vb 2017 MADRID

virus BULLETIN

Virus Bulletin International Conference

4–6 October 2017 Madrid, Spain





- Emerging and advanced threats
- State-sponsored attacks
- Mobile security
- Healthcare security
- Insider threats
- Spyware
- Anti-malware tools & techniques
- Attacks on civil society
- Network security
- Botnets
- The fight against organized online crime
- World-leading security experts
- Networking opportunities

sponsored by:

ESET ENJOY SAFER TECHNOLOGY™ Tencent 腾讯 PC Matic THE WORLD NEEDS BETTER SECURITY. WE GOT IT. OPSWAT Symantec 360 TOTAL SECURITY Free Forever! secudit the risk analyzer

REGISTER ONLINE AT WWW.VIRUSBULLETIN.COM

DAY 1: WEDNESDAY 4 OCTOBER 2017

	RED ROOM	GREEN ROOM	SMALL TALKS
08:00	**Registration / badge collection**		
08:30	**Early morning refreshments**		
10:30 – 10:50	**Opening address**		
10:50 – 11:30	**Keynote address: Inside Cloudbleed** John Graham-Cumming *Cloudflare*		
11:30 – 12:00	**Have you scanned your BIOS recently?** Aditya Kapoor *Cylance*	**BPH exposed – RBN never left they just adapted and evolved. Did you?** Dhia Mahjoub *Cisco Umbrella (OpenDNS)* Jason Passwaters *Intel471*	**TBA**
12:00 – 12:30	**Getting under the skin: an in-depth look at MSIL malware obfuscation techniques and strategies for deobfuscation** Kaarthik Muthukrishnan *K7 Computing*	**Walking in your enemy's shadow: when fourth-party collection becomes attribution hell** Juan Andres Guerrero-Saade & Costin Raiu *Kaspersky Lab*	
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Nine circles of Cerber** Stanislav Skuratovich & Neomi Rona *Check Point Software Technologies*	**Modern reconnaissance phase on APT – protection layer** Paul Rascagneres & Warren Mercer *CiscoTalos*	**TBA**
14:30 – 15:00	**Dridex v4 - AtomBombing and other surprises** Magal Baz *IBM*	**TBA** Claudio Guarnieri *Amnesty International*	
15:00 – 15:30	**Attack points in browsers still abused by banking trojans** Peter Kalnai & Michal Poslusny *ESET*	**The sprawling market of consumer spyware** Joseph Cox *VICE Motherboard*	
15:30 – 16:00	**Tea/coffee**		
16:00 – 16:30	**Hacktivism and website defacement: motivations, capabilities and potential threats** Marco Romagna & Niek Jan van den Hout *The Hague University of Applied Sciences*	**Offensive malware analysis: dissecting OSX/FruitFly via a custom C&C server** Patrick Wardle *Synack*	**TBA**
16:30 – 17:00	**Crypton – exposing malware's deepest secrets** Julia Karpin & Anna Dorfman *F5 Networks*	**XAgent: APT28 cyber espionage on macOS** Tiberius Axinte *Bitdefender*	
17:00 – 17:30	**TBA (sponsor presentation)**	**TBA (sponsor presentation)**	
19:30	**VB2017 drinks reception**		

The conference

The packed programme boasts an exceptional line-up of some of the world's top IT security experts, covering topics ranging from network security, hacking and vulnerabilities, to anti-malware tools and techniques, mobile threats, spam and social networking threats.

Ten sessions are set aside for the highly popular 'last-minute' technical presentations which deal with up-to-the-minute specialist topics and are submitted and selected just three weeks before the conference (the schedule will be announced to delegates prior to the start of the conference).

DAY 2: THURSDAY 5 OCTOBER 2017

	RED ROOM	GREEN ROOM	SMALL TALKS
08:00	**Early morning refreshments**		
09:00 – 09:30	**The life story of an IPT – Inept Persistent Threat actor** Adam Haertle *UPC Poland*	**Last-minute paper: TBA**	**TBA**
09:30 – 10:00	**Operation Orca – a cyber espionage diving in the ocean for at least six years** Chia-Ching Fang & Shih-Hao Weng *Trend Micro*	**Last-minute paper: TBA**	
10:00 – 10:30	**Linking Xpaj and Nymaim** Doina Cosovan & Catalin Valeriu Lita *Security Scorecard*	**Last-minute paper: TBA**	
10:30 – 11:00	**Tea/coffee**		
11:00 – 11:30	**Last-minute paper: TBA**	**Android reverse engineering tools: not the usual suspects** Axelle Apvrille *Fortinet*	**TBA**
11:30 – 12:00	**Last-minute paper: TBA**	**Sophisticated router malware: more than just default passwords and silly scripts** Himanshu Anand & Chastine Menrige *Symantec*	
12:00 – 12:30	**Last-minute paper: TBA**	**Mariachis and jackpotting: ATM malware from Latin America** Thiago Marques & Fabio Assolini *Kaspersky Lab*	
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Healthcare security: an inside view** Jelena Milosevic *Independent security researcher*	**Last-minute paper: TBA**	**TBA**
14:30 – 15:00	**Minimum viable security: reaching a realistic SMB security maturity?** Claus Cramon Houmann *Peerlyst*	**Last-minute paper: TBA**	
15:00 – 15:30	**The state of cybersecurity in Africa: Kenya** Tyrus Kamau *Euclid Consultancy*	**Last-minute paper: TBA**	
15:30 – 16:00	**Tea/coffee**		
16:00 – 16:30	**Last-minute paper: TBA**	**Exploring the virtual worlds of advergaming** Chris Boyd *Malwarebytes*	**TBA**
16:30 – 17:00	**TBA** (sponsor presentation)	**TBA** (sponsor presentation)	
19:30	**Pre-dinner drinks followed by gala dinner**		

The 'Small Talk' sessions are slightly longer than the papers on the rest of the programme, with a more informal format that is designed to encourage discussion and debate on a number of topics that are important for the security community. The details of these will be announced in due course.

The VB conference also presents a wealth of networking opportunities: seated lunches on each day of the conference, an informal drinks reception on Wednesday 5 October, and VB's gala dinner evening on Thursday 6 October all provide excellent opportunities to make new contacts, catch up with old ones and discuss the hot topics of the conference.

DAY 3: FRIDAY 6 OCTOBER 2017

	RED ROOM	GREEN ROOM	SMALL TALKS
08:30	**Early morning refreshments**		
09:30 – 10:00	**VirusTotal tips, tricks, and myths** Randy Abrams *Independent security analyst*	**The story of one geographically and industrially targeted zero-day** Denis Legezo *Kaspersky Lab*	**TBA**
10:00 – 10:30	**Chkrootkit: eating APTs for breakfast since 1997** Nelson Murilo Rufino *Pangeia*	**When worlds collide – the story of the Office exploit builders** Gabor Szappanos *Sophos*	
10:30 – 11:00	**Tea/coffee**		
11:00 – 11:30	**Malware deobfuscation: symbolic analysis to the rescue!** Sébastien Bardin *CEA LIST* Robin David *CEA LIST* Jean-Yves Marion *LORIA*	**Stuck between a ROC and a hard place** Holly Stewart *Microsoft*	**TBA**
11:30 – 12:00	**Say hi to malware - using a deep learning method to understand malicious traffic** Zhaoyan Xu, Tongbo Luo, Wei Xu & Kyle Sanders *Palo Alto Networks*	**Knock, knock, knocking on PwC's door** Bart Parys *PwC*	
12:00 – 12:30	**Still a lot to learn: bypassing machine-learning AV solutions** Gilbert Sison & Brian Cayanan *Trend Micro*	**From insider threat to insider asset: a practical guide** Kristin Leary & Richard Ford *Forcepoint*	
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Beyond lexical and PDNS: using signals on graphs to uncover online threats at scale** Dhia Mahjoub & David Rodriguez *Cisco Umbrella (OpenDNS)*	**TBA** Ryan MacFarlane *FBI*	**TBA**
14:30 – 15:00	**A new technique for detecting and blocking the installation of a malicious software based on the reputation of the loadpoint n-grams** Sujit Magar & Prachi Jhanwar *Symantec*	**TBA** Michael Moran *An Garda Síochána*	
15:00 – 15:30	**Tea/coffee**		
15:30 – 16:10	**Keynote address: TBA** Brian Honan *BH Consulting*		
16:10 – 16:30	**Conference closing session**		

Reserve papers

- **Inside Netrepser – a JavaScript-based targeted attack** Cristina Vatamanu, Adrian Schipor & Alexandru Maximciuc *Bitdefender*
- **Peering into spam botnets** Maciej Kotowicz & Jarosław Jedynak *CERT Poland*
- **Record and replay debugging against in-the-wild exploit kits and other practical cases** Jarkko Turkulainen & Jarno Niemelä *F-Secure*
- **Malware on the Go** Angel Villegas *Cisco Systems*
- **Visual malware forensics** Ankur Tyagi *Qualys*

The organizers reserve the right to change the programme without notice.

4–6 October 2017
Novotel Madrid Center, Madrid, Spain

VB2017

VB2017 is hosted by Virus Bulletin, a security information portal, testing and certification body with a formidable reputation for providing users with independent intelligence about the latest developments in the global threat landscape.

Conference registration fee

- Early bird registration fee (until 30 June 2017): US$1705.50 (+ VAT)
- Standard fee: US$1895 (+ VAT)
- *Bona fide* charities and educational institutions: US$947.50 (+ VAT)
- Student tickets will be available for those in full-time education (pricing TBC). Please contact conference@virusbulletin.com.

In order to comply with Spanish VAT laws we are obliged to charge 21% VAT on all conference tickets (with the exception of tickets purchased by Spanish companies providing their Spanish VAT number during the billing process). Under the EU 8th Directive VAT system, EU companies can submit Spanish VAT recovery applications through online portals operated by their own national tax authority. Where there is a tax reciprocity agreement under the 13th VAT Directive between Spain and their home territory, non-EU companies may also be able to reclaim the Spanish VAT charged.

Accommodation

The Novotel Madrid Center is offering VB2017 delegates a special discounted rate of 145 EUR per night for the conference period. (*Please note that the availability of these rates cannot be guaranteed after 1 September 2017*.)

THE CONFERENCE REGISTRATION FEE INCLUDES:

- Admission to all conference sessions
- Conference proceedings in hard copy format
- Exclusive admission to the VB2017 exhibition
- Drinks reception on Wednesday 4 October
- Lunch, early morning refreshments and mid-session coffee breaks on all three days of the event
- Drinks reception followed by gala dinner & entertainment on Thursday 5 October
- Commemorative conference bag and t-shirt
- Wireless Internet access in the conference area of the Novotel Madrid Center hotel

Cover images: Gran Vía. Capitol Building (© José Barea); Glass Palace. The Retiro Park (© Madrid Destino, Cultura, Turismo y Negocio S.A.); La Almudena Cathedral (© Madrid Destino, Cultura, Turismo y Negocio S.A.); Cibeles Fountain (© Madrid Destino, Cultura, Turismo y Negocio S.A.); Plaza de la Villa (© Madrid Destino, Cultura, Turismo y Negocio S.A.); Plaza Mayor (© José Barea); Palacio de Cibeles (© Madrid Destino, Cultura, Turismo y Negocio S.A.).

Virus Bulletin Ltd • The Pentagon • Abingdon • OX14 3YP • UK
Tel +44 1235 555139 • Email conference@virusbulletin.com

Register online at www.virusbulletin.com

Testimonials

The VB Conference is considered by many information security professionals to be the best conference on the circuit – but don't just take our word for it. The following are some of the comments made by delegates of recent VB Conferences:

"This is my favourite conference to attend each year. The content is superb, the networking is bar-none, the organizational aspects are well-polished, you walk away better educated; overall a highly beneficial experience. I love how Virus Bulletin conference brings deep technical talks for researchers but also offers useful information for the enterprise defenders, and then you have small-talks where you can have more intimate and deep conversations with the best security experts in the world." *Jeannette Jarvis, Director, McAfee*

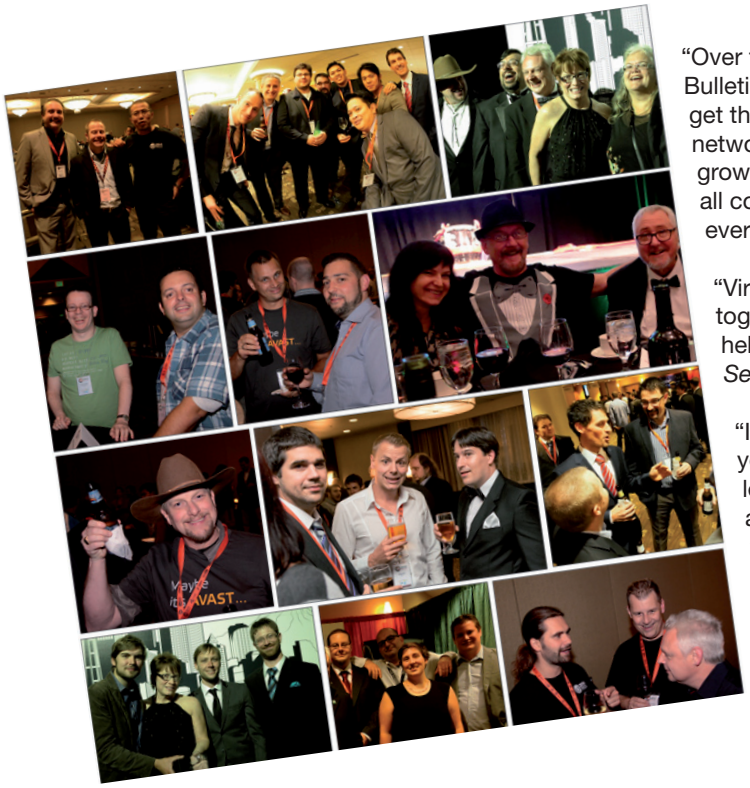
"An outstanding conference to learn the latest in IT security, get new ideas and create new contacts in a very friendly atmosphere. Number 1 for me for many years both in the short and long term." *Conny Javerdal, Swedish Transport Administration*

"Not all security events are created equal – the Virus Bulletin Conference remains one of the few places to find deep, accurate, and above all actionable information that can help your organization defend itself from malicious code today." *Richard Ford, PhD, Chief Technology Officer, Forcepoint*

"A great way to keep up with what's happening in the anti-malware industry." *John Aycock, Associate Professor, University of Calgary*

"Securing our digital world takes innovation and collaboration across all disciplines and industries. There are few gatherings focused on this endeavor that are of the highest quality and passion… VB is one of them. Sharing information, learning the latest research, and connecting with others fighting the good fight is exactly the reason I have been involved for more than 5 years. Don't miss it!" *Jewel Timpe, Security Research Manager*

"The Virus Bulletin conference is a rare opportunity for world's anti-malware experts to gather and freely share ideas. VB is a forum that provides detailed descriptions of timely tools and techniques to combat all forms of malware, making the industry stronger. It is also a chance for us to take off our company hats and socialize. The ability to network with peers from around the industry and around the world makes VB an essential resource for the entire industry." *Mark Kennedy, Distinguished Engineer, Security Technology And Response, Symantec Corporation*



"Over the past 15 years, I have probably attended at least ten Virus Bulletin conferences, and they are truly stellar events. They totally get that we are all there to learn, to share new research and to network. Not only have I made fantastic contacts that have helped grow my business, but I have made some great friends, too. I wish all conferences I attended had the same attention to detail. Worth every penny." *Carole Theriault, Director, Tick Tock Social*

"Virus Bulletin is amazing. Few places have a whole industry together in one place. The connections are invaluable and have helped change the world" *John Alexander, Senior Information Security Engineer, Mayo Clinic*

"I've been attending the Virus Bulletin conference for over 20 years. The reason? There is no better place to be if you want to learn more about the attacks that cybercriminals are launching against companies, and to meet the people who are developing the security software that defends us. If you don't attend VB you're not just missing a great conference, you're putting your company's defences at a disadvantage." *Graham Cluley, Computer Security Expert, grahamcluley.com*