Incident Response: Sharing to Win
Conrad Hotel | Bangkok, Thailand
16-21 June 2013
25th Bangkok June 2013 Annual FIRST Conference
FIRST
Improving Security Together

LOCAL HOST

ThaiCERT

ETDA

DIAMOND

BT

PLATINUM

Microsoft

citi

Adobe

GOLD

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

CONFERENCE PROGRAM

Agenda last updated 10 June 2013. Please note that the program is subject to change.

Please note that some special interest groups are invite-only.

To view an abstract, please click on titles that have the **[+]** indication to expand. Speaker bios will be posted soon.

Print Version Available

Saturday, 15 June 2013

1000-1630	**Education & Training Committee Meeting (Open to non-members)** London 1 - Level 1

Sunday, 16 June 2013

1000-1330	**Education & Training Committee Meeting (Open to non-members)** London 1 - Level 1
1400-1800	**Registration** Hong Kong - Level 2
1830-2000	**Registration (During Reception)** Spa/Pool Level - Conrad Terrace Pool
1500-1600	**2013 Session Chairs Meeting** Willow I - Level 3
1830-1900	**Newbie Reception w/ FIRST Steering Committee & Membership Committee** Spa/Pool Level - Conrad Terrace Pool FIRST Newbies (non-members) & First Time Attendees (members and non-members) are cordially invited to mix and mingle with each other and the FIRST Steering Committee & Member Committee. Beverages and appetizers will be served - find all the unique food & beverage stations spread out alongside the pool and walking paths!
1900-2100	**Ice Breaker Reception sponsored by Solera Networks** Spa/Pool Level - Conrad Terrace Pool All attendees are encouraged to attend this kick-off networking event.

Monday, 17 June 2013

0730-1700	**Registration** Hong Kong - Level 2
0730-0900	**CVSS v3 Special Interest Group (SIG) - *click here for details*.** London 1 - Level 1 | Invite-only
0730-0830	**Morning Coffee & Tea Service** Prefunction - Level 4 Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.
0830-0900	***Conference Opening & Welcome Remarks*** Grand Ballroom - Level 4

NETWORK

QUESTIONS?

Do you have specific questions? Please send inquiries to first-2013@first.org.

Direct line to conference office:
+1 312 646 1013

Direct mailing address to conference office:
FIRST Conference Office
219 W. Chicago Avenue, Suite 300
Chicago, Illinois 60654

CONNECT WITH US

FIRST News!

FIRST Podcasts!

	Chris Gibson Chair, FIRST.Org Director, Citi, UK		
0900-0930	***Opening Remarks by Her Excellency Ms. Yingluck Shinawatra Prime Minister of the Kingdom of Thailand*** Grand Ballroom - Level 4 **Ms. Yingluck Shinawatra** Prime Minister, Kingdom of Thailand		
0930-1030	**Keynote Presentation: INTERPOL Global Complex for Innovation--Facilitating international police cooperation to combat cybercrime** Grand Ballroom - Level 4 **James Pang** Assistant Director for Digital Crime Investigation Support, INTERPOL		
1030-1100	**Coffee & Networking Break** Prefunction - Level 4		
1100-1200	**Plenary: Big Data, Big Breaches, Big Headaches [+]** Grand Ballroom - Level 4 **Scott McIntyre** Senior Technology Architecture Specialist, Telstra, AU		
1200-1330	**Lunch (2 locations)** Cafe @2 - Level 2 Kisara Restaurant - Level 3		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
1335-1420	**Chasing the Fox: A closer look at an APT malware [+]** **Andreas Schuster** Deutsche Telekom AG	**The CERT Assessment Tool: Increasing a Security Incident Responder's Ability to Assess Risk [+]** **Anne Connell** **Todd Waits** CERT/CC - SEI CMU, US	**Cyber-EXE Poland 2012. How to organize the cyber exercises on a national level. [+]** **Miroslaw Maj** Cybersecurity Foundation / ComCERT,PL
1425-1510	**Proactive Forensics of Web Application Attacks—A Step by Step Guide [+]** **Shlomi Ben-Hur** **Shay Chen** Hacktics ASC, Ernst & Young, LLP, IL	**Industrial Owner's Manual: Case studies in publicly accessible ICS [+]** **Eireann Leverett** IOActive, UK	**Global Disaster Recovery Panel: [+]** **Moderator:** **Takayuki Uchiyama** JPCERT/CC, JP **Panelists:** **Mark Graff** NASDAQ, US **Damir Rajnovic** Panasonic Europe **GP. CAPT. Surapol Navamavadhana** Advisor to the Minister of Information and Communication Technology, TH **Itaru Kamiya** NTT-CERT, JP
1515-1545	**Coffee & Networking Break** Prefunction - Level 4 Prefunction - Level 2		
1550-1635	**Breaking the Bank: An Analysis of the 2012-2013 'Triple Crown' DDoS Financial Industry DDoS Attacks [+]** **Roland Dobbins** Arbor Networks	**Flying Under the Radar: Custom Exploit Kits [+]** **Nancy Strutt** Verisign, US	**Using Threat Intelligence and Incident Response in Modern Malware Warfare [+]** **Kyle Wilhoit** Trend Micro, US
1640-1725	**Mining Billion Nodes Malicious Network Behavior in Practice—Chinese Taipei Perspective [+]** **Ching-Hao Mao** Institute for Information Industry, TPE	**Secure Windows—Mitigating Windows Vulnerabilities to deter APTs [+]** **David Jones** **Gavin Reid** Cisco Systems, US	**Reaching Common Ground: Information Sharing & the Fight Against Cybercrime [+]** **Andrea Dufkova** **Jo De Muynck** ENISA
1730-1830	**Lightning Talks - Day 1** Grand Ballroom - Level 4 Sign-up is located at the registration desk. First-come-first-served!		

Tuesday, 18 June 2013

0730-1700	**Registration** Hong Kong - Level 2		
0730-0900	**CVSS v3 Special Interest Group (SIG) - *click here for details*.** London 1 - Level 1		
0800-0900	**Morning Coffee & Tea Service** Prefunction - Level 4 Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.		
0900-0930	***Opening Remarks*** Grand Ballroom - Level 4 **Chris Gibson** Chair, FIRST.Org Director, Citi, UK		
0930-1030	**Keynote: Economic Products and By-products of Open, Shared, Real Time Sinkholes--Lessons From GhostClick and Conficker [+]** Grand Ballroom - Level 4 **Dr. Paul Vixie** Chairman and Founder, Internet Systems Consortium (ISC), US		
1030-1100	**Coffee & Networking Break** Prefunction - Level 4		
1100-1200	**FIRST Session: FIRST Financials Review** Grand Ballroom - Level 4 **Peter Allor** CFO, FIRST.Org		
1200-1330	**Lunch (2 locations)** Cafe @2 - Level 2 Diplomat Bar - Lobby Level		
1230-1420	**VRDX Special Interest Group (SIG)** London 1 - Level 1		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
1335-1420	**Virut Botnet Takedown [+]** **Przemek Jaroszewski** CERT Polska/NASK, PL	**Tracing Botnet in Chinese Taipei [+]** **Kai-Chi Chang** Institute for Information Industry, TPE	**Declared Level of Response as a Voluntary CERT Community Cooperation Model in Incident Handling [+]** **Krzysztof Silicki** NASK, PL
1425-1510	**BlackHole, the hidden stuff beyond the spotlight [+]** **Adnan Shukor** Blue Coat Systems, US	**Lessons Learned in Automating Threat Intelligence Sharing with Open IOC [+]** **Douglas Wilson** Mandiant, US	**CERT Certification - A certification scheme for CERTs/CSIRTs using the SIM3 maturity model [+]** **Antonio Liu** DFN-CERT Services GmbH, DE **Don Stikvoort** S-CURE bv, NL
1500-1700	**Net Infrastructure BoF (open)** London 1 - Level 1		
1515-1545	**Coffee & Networking Break** Prefunction - Level 4 Prefunction - Level 2		
1550-1635	**Nfsen + Hadoop [+]** **Vytautas Krakauskas** LITNET CERT, LT	**Combating Insider Threats and Targeted Attacks [+]** **Matt McKinley** Lancope, US	**Timeline of a 0-Day: Reducing Exposure Through Information Sharing [+]** **Alex Kirk** Sourcefire, US
1640-1725	**Analysis of DNS data from Chinese Telecom Operators [+]** **Chunyang Yuan** CNCERT/CC, CN	**Data Transformation for Normalization [+]** **Sebastian Tricaud** **Fred Wilmot** Splunk, US	**Enabling the Secure Exchange of Cyber Security Information [+]** **Kathleen Moriarty** EMC Corporation, US
1730-1800	**Lightning Talks - Day 2** Grand Ballroom 1&2 - Level 4 Sign-up is located at the registration desk. First-come-first-served!		
1730-1900	**CVSS v3 Training BoF (open)** London 1 - Level 1		

1800-2000	**Vendor Showcase** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4 An evening to network with our conference sponsors, exhibitors and your peers. Light snacks and beverages will be served. Don't forget to get your raffle cards stamped!

Wednesday, 19 June 2013

0800-1400	**Registration** Hong Kong - Level 2		
0800-0900	**CVSS v3 Conference Update** Grand Ballroom - Level 4 | Open to All Attendees **Seth Hanford** Cisco Systems, US		
0800-0900	**Morning Coffee & Tea Service** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4 Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
0900-0945	🇨🇭 **Detecting Malware infections through DNS live monitoring [+]** **Hector Ortiz** Swisscomm, CH	🇺🇸 **Winning the Game with the Right Playbook [+]** **Jeff Bollinger** **Brandon Enright** **Matthew Valites** Cisco Systems, US	🇳🇱 **When security incidents drive an incumbent ISP to change its security strategy 180 degrees [+]** **Martijn van der Heide** KPN-CERT, NL
0950-1035	🇺🇸 **Incubations: Cyber Espionage Operators and Their Tools [+]** **Brandon Dixon** Verisign, US	🇵🇱 🇪🇺 **A Pragmatic Approach to Gathering Threat Data Using Honeypots [+]** **Cosmin Ciobanu** ENISA **Przemek Jaroszewski** CERT Polska/NASK, PL	🇺🇸 **Implementing the Traffic Light Protocol at US-CERT: Minutes to Learn, a Lifetime to Master [+]** **Thomas Millar** US-CERT, US
1040-1140	**Re-writing the CSIRT Playbook BoF** London 1 - Level 1		
1040-1110	**Coffee & Networking Break with Exhibits** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		
1115-1205	🇺🇸 **Journeys Through Unallocated Space [+]** **Timothy Slaybaugh** General Dynamics - AIS, US	🇩🇰 **The Workings of the Shylock Gang [+]** **Peter Kruse** **Yuriy Khvyl** CSIS Security Group A/S	🇦🇺 **Building a Guerilla CSIRT Software Development Team [+]** **Chris Horsley** CSIRT Foundry, AU
1210-1330	**Lunch (2 locations)** Cafe @2 - Level 2 Liu Restaurant - Level 3		
1300-1600	**Vendor Special Interest Group (SIG) - *click here for details*.** London 1 - Level 1		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
1335-1420	🇵🇱 **Zeus Gameover - P2P Spyware at Work [+]** **Tomasz Bukowski** NASK/CERT Polska, PL	🇺🇸 **The Case for NetFlow for Law Enforcement [+]** **Richard Nolan** **Kristopher Rush** SEI, CERT/CC, US	🇺🇸 **Ten Years of Data Sharing for Mitigation - Lessons Learned and the Long Road Ahead [+]** **Rod Rasmussen** Internet Identity, US
1425-1510	🇺🇸 **Web Malware Outsmarting Security Products [+]** **Arseny Levin** **Rami Kogan** Trustwave, US	🇯🇵 **Cyber Security Trend in Japan [+]** **Kazuya Hiradate** **Naoshi Matsushita** NRI SecureTechnologies, JP	🇺🇸 **Bad Signs at Adobe: Code Signing Certificate Misuse and Lessons Learned [+]** **David Lenoe** **Lindsey Wegrzyn** Adobe, US
1510-1530	**Coffee & Networking Break** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		
1600-1630	**Buses to Conference Banquet - Meet in Conrad Main Lobby** Additional attendee directions will be provided onsite. **Please be on time!**		
1630-2200	**Conference Reception & Banquet Dinner** Location & event details will be anounced onsite!		

Thursday, 20 June 2013

0800-1600	**Registration** Hong Kong - Level 2		
0800-0900	**Morning Coffee & Tea Service** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4 Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
0900-0945	**Conducting Technical Incident Investigations on Apple iOS Devices [+]** **Kenneth van Wyk** KRvW Associates, LLC, US	**The Korean Intrusion Spree [+]** **Snorre Fagerland** Norman AS, NO	**Vulnerability Handling Processes: When Hackers Come A-Knockin [+]** **Katie Moussouris** Microsoft, US
0950-1035	***Conducting Technical Incident Investigations on Apple iOS Devices Continued***	**Monitoring DDoS Botnets in the Wild to Understand Behavior and Collect Intel [+]** **Shahan Sudusinghe** Verisign, US	**Best Practices for Coordinating Response and Information Sharing: Finding Them Out, Writing Them [+]** **Timothy Grance** NIST, US **Tim Mather** Splunk, US **Thomas Millar** US-CERT, US
1040-1110	**Coffee & Networking Break with Exhibits** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		
1115-1205	**A Sampling of Internetwork Security Issues Involving IPv6 [+]** **John Kristoff** Team Cymru, US	**Internet Routing Security [+]** **Arturo Servin** LACNIC, UY	**Expanding CSIRT Activity: How we implement application security into subsidiaries [+]** **Yusuke Gunji** Rakuten, Inc, JP
1210-1330	**Lunch (2 locations)** Cafe @2 - Level 2 Kisara Restaurant - Level 3		
1230-1420	**VRDX Special Interest Group (SIG)** London 1 - Level 1		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
1335-1420	**Malware Analysis Case Study [+]** **Yuji Kubo** **Teiichi Torikai** National Police Agency, JP	**Dynamic Analysis vs Next Generation Malware [+]** **Fatih Haltas** Center for Interdisciplinary Studies in Security and Privacy New York University Abu Dhabi, TR	**Cyber Security Strategy @ EU [+]** **Francisco García Morán** European Commission
1425-1510	**Intelligent Defence: deriving malicious intent using domain registrar information [+]** **Michael Jordon** Context, UK	**The Mayans were right! A new age of data breaches [+]** **Carsten Eiram** Risk Based Security, US **Jake Kouns** Open Security Foundation, US	**Findings About Massive Cyber Attack Emergence Mechanisms in Japan [+]** **Mariko Miya** Cyber Defense Institute, JP
1515-1600	**Coffee & Networking Break with Exhibits - Non-Members Break** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		
15:30-17:30	**Annual General Meeting (AGM)** Grand Ballroom 1&2 - Level 4 **AGM Registration will be located outside of the doors.** Members-only meeting. Please be on time and have a valid government issued photo ID for entry into meeting room. No exception. Coffee break for members will be served in the meeting room.		

Friday, 21 June 2013

0800-1400	**Registration** Hong Kong - Level 2
0800-0900	**Morning Coffee & Tea Service**

	Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4 Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.		
0830-0900	***Opening Remarks*** Grand Ballroom - Level 4 **Chris Gibson** Chair, FIRST.Org Director, Citi, UK		
BREAKOUTS	**DEEP TECHNICAL DIVES** **Grand Ballroom 1&2 - Level 4**	**TECHNICAL FOUNDATIONS** **New York Ballroom - Level 2**	**POLICY & MANAGEMENT** **Beverly Hills Ballroom - Level 2**
0900-0945	**Memory Analysis Update - Volatility v2.3 [+]** **Andreas Schuster** Deutsche Telekom, AG	**Sharing by Wim [+]** **Willem Biemolt** SURFnet/SURFcert, NL	**A Glimpse Into the Future: The Evolution of Cybercrime in the Next Decade [+]** **Ziv Mador** Trustwave, US
0950-1035	***Memory Analysis Update***	**WARDEN: realtime sharing of detected threats between CSIRT teams [+]** **Pavel Kácha** CESNET, CZ	**The Art of Cyber Warfare [+]** **Michael Lotas** General Dynamics Fidelis Cybersecurity Solutions, US
1040-1110	**Coffee & Networking Break with Exhibits** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		
1115-1205	***Memory Analysis Update***	**Improving Cybersecurity Capabilities of Critical Infrastructures - Findings in Assessing ICS[+]** **Lauri Korts-Pärn** **Masako Someya** Cyber Defense Institute, Inc., JP	**National CSIRT Community to Protect Key Strategic Resources and Critical Information Infrastructures [+]** **Bisyron Wahyudi** ID-SIRTII, ID
1210-1330	**Lunch (2 locations)** Cafe @2 - Level 2 Diplomat Bar - Lobby Level		
1335-1400	**Closing Remarks, Security Challenge Winners & Raffles** Grand Ballroom 1&2 - Level 4		
1300-1700	**Metrics Special Interest Group (SIG) - *click here for details*.** London 1 - Level 1		
1400-1430	**Closing Coffee & Networking Break** Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4		

Press Policy | **Network Privacy Statement & Conference Monitoring** | **FIRST Board of Directors** | **Contact the FIRST Secretariat**

Site powered by CAPS, LLC