky Pun and Neo Tan looked at the Caphaw malware, while Hexiang Hu's talk covered analysing .NET malware, and Jean-Ian Boutin discussed the webinjects used (in practice) by *Windows* malware.

BEYOND THE OS AND ON TO THE NETWORK

Some speakers went a little deeper and looked beneath the operating system: Xeno Kovah captivated the audience with his presentation on BIOS-level attacks, while Shane Macaulay explained how one could detect any changes in process or kernel memory, and thus detect the presence of rootkits.

There were more than 50 presentations, each of which looked at a particular aspect of cybersecurity, and each of which considered the problem from a different angle.

Other speakers looked at the network: Cristina Vatamanu revealed details of a clever proxy network sold to botnet owners to hide their locations; Wei Xu and Kyle Sanders talked about a method for predicting malicious domains; and Dhia Mahjoub looked for hotspots of maliciousness by studying the AS graph.

Of course, several presentations discussed the oldest vulnerability of all: gullible humans. Jérôme Segura, for instance, talked about recent developments in the world of tech support scams. But it's not only the victims of cybercrime that make mistakes: Matt Bing shared what he found by crawling open directories on malware servers.

In total, there were more than 50 presentations, each of which looked at a particular aspect of cybersecurity, and each of which considered the problem from a different angle.

We cannot make those who have never attended a *VB* conference understand what it is like to be at one (for that, you'll have to come to Prague in 2015 or Denver in 2016), but we can share the content presented at the conference. We are currently in the process of uploading most of the VB2014 papers and recordings to our website and *YouTube* channel, respectively.

SLEEPLESS IN SEATTLE

As always during security conferences, much of the important stuff happened in the fringes of the actual event, whether during private discussions in hotel rooms, in the hotel bar late at night or, of course, during the drinks reception and the gala dinner.

The latter was made extra special this year because the first ever Péter Szőr Award was presented. The Award commemorates the life and work of the brilliant security researcher, who sadly passed away in November last year. Jeannette Jarvis presented the award to *ESET* researchers Pierre-Marc Bureau, Alexis Dorais-Joncas and Marc-Etienne Léveillé, for their work on 'Operation Windigo', which was performed together with their colleagues Olivier Bilodeau, Joan Calvet and Benjamin Vanheuverzwijn.

Around this emotional moment there was great food and wine, and colourful entertainment from a local group of Chinese lion dancers as well as a stunning show combining fire, dance and acrobatics from local acrobatic troupe Cabiri.

SEE YOU IN PRAGUE… AND/OR DENVER!

This conference report hasn't come close to mentioning all of the papers presented, and covers only a small part of what

As always, there were plenty of opportunities at VB2014 for networking and having some fun.

went on in Seattle. I would encourage readers to check out the papers, slides and recordings from VB2014, which can be accessed via the abstract page for each paper at http://www.virusbtn.com/conference/vb2014/programme.

I would like to thank all of the speakers, the session chairs and panel members for their huge contribution to the event, and of course the conference sponsors (*Avast*, *ESET*, *HP*, *Qihoo 360*, *Baidu Antivirus*, *Microsoft*, *NSS Labs*, *Tencent*, *Bitdefender*, *Cylance*, *Lynx Software* and *OPSWAT*), without whose support the conference wouldn't be possible. And of course, I'd like to thank the *VB* team and the *Cue Media* technicians.

I hope to see you for another exciting event next year in Prague (VB2015: 30 September to 2 October 2015), and in 2016, when we're back in the States, in Denver, CO (VB2016: 5–7 October 2016).

(Photographs courtesy of Andreas Marx, Eddy Willems, Jiri Sejtko, Morton Swimmer and Pavel Baudis. More photographs from the event can be viewed at http://www.virusbtn.com/conference/vb2014/photos.)

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Consultant Technical Editors: Dr Morton Swimmer, Ian Whalley

© 2014 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England.
Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/