vb 2016 DENVER

Virus Bulletin International Conference

5–7 Oct 2016 Denver, CO, USA

- Emerging threats
- Mobile threats
- Hacking & vulnerabilities
- Anti-malware tools & techniques
- Targeted attacks
- Spam & social networks
- Network security
- Botnets
- World-leading security experts
- Networking opportunities
- The fight against organized online crime

virus BULLETIN

sponsored by:

ESET ENJOY SAFER TECHNOLOGY™ · Microsoft · Tencent 腾讯 · OPSWAT · WEBROOT Smarter Cybersecurity® · AVG Be Yourself · PC Matic THE WORLD NEEDS BETTER SECURITY. WE GOT IT. · CYLANCE · paloalto NETWORKS · 360 TOTAL SECURITY Free Forever! · secudit the risk analyzer

REGISTER ONLINE AT WWW.VIRUSBULLETIN.COM

DAY 1: WEDNESDAY 5 OCTOBER 2016

	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: TBA**		
11:30 – 12:00	**Wild Android Collusions** Prof. Igor Muttik *Intel Security* Jorge Blasco *London City University* Markus Roggenbach *Swansea University*	**Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks** Juan-Andres Guerrero Saade & Brian Bartholomew *Kaspersky Lab*	**TBA**
12:00 – 12:30	**Beware! Zombies are Coming** Zhi Xu, Tongbo Luo & Cong Zheng *Palo Alto Networks*	**APT Reports and OPSEC Evolution, or: These Are Not the APT Reports You Are Looking For** Gadi Evron *Cymmetria* Inbar Raz *Perimeter X*	
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Automating Visibility into User Behaviour Vulnerabilities to Malware Attack** Ferenc Leitold, Anthony Arrott Secudit, Eszter Oroszi & Kalman Hadarics *Secudit*	**"$ echo Internet $>_...": Towards Practical Internet-wide Probing and Crawling** Zhaoyan Xu, Jun Wang Palo Alto Networks, Yucheng Zhou, Wei Xu Palo & Kyle Yang *Palo Alto Networks*	**Android Security** Sebastian Porst & Jason Woloz *Google*
14:30 – 15:00	**Are They Real? Real-Life Comparative Tests of Anti-Virus Products** Fanny Lalonde Lévesque *École Polytechnique de Montréal* Dennis Batchelder *AppEsteem* José M. Fernandez *École Polytechnique de Montréal*	**Detecting Man in the Middle Attacks With Canary Requests** Brian Wallace *Cylance*	
15:00 – 15:30	**Breach Detection, Protection and Response Testing: The Next-Gen Approach** Simon Edwards *SE Labs*	**Hunting Spear Phishers Across the Internet** Suchin Gururangan, Bob Rudis, Roy Hodgman, Aditya Kuppa & Paul Deardorff *Rapid7*	
15:30 – 16:00	**Tea/coffee**		
16:00 – 16:30	**Diving into Malware's Furtive Plumbing** Omer Yair & Or Safran *IBM*	**One-Click Fileless Infection** Himanshu Anand & Chastine Menrige *Symantec*	**IEEE Anti-Malware Support Service** Mark Kennedy *Symantec*
16:30 – 17:00	**Trusted Code Execution on Untrusted Platform Using Intel SGX** Prof. Guevara Noubir & Amirali Sanatinia *Northeastern University*	**Great Crypto Failures** Yaniv Balmas & Ben Herzog *Check Point Software Technologies*	
17:00 – 17:30	**TBA** (sponsor presentation)	**TBA** (sponsor presentation)	
19.30	**VB2016 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.

Nine 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 6 OCTOBER 2016

	RED ROOM	GREEN ROOM	SMALL TALKS
08:00	**Early morning refreshments**		
09:00 – 09:30	**Last-minute paper: TBA**	**Building a Local PassiveDNS Capability for Malware Incident Response** Kathy Wang & Steve Brant *Splunk*	**The Chinese Underground Economy: the Hook007 Group** TBA *Qihhoo 360*
09:30 – 10:00	**Last-minute paper: TBA**	**Open Source Malware Lab** Robert Simmons *ThreatConnect*	
10:00 – 10:30	**Last-minute paper: TBA**	**Debugging and Monitoring Malware Network Activities with Haka** Benoit Ancel & Mehdi Talbi *Stormshield*	
10:30 – 11:00	**Tea/coffee**		
11:00 – 11:30	**Last-minute paper: TBA**	**Defeating Sandbox Evasion: How to Increase Successful Emulation Rate in your Virtualized Environment** Stanislav Skuratovich & Aliaksandr Chailytko *Check Point Software Technologies*	**Inside Exploit Kits** John Bambenek *Fidelis Cybersecurity*
11:30 – 12:00	**Last-minute paper: TBA**	**(In-) Security of Smartphone AntiVirus and Security Apps** Stephan Huber Fraunhofer *SIT* Siegfried Rasthofer Fraunhofer *SIT / TU Darmstadt*	
12:00 – 12:30	**Anti-virus: Help or Hindrance?** Tavis Ormandy *Google* Ryan Naraine *Kaspersky Lab*		
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Last-minute paper: TBA**	**Neverquest: Crime as a Service and On the Hunt for the Big Bucks** Peter Kruse *CSIS*	**The Tor Project** David Goulet *The Tor Project*
14:30 – 15:00	**Last-minute paper: TBA**	**Modern Attacks on Russian Financial Institutions** Jean-Ian Boutin & Anton Cherepanov *ESET*	
15:00 – 15:30	**Last-minute paper: TBA**	**Unveiling the Attack Chain of Russian-Speaking Cybercriminals** Wayne Huang & Sun Huang *Proofpoint*	
15:30 – 16:00	**Tea/coffee**		
16:00 – 16:30	**Last-minute paper: TBA**	**Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis** Stephen Cobb *ESET*	**VB2016 reserve paper** 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 traditional formal 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 7 OCTOBER 2016

	RED ROOM	GREEN ROOM	SMALL TALKS
08:30	**Early morning refreshments**		
09:30 – 10:00	**Smart Outlets. Why We Need Responsible Disclosure!** George Cabau, Radu Basaraba, Dragos Gavrilut & Ciprian Oprisa *Bitdefender*	**Locky Strike: Smoking the Locky Ransomware Code** Roland Dela Paz, Rommel Joven & Floser Bacurio *Fortinet*	**TBA**
10:00 – 10:30	**Mobile Applications: A Backdoor into Internet of Things?** Axelle Apvrille *Fortinet*	**Real-Time Static Analysis : Detecting Zero-Day Ransomware Campaigns** Erdem Aktas & Rachit Mathur *Intel*	
10:30 – 11:00	**Tea/coffee**		
11:00 – 11:30	**Using Machine Learning to Stop Exploit Kits In-Line in Real-Time** Josiah Hagen, Brandon Niemczyk & Jonathan Andersson *Trend Micro Tipping Point*	**All Your Creds Are Belong To Us** Santiago Martin Pontiroli *Kaspersky Lab* Bart Blaze *Independent Researcher*	**The Clean Software Alliance: the Enforcement Perspective** TBA
11:30 – 12:00	**Uncovering The Secrets Of Malvertising** Jérôme Segura & Chris Boyd *Malwarebytes*	**Diving into Pinkslipbot's Latest Campaign** Sanchit Karve, Guilherme Venere & Mark Olea *Intel Security*	
12:00 – 12:30	**The Good, The bad & The Ugly: The Advertiser, the Bot & the Traffic Broker** Matthieu Faou *École Polytechnique de Montréal* Joan Calvet *ESET* Pierre-Marc Bureau *Google* Antoine Lemay & José M. Fernandez *École Polytechnique de Montréal*	**The Elknot DDoS Botnets We Watched** Ya Liu & Hui Wang *Qihoo 360*	
12:30 – 14:00	**Lunch**		
14:00 – 14:30	**Exploit Millions of Pebble Smartwatches for Fun and Profit** Yulong Zhang & Lenx Wei *Baidu X-Lab*	**Operation Sentry Stopper: A Long-Standing Cyber Espionage** Lenart Bermejo, Mingyen Hsieh & Razor Huang *Trend Micro*	**VB2016 reserve paper** TBA
14:30 – 15:00	**GPS Attacks on a 'Shoe String': Methods of Analysis and Countermeasures** Oleg Petrovsky *HP*	**BlackEnergy – What We Really Know About the Notorious Cyber-Attacks** Anton Cherepanov & Robert Lipovsky *ESET*	**VB2016 reserve paper** TBA
15:00 – 15:30	**Tea/coffee**		
15:30 – 16:10	**Keynote address: TBA**		
16:10 – 16:30	**Conference closing session**		

Reserve papers

- Anti-malware Testing Undercover
  Luis Corrons Panda Security & Righard Zwienenberg ESET
- Automatic Classifying of Mac OS X Samples
  Spencer Hsieh, Pin Wu & Haoping Liu Trend Micro
- The TAO of Automated Iframe Injectors – Building Drive-by Platforms For Fun and Profit
  Aditya K. Sood Blue Coat Systems (Elastica)
- Professional Phishers and Their Habits *Marius*
  Tibeica & Cristian Dantus Bitdefender

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

5–7 October 2016
The Hyatt Regency Denver at Colorado Convention Center
Denver, CO, USA

VB2016

VB2016 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 2016): US$1705.50
- Standard fee: US$1895
- *Bona fide* charities and educational institutions: US$947.50
- Student tickets will be available for those in full-time education (pricing TBC). Please contact conference@virusbtn.com.

Accommodation

The Hyatt Regency Denver is offering VB2016 delegates a special discounted rate of $219 (+ taxes) per night for the conference period. (*Please note that the availability of these rates cannot be guaranteed after 12 September 2016*.)

THE CONFERENCE REGISTRATION FEE INCLUDES:

- Admission to all conference sessions
- Conference proceedings in hard copy and CD-ROM format
- Exclusive admission to the VB2016 exhibition
- Drinks reception on Wednesday 5 October
- Lunch, early morning refreshments and mid-session coffee breaks on all three days of the event
- Drinks reception followed by gala dinner & cabaret evening on Thursday 6 October
- Wireless Internet access in the conference area of the Hyatt Regency Denver hotel

Cover images: © VISIT DENVER (Denver skyline, Coors Field); StevieCrecelius (Blue Bear); StanObert (City County Building); SarahWelch (Denver Union Station)

Virus Bulletin Ltd • The Pentagon • Abingdon • OX14 3YP • UK
Tel +44 1235 555139 • Fax: +44 1865 543153 • Email conference@virusbtn.com

Register online at www.virusbulletin.com