

2013 8th International Conference on Malicious and Unwanted Software: The Americas

(MALWARE 2013)

**Fajardo, Rwigyira, USA
22-24 October 2013**



**IEEE Catalog Number: CFP1359F-POD
ISBN: 978-1-4799-2536-0**

Technical Papers

Session – 1	Emerging Threats and Malware Classification
Date/Time	October 22, 2013 / 10:30 – 12:30 PM
Chair	Dr. Colón Osorio

- 🔴 **Noninvasive Detection of Anti-Forensic Malware**³
Mordehai Guri, Gabi Kedma, Tom Sela, Buky Carmeli, Amit Rosner and Yuval Elovici
- 🔴 **Heuristic Malware Detection via Basic Block Comparison**³³
Francis Adkins, Luke Jones, Martin Carlisle and Jason Upchurch
- 🔴 **Dynamic Classification of Packing Algorithms for Inspecting Executables using Entropy Analysis**³;
Munkhbayar Bat-Erdene, Taebeom Kim, Hongzhe Li and Heejo Lee

Session – 2	The Measurement Problem
Date/Time	October 22, 2013 / 03:15 – 05:30 PM
Chair	Dr. Fernando C. Colon Osorio

- 🔴 **Measuring the Effectiveness of Modern Security Products to Detect and contain Emerging Threats - A Consensus-based Approach**⁴⁹
Fernando C. Colón Osorio, Ferenc Leitold, Dorottya Mike, Chris Pickard, Sveta Miladinov and Anthony Arrott
- 🔴 **Use-Case-Specific Metrics for Comparative Testing of Endpoint Security Products**⁵⁷
Jeffrey Wu and Anthony Arrott




Invited Paper: Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors⁶³

Session – 3	Mobile Malware
Date/Time	October 23, 2013 / 10:15 – 12:15 PM
Chair	Dennis Batchelder, Microsoft

- 🔴 **It's you on photo?: Automatic Detection of Twitter Accounts Infected With the Blackhole Exploit Kit**⁷³
Joshua S. White and Jeanna N. Matthews
- 🔴 **PANDORA Applies Non-Deterministic Obfuscation Randomly to Android**⁷;
Mykola Protsenko and Tilo Müller
- 🔴 **First Byte: Force-Based Clustering of Filtered Block N-Grams to Detect Code Reuse in Malicious Software**⁸;
Jason Upchurch and Xiaobo Zhou
- 🔴 **An Antivirus API for Android Malware Recognition**⁹⁹
Rafael Fedler, Marcel Kulicke and Julian Schütte

Session – 4	Cloud Computing Malware & Defenses
--------------------	---

Date/Time	October 23, 2013 / 01:15 - 02:45 PM
Chair	Dr. Anthony Arrott

- 
Countering Malware Evolution Using Cloud-Based Learning''''''7
Jacob Ouellett, Avi Pfeffer and Arun Lakhotia
- 
REcompile: A Decompilation Framework for Static Analysis of Binaries''''''7
Khaled Yakdan, Sebastian Eschweiler and Elmar Gerhards-Padilla
- 
Circumventing Keyloggers and Screendumps''''''325
Karan Sapra, Benafsh Husain, Richard Brooks and Melissa Smith

Session – 5	Botnets, Targeted Advances Persistent Threats
Date/Time	October 23, 2013 / 03:00 – 05:20 PM
Chair	Dr. Anthony Arrott

- 
Analysis and Diversion of Duqu’s Driver''''''32; "
Guillaume Bonfante, Jean-Yves Marion, Fabrice Sabatier and Aurélien Thierry
- 
Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus''''''338''
Dennis Andriess, Christian Rossow, Brett Stone-Gross, Daniel Plohmann and Herbert Bos
- 
A Simple Client-Side Defense Against Environment-Dependent Web-Based Malware''''''346
Gen Lu, Karan Chadha and Saumya Debray
- 
Static Malware Detection with Segmented Sandboxing''''''354''
Hongyuan Qiu and Fernando C. Colón Osorio