2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

Tuesday, October 18, 2016 - AM	
7:00 - 9:00 AM	Registration & Breakfast
9:00 - 9:15 AM	Welcome Remarks - Dr. Fernando Colon Osorio, General Program Chair
9:15 - 10:15 AM	**Keynote -** Dmitri Vitaliev, Director at Equalit.ie and Information Technology and Services Consultant Biography: Dmitri is the founder and director of eQualit.ie with over a decade of experience working on digital security and privacy technology within the human rights and independent media sector. He has led and participated in missions to over 40 countries, and is a recognized expert on technology training and organizational security. He is the author of the Digital Security and Privacy for Human Rights Defenders manual and was a founding member and coordinator of the NGO-in-a-Box Security Edition project. He has helped to create worldwide networks of trainers, developed curricula for various security programs and is also a regular contributor to technology publications. But his real job is bringing up two kids and trying to be more at home. Topic: Privacy, Security and the Future of Our Society
10:15 - 10:30 AM	Break
10:30 - 12:30 PM: **Session # 1:** Emerging threats and Malware classification Session Chair: Dr. Colon Osorio	1570293834: Malware Provenance - Code Reuse Detection in Malicious Software at Scale by Jason Upchurch, United States Air Force Academy & University of Colorado at Colorado Springs, USA; Xiaobo Zhou. University of Colorado at Colorado Springs, USA 1570297790: Reverse Engineering with Bioinformatics Algorithms Over a Sound Android Covert Channel by Sergio Vargas and Eleazar Aguirre, Instituto Politécnico Nacional Centro de Investigación en Computación, Mejico 1570297288: Dissecting Developer Policy Violating Apps: Characterization and Detection by Su Mon Kywe and Yingjiu Li, Singapore Management University, Singapore; Jason Hong, Carnegie Mellon University, USA; Yao Cheng, Singapore Management University, Singapore 1570297243: Impact of Base Transceiver Station Selection Mechanisms on a Mobile Botnet Over a LTE Network Asem Kitana and Issa Traore, University of Victoria, Canada; Isaac Woungang, Ryerson University, Canada .
12:30 - 01:30 PM	Lunch

2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

Tuesday, October 18, 2016 - PM

01:30 - 03:00 **Panel** Moderator: Randy J. Jordan, FBI	**Description:** It is universally agreed amongst "Security Professionals" that the most significant weakest links in the cyber security chain are: 1. System complexity - if Windows XP is estimated to have 40 Million lines of code, and Windows 10 even a higher number, then, a. the ability to proof the correctness of the code is NOT possible, and b. the number of defects present in most modern systems increases with the increased complexity of the system. Said complexity leads to incremental defects, and therefore, increased vulnerabilities that can be exploited. Bottom line is that increase functionality results in higher security risks; and 2. Humans. In the past a lot of emphasis has been applied to item # 1. However, often the efforts to deal with vulnerable humans is less defined, with limited number of tools available to address the problem. This difficulty, and the corresponding tension between Privacy and Security is a critical issue that must be addressed. The panelist will have an opportunity to discuss the limits that must be present when organizations infringe on its members privacy.
03:00 - 03:15	Break
03:15 - 05:30 PM **Session 2 -** Broad Spectrum Malware, Defense Strategies & Mechanisms Session Chair: Dr. Anthony Arrott	1570294110: Reconstructing packed binaries with dynamic binary instrumentation by David Korczynski, University of Oxford, United Kingdom 1570289540: CARDINAL - Similarity Analysis to Defeat Malware Compiler Variations by Luke T Jones, United States Air Force Academy & Chthonian Cyber Services, USA; Andrew Sellers, US Air Force Academy, USA; Martin Carlisle, Carnegie Mellon University, USA 1570289001: Automatic Extraction of Malicious Behaviors by Khanh-Huu-The Dam, IRIF, University Paris Diderot and Tayssir Touili, CNRS and University Paris 13, France

2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

Tuesday, October 18, 2016 - Evening Program

05:30 -07:30 PM	Free Time
07:30 - 08:00 PM	Cocktail Reception
08:00 - 10:30 PM	"Best Paper" Award Gala Dinner

Wednesday, October 19, 2016 - AM

7:00 - 8:00 AM	Registration & Breakfast
8:00 - 10:15 AM **Session 3 -** Mobile Malware, Detection & Thwarting Session Chair: Prof Arun Lakhotia	1570297970: SigPID - Significant Permission Identification for Android Malware Detection by Lichao Sun, Zhiqiang Li, Qiben Yan, Witawas Srisa-an and Yu Pan, University of Nebraska, Lincoln, USA 1570300232: Native Malware Detection in Smartphones with Android OS Using Static Analysis, Feature Selection and Ensemble Classifiers by Salvador Morales-Ortega, P.J. Escamilla-Ambrosio, A. Rodríguez-Mota and L.D. Coronado-De-Alba, Instituto Politécnico Nacional, Centro de Investigación en Computación. Mejico 1570293916: On the Effectiveness of Application Characteristics in the Automatic Classification of Malware on Smartphones by Matthew Ping and Spiros Mancoridis, Drexel University, USA
10:15 - 10:30 AM	Break
10:30 - 12:30 **Session 4 -** Offense, Defense, and Malware Provenance Session Chair: Fernando Colon Osorio	1570297589: On Periodic Behavior of Malware - Experiments, Opportunities and Challenges by Anh Huynh, Wee-Keong Ng and Hoang Giang Do, Nanyang Technological University, Singapore 1570289049: A covert data transport protocol by Yu Fu, Jia Zhe, Lu Yu and Richard Ree Brooks, Clemson University, USA 1570293834: Malware Provenance - Code Reuse Detection in Malicious Software at Scale by Jason Upchurch, United States Air Force Academy & University of Colorado at Colorado Springs, USA; Xiaobo Zhou. University of Colorado at Colorado Springs, USA
12:30 - 01:30 PM	LUNCH
Session 5 - Malware: The emergence of New Threats, and the analysis of old friends 01:30 - 03:00 PM: Session Chair: Richard F. Brooks	1570297595: ZoneDroid: Control Your Droid Through Application Zoning by Md Shahrear Iqbal, Queen's University & Bangladesh University of Engineering and Technology, Canada; Mohammad Zulkernine, Queen's University, Canada 1570297781: Advanced Transcriptase for JavaScript Malware by Fabio Di Troia and Visaggio Corrado, Universita degli Studi del Sannio, Italy; Thomas Austin and Mark Stamp, San Jose State University, USA 1570304504: Anti-Analysis Trends in Banking Malware by Paul Black and Joseph Opacki, PhishLabs, USA

2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

03:00 - 03:15 PM	Break
03:15 - 05:30 PM **Session 6** -Mechanisms & Strategies to Detect Mobile Malware Session Chair: Fernando Colon Osorio	1570294080: DySign: Dynamic Fingerprinting for the Automatic Detection of Android Malware by ElMouatez Billah Karbab, Mourad Debbabi, and Saed Alrabaee, Concordia University, Canada; Djedjiga Mouheb, University of Sharjah, United Arab Emirates (UAE) 1570299944: Signature Limits: An Entire Map of Clone Features and Their Discovery in Nearly Linear Time by William Casey, Carniege M ellon University and William Casey and Aaron Shelmire, Anomali, USA 1570297648: Function Identification and Recovery Signature Tool by Angel Villegas, Cisco Systems, Inc., USA
04:30 - 05:00	Concluding Remarks - Dr. Fernando Colon Osorio, General Program Chair

Thursday, October 20, 2016 - ALL DAY	
	Option # 1: Capture teh Flag Contest
07:00 - 08:00 AM	Registration & Breakfast
0 8:00 - 08:15 AM	Welcome Remarks - Dr. Fernando Colon Osorio, General Program Chair
08:15 - 12:15 PM **Penetration Testing Tutorial & Capture The Flag Contest**	Session A: Penetration Testing Tutorial - Assessing Your Overall Security Before the Attackers do. What is Pen-Testing? Why Perform Pen-Testing? Pen-Testing Tools And Reporting Analysis Of CORE IMPACT Metasploit Framework 3.0
12:15 - 01:15	Lunch

2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

01:15 pm to 05:00 pm Session Chair: Dr. Jose A. Morales	**2nd Annual Capture The Flag Contest as part of the** **First Price (Must capture all 5 flags)** — **$2,000.00 USD** **2nd Price** — **Certificate 2nd Place plus $ 150.00** **3rd Price** — **Certificate 3rd Place plus $ 75.00** **Winners will be announced and prizes awarded at the end of the MALCON 2016 Conference.** **All participants in the conference are welcomed to form a team.** **For Further Information contact:** Dr. Jose A. Morales, CFT Organizer and/or Mr. Dan Klinedinst, CTF Organizer To Register, click here
12:30 - 01:30 PM	LUNCH

2016 MALCON

KNOW YOUR ENEMY ◆ Broad Spectrum Malware ◆ ATP

IEEE computer society

October 18-21

Thursday, October 20, 2016 - ALL DAY

Culebra Getaway Networking Event - *Beach and Snorkel Tour & Day Trip*

0 9:00 - 03:45 PM

- Check in time: 9:00am

Includes:

- Lunch buffet with options for all
- Beverages, including rum drinks
- Quality snorkeling equipment for all ages
- Floating devices
- Swim platforms where our guest have easy access to the water
- Snorkeling instruction for our beginners

Cost: $ 125.00 pp

Upon departing marina Puerto Del Rey, we head straight out to Culebra along the Cordillera Islands. After about 45 minutes on our high-speed catamaran we arrive at one of Culebra's beautiful reefs and anchor for about an hour and a half of snorkeling. Depending on water condition our captains may take you to: Luis Pena, Carlos Rosario, or Melones

We then move on to our beach stop, Culebrita, Playa Tortuga or another beautiful beach that will be the best to enjoy the rest of the afternoon. At either location you can swim into the beach or do some more snorkeling. We depart Culebra around 3:00 pm, returning to the marina between 3:45- 4:00pm.

Lunch is served at approximately 11:45-12:00pm, where our guests can enjoy local pastries; build your own sandwiches with fresh baked bread, fresh fruit, our signature pasta salad, chicken salad, coleslaw and cookies.

Important: Be advised that this Snorkeling beach Trip travels by high speed boat in open waters and may not be appropriate for pregnant women, those with recent surgeries, back injuries and children under 3 yrs of age.

If you tend to get seasick, we remind you that you should take an over-the-counter remedy with food at least 1 hour before the voyage.

To register and reserve your spot, click here. Seats are limited !!!!!!