

# **2014 9th International Conference on Malicious and Unwanted Software: The Americas**

**(MALWARE 2014)**

**Fajardo, Puerto Rico, USA  
28 – 30 October 2014**



**IEEE Catalog Number: CFP1459F-POD  
ISBN: 978-1-4799-7330-9**

|                    |  |
|--------------------|--|
| <b>Session – 1</b> | <b>Emerging threats and Malware classification</b> |
| <b>Date/Time</b>   | October 28, 2014 / 10.30 – 12.30 PM                |
| <b>Chair</b>       | <b>Dr. Colon Osorio</b>                            |

 **Identifying Malware Genera using the Jensen-Shannon Distance between System Call Traces** 1

*Jeremy D. Seideman, Bilal Khan and Antonio Cesar Vargas*

 **Host-Based Code Injection Attacks: A Popular Technique used by Malware** 8

*Thomas Barabosch and Elmar Gerhards-Padilla*

 **Automatic Construction of Printable Return-Oriented Programming Payload** 18

*Wenbiao Ding, Xiao Xingy, Ping Chenz, Zhi Xinx and Bing Mao*


|                    |                                     |
|--------------------|-------------------------------------|
| <b>Session – 2</b> | <b>The Measurement Problem</b>      |
| <b>Date/Time</b>   | October 28, 2014 / 03:15 – 06:00 PM |
| <b>Chair</b>       | <b>Dr. Anthony Arrott</b>           |

 **Protection Against Remote Code Execution Exploits of Popular Applications in Windows** 26

*Jeffrey Wu, Anthony Arrott and Fernando C. Colón Osorio*

 **Global and Local Prevalence Weighting of Missed Attack sample Impacts for Endpoint Security Product Comparative Detection Testing** 32

*Andreas Clementi, Peter Stelzhammer and Fernando C. Colón Osorio*

- 
**Combining Commercial Consensus and Community Crowd-Sourced Categorization of Web Sites for Integrity Against Phishing and other Web Fraud** 40

*Ferenc Leitold, Anthony Arrott and Fernando C. Colón Osorio*

|                    |  |
|--------------------|--|
| <b>Session – 3</b> | <b>Mobile Malware</b>                  |
| <b>Date/Time</b>   | October 29, 2014 / 10:00 AM – 12:30 PM |
| <b>Chair</b>       | <b>Dennis Batchelder, Microsoft</b>    |

- 
**MysteryChecker: Unpredictable Attestation to Detect Repackaged Malicious Applications in Android** 50

*Jihwan Jeong, Dongwon Seo, Chanyoung Lee, Jonghoon Kwon , Heejo Lee and John Milburn*

- 
**AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies** 58

*Mordechai Guri, Gabi Kedma, Assaf Kachlon and Yuval Elovici*

- 
**CrowdSource: Automated Inference of High Level Malware Functionality from Low-Level Symbols Using a Crowd Trained Machine Learning Model** 68

*Joshua Saxe, Rafael Turner and Kristina Blokhin*

|                    |  |
|--------------------|--|
| <b>Session – 4</b> | <b>Botnets &amp; Other Musings</b>     |
| <b>Date/Time</b>   | October 28, 2014 / 01.30 PM – 02.45 PM |
| <b>Chair</b>       | <b>Neil Rubenking</b>                  |

- 
**BoTGen: A New Approach for In-Lab Generation of Botnet Datasets** 76

*Muhammad H. ElSheikh, Mohammed S. Gadelrab, Mahmoud A. Ghoneim and Mohsen Rashwan*

- ❸
**PsyBoG: Power Spectral Density Analysis for Detecting Botnet Groups**    85  
*Jonghoon Kwon, Jeongsik Kim, Jehyun Lee, Heejo Lee and Adrian Perrig*
  
- ❸
**Fighting Banking Botnets by Exploiting Inherent Command and Control Vulnerabilities**    93  
*Lanier Watkins ,Christina Kawka, Cherita Corbett and William H. Robinson*
  
- ❸
**Bacterial Quorum Sensing for Coordination of Targeted Malware**    101  
*Mark E. Fioravanti II and Richard Ford*

|                    |   |
|--------------------|---|
| <b>Session – 5</b> | <b>HoneyAgents, Intelligent Defenses, and other Anti-Malware techniques</b> |
| <b>Date/Time</b>   | October 28, 2014 / 03:00 PM – 05:00 PM                                      |
| <b>Chair</b>       | <b>Dr. Anthony Arrott</b>   |

- ❸
**HoneyAgent: Detecting Malicious Java Applets by using Dynamic Analysis**    109  
*Jan Gassen and Jonathan P. Chapman*
  
- ❸
**Codescanner: Detecting (Hidden) x86/x64 Code in Arbitrary Files.**    118  
*Viviane Zwanger, Elmar Gerhards-Padilla and Michael Meier*
  
- ❸
**Risk prediction of Malware victimization based on user behavior**    128  
*Fanny Lalonde Lévesque, José M. Fernandez and Anil Somayaji*
  
- ❸
**Agent-based Trace Learning in a Recommendation-Verification System for Cybersecurity**    135  
*William Casey, Evan Wright, Jose Andre Morales, Michael Appel, Jeff Gennari and Bud Mishra*