vb 2018
MONTREAL 🇨🇦
3 – 5 October 2018

virus BULLETIN

Virus Bulletin
International Conference
3–5 October 2018 Montreal, Canada

- **Emerging and advanced threats**
- **Nation-state attacks**
- **Mobile security**
- **Automotive security**
- **APT groups**
- **Anti-malware tools & techniques**
- **Network security**
- **Botnets**
- **The fight against organized online crime**
- **Workshops - NEW!**
- **World-leading security experts**
- **Networking opportunities**

REGISTER ONLINE AT WWW.VIRUSBULLETIN.COM

DAY 1: WEDNESDAY 3 OCTOBER 2018

	RED ROOM	GREEN ROOM	SMALL TALKS
08:00	Registration / badge collection		
08:30	Early morning refreshments		
10:30 – 10:50	Opening address Martijn Grooten *Virus Bulletin*		
10:50 – 11:30	Keynote address(title TBA) John Lambert *Microsoft*		
11:30 – 12:00	**Exploiting ActionScript3 interpreter** Boris Larin & Anton Ivanov *Kaspersky Lab*	**From Hacking Team to hacked team to…?** Filip Kafka *ESET*	TBA
12:00 – 12:30	**Analysing compiled binaries using logic** Thais Moreira Hamasaki *F-Secure*	**Title TBA** Masashi Nishihata & John Scott Railton *Citizen Lab*	
12:30 – 14:00	Lunch		
14:00 – 14:30	**Unpacking the packed unpacker: reversing an Android anti-analysis library** Maddie Stone *Google*	**Draw me like one of your French APTs – expanding our descriptive palette for digital threat actors** Juan Andres Guerrero-Saade *Insikt Group, Recorded Future*	**The botnet landscape – live threats and steps for mitigation** Peter Dorey *Spamhaus Technology*
14:30 – 15:00	**The missing link in the chain? Android network analysis** Rowland Yu *Sophos*	**Now you see it, now you don't: wipers in the wild** Saher Naumaan *BAE Systems Applied Intelligence*	
15:00 – 15:30	**VB2018 partner presentation (TBA)**	**Who wasn't responsible for Olympic Destroyer?** Paul Rascagneres & Warren Mercer *Cisco Talos*	
15:30 – 16:00	Tea/coffee		
16:00 – 16:30	**DOKKAEBI: Documents of Korean and Evil Binary** Jaeki Kim, Kyoung-Ju Kwak & Min-Chang Jang *Financial Security Institute*	**Fire & ice: making and breaking macOS firewalls** Patrick Wardle *Digita Security*	**Workshop: Manual kernel mode malware analysis** Vanja Svajcer *Cisco Talos*
16:30 – 17:00	**Lazarus Group: one mahjong game played with different sets of tiles** Peter Kalnai & Michal Poslusny *ESET*	**Code signing flaw in macOS** Thomas Reed *Malwarebytes*	
17:00 – 17:30	**Since the hacking of Sony Pictures** Minseok (Jacky) Cha *AhnLab*	**Adware is just malware with a legal department – how we reverse engineered OSX/Pirrit, received legal threats, and survived** Amit Serper *Cybereason*	
19:30	VB2018 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, nation-state attacks and automotive security.

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 4 OCTOBER 2018

	RED ROOM	GREEN ROOM	SMALL TALKS
08:00	Early morning refreshments		
09:00 – 09:30	**Tricky sample? Hack it easy! Applying dynamic binary instrumentation to lightweight malware behaviour analysis** Maksim Shudrak *Salesforce*	**Last-minute paper: TBA**	**TBA**
09:30 – 10:00	**VBA + AMSI: evening the score with macro malware** Giulia Biagini *Microsoft*	**Last-minute paper: TBA**	
10:00 – 10:30	**VB2018 partner presentation (TBA)**	**Last-minute paper: TBA**	
10:30 – 11:00	Tea/coffee		
11:00 – 11:30	**The dark side of WebAssembly** Aishwarya Lonkar & Siddhesh Chandrayan *Symantec*	**Last-minute paper: TBA**	**TBA**
11:30 – 12:00	**TBA**	**Last-minute paper: TBA**	
12:00 – 12:30	**VB2018 partner presentation (TBA)**	**Last-minute paper: TBA**	
12:30 – 14:00	Lunch		
14:00 – 14:30	**Last-minute paper: TBA**	**Uncovering the wholesale industry of social media fraud: from botnet to bulk reseller panels** Masarah Paquet-Clouston *GoSecure*	**Workshop: Android malware reverse engineering for the brave** Axelle Apvrille *Fortinet*
14:30 – 15:00	**Last-minute paper: TBA**	**Explain Ethereum smart contract hacking like I am five** Zoltan Balazs *MRG Effitas*	
15:00 – 15:30	**Last-minute paper: TBA**	**Anatomy of an attack: detecting and defeating CRASHOVERRIDE** Joe Slowik *Dragos*	
15:30 – 16:00	Tea/coffee		
16:00 – 16:30	**Internet balkanization: why are we raising borders online?** Stefan Tanase *Ixia*	**TBA**	**TBA**
16:30 – 17:00	**Where have all the good hires gone?** Lysa Myers *ESET*	**Little Brother is watching – we know all your secrets!** Siegfried Rasthofer, Stephan Huber & Steven Arzt *Fraunhofer SIT*	
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. This year's programme also includes a number of workshops. 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 3 October, and VB's gala dinner evening on Thursday 4 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 5 OCTOBER 2018

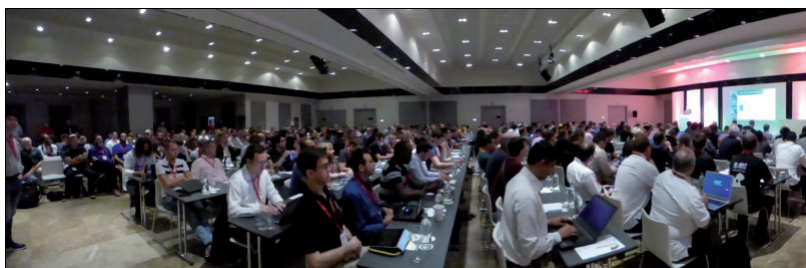|	RED ROOM	GREEN ROOM	SMALL TALKS
08:30	Early morning refreshments		
09:30 – 10:00	**Tracking Mirai variants** Ya Liu & Hui Wang *Qihoo*	**Cost of pwnership: how black market tools and services facilitate the operation of cybercriminal enterprises** Loucif Kharouni *Deloitte*	**TBA**
10:00 – 10:30	**Hide'n'Seek: an adaptive peer-to-peer IoT botnet** Adrian Șendroiu & Vladimir Diaconescu *Bitdefender*	**Artificial intelligence to assist with ransomware cryptanalysis** Alexander Adamov *NioGuard Security Lab*	
10:30 – 11:00	Tea/coffee		
11:00 – 11:30	**Starving malware authors through dynamic classification** Karishma Sanghvi & Joe Blackbird *Microsoft*	**The modality of mortality in domain names** Paul Vixie *Farsight Security*	**TBA**
11:30 – 12:00	**TBA**	**Office bugs on the rise** Gabor Szappanos *Sophos*	
12:00 – 12:30	**VB2018 partner presentation (TBA)**	**From drive-by download to drive-by mining: understanding the new paradigm** Jérôme Segura *Malwarebytes*	
12:30 – 14:00	Lunch		
14:00 – 14:30	**Under the hood – the automotive challenge** Inbar Raz *Argus Cyber Security*	**Windows Defender under the microscope: a reverse engineer's perspective** Alexei Bulazel *River Loop Security*	**TBA**
14:30 – 15:00	**Security issues of IoV devices** Spencer Hsieh & Aaron Luo *Trend Micro*	**Fake News, Inc.** Andrew Brandt *Independent researcher*	
15:00 – 15:30	Tea/coffee		
15:30 – 16:10	Keynote address: **Title TBA** Wendy Nather *Duo Security*		
16:10 – 16:30	**Conference closing session** Martijn Grooten *Virus Bulletin*		

Reserve papers

- **Inside Formbook infostealer** Gabriela Nicolao *Deloitte*
- **Android app deobfuscation using static-dynamic cooperation** Yoni Moses & Yaniv Mordekhay *Check Point*
- **U2Fishing: potential security threat introduced by U2F key wrapping mechanism** Wang Kang *Alibaba Group*

Should no need arise for the reserve papers to replace papers in the main programme, they will each be presented in the Small Talks stream on Friday 5 October.

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, Fortinet

"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

3–5 October 2018
Fairmont The Queen Elizabeth, Montreal, Canada

VB2018

VB2018 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 2018): 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@virusbulletin.com.

Accommodation

The Fairmont The Queen Elizabeth is offering VB2018 delegates a special discounted rate of CAD289 per night (+taxes) for the conference period. (*Please note that the availability of these rates cannot be guaranteed after 7 September 2018*.)

THE CONFERENCE REGISTRATION FEE INCLUDES:

- Admission to all conference sessions

- Conference proceedings in hard copy format

- Exclusive admission to the VB2018 exhibition

- Drinks reception on Wednesday 3 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 4 October

- Commemorative conference bag and t-shirt

- Wireless Internet access in the conference area of the Fairmont The Queen Elizabeth hotel

---

Register online at www.virusbulletin.com