MALWARE 2013 - THE AMERICAS

KNOW YOUR ENEMY

Research • Practical Solutions (Industry Track) • The Law

8th IEEE International Conference on Malicious and Unwanted Software "The Americas"

Call for Papers

Theme: "Malware in the Era of Cloud Services and Mobile Endpoints"

Submission of papers	
Research Track	NOW CLOSED
Industry Track	August 12th, 2013, 23:59:59 EST
Short Paper Track	August 12th, 2013, 23:59:59 EST
Notification of Acceptance	August 18th, 2013, 23:59:59 EST
Camera ready paper:	September 14th, 2013: 23:59:59 EST
Conference dates	October 22-24, 2013

The **8th IEEE International Conference on Malicious and Unwanted Software "The Americas" (Malware 2013 The Americas) will be held at El Conquistador Hotel & Resort, Fajardo, Puerto Rico, USA**, **October 22-24, 2013.** This year's conference has adopted as its main theme "Malware in the Era of Cloud Services and Mobile Endpoints" in recognition of a major paradigm shift that has transformed the computer industry as a whole, and created major challenges to the Security Community in particular.

Fundamentally, Over the last 12 years three important dates have marked the beginnings of a major paradigm shift in computing and the security models applied to protect an emerging computing environment - March 1999, January 9th, 2007, and July 2007. These dates roughly correspond to the birth of SalesForce.com, the most successful Software as a Service (SaS) provider to date, Steve Jobs introduction of the Iphone,, and the discovery of the Zeus Botnet. These innovations have been instrumental in enabling a paradigm shift in computing, away from a corporate network centric model with Windows end-point devices to what we called the Circa 2020 Computing Model. In the circa 2020 Computing model applications and data reside in the Cloud, the concept of an extended Trust Domain (network) disappears - there are no barriers to protect when your data and applications reside with your vendors, and the end-point device is a SmartPhone owned and operated by your employees- Bring Your Own Device (BYOD).

Three major research trends have emerged within this context. First, at the end of the chain, the end-point device is a mobile BYOD with security and mobility properties never anticipated. If the end-point device is own and operated by the employee of a large corporation, and the boundaries between "personal" and "Corporate" data, as well as applications disappears, then what is the protection model that can be used? Is the device to be "trusted", Un-Trusted, or simply operates in different modes of protection, one when interacting in a corporate environment, and one when being used strictly as a personal device?

Second, the existence of either a physical or a logical "Trusted Domain" that resides and operates within the confines of a single corporate entity has disappeared. Within this context, we encourage the submission of manuscripts exploring new models of protection that do not depend on ownership or management of a Corporate Trusted Domain, and incorporate elements whereas part of the data, applications, and infrastructure are managed by third parties such as SalesForce.com or Amazon Cloud Services.

Finally, the protection model and measures to be applied within the context of the new computing/protection paradigm is an important challenge. Do we protect the data?, the applications?, and how do we measure protection? In this last area, we clearly understand that measuring how many infected files are detected by an Anti-Malware product is a very limiting and not very practical measure. We encourage authors to propose innovative solutions to this problem, and the set of associate metrics to be used. We encourage authors to submit manuscripts that addresses issues in each one of these new research directions.

Submissions are solicited in, but not limited to, the following areas:

- Theoretical aspects and new directions in Malware related research, specifically, manuscripts that explore the concepts of "Trust Domains" that do not have or desire physical boundaries
- Smartphone Malware, protecting a new class of end-points with hyper-mobility
- Analysis and measurements of real malware incidents
- Worms, viruses and other propagating Malware
- Spyware, keystroke loggers, information theft Malware
- Honeypots and other sample collection methodologies
- Botnet attacks, detection/tracking and defense
- Malware economics and black market studies
- Code reverse engineering tools and practices
- Malware performance, analysis and capture tools
- Anti-spam and anti-phishing techniques and practices
- Legal aspects of unwanted software use
- Malware and its impact in social networking and cloud computing
- Rootkit and virtualization techniques
- Malware in wireless mobile devices

MALWARE 2013 - THE AMERICAS

KNOW YOUR ENEMY

Research • Practical Solutions (Industry Track) • The Law

Publication

The proceedings of the conference will be published in printed, and DVD, form and will be included in the IEEE Xplore digital library. In addition, the Conference's Technical Program Committee will select one manuscript as a recipient of the "Best Paper Award". The Best Paper Award author, together with the authors of a few selected manuscripts from the conference, will be invited to submit an extended version to a special issue of the Journal of Computer Security.

Paper Submission Information

Papers should be submitted through EDAS system at:
http://www.edas.info/
Submitted manuscripts must be 10-point font size, and should not exceed 8 single-spaced pages in length, including the abstract, figures, and references. Authors whose manuscript exceeds the 8 page limit may be allowed to include two additional pages for an extra charge. However, under no circumstances shall a submitted manuscript exceed the 10 page limit. Submitted papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings.

Additional Information

For more information on Malware 2013 or if you are interested in contributing to the organization of the conference please contact Dr. Fernando C. Colon Osorio, General Program Chair, Malware 2013 at fcco@brandeis.edu or visit our web site www.malwareconference.org. For information concerning submission of an original manuscript to the conference, please contact the Technical Program Committee Chairs (TPC), Dr. Anthony Arrott, Trends Micro, USA - mailto:mAnthony_Arrott@trendmicro.com, and Prof. Arun Lakhoita, Director of CajunBot Lab, University of Louisiana at Lafayette - mailto:arun@louisiana.edu.

Malware 2013 Program Committee

General Program Chair:

- Dr. Fernando C. Colon Osorio, WSSRL and Brandeis University, USA

Technical Program Committee Co-Chairs:

- Dr. Anthony Arrott, Trend Micro, USA
- Prof. Arun Lakhoita, Director of CajunBot Lab, University of Louisiana at Lafayette

Technical Program Committee Members :

- Dr. Davidson Boccardo, Inmetro, Brazil
- Dr. Guillaume.Bonfante, LORIA, France
- Mr. Pierre-Marc Bureau, ESET, CANADA
- Dr. Andreas Clemente, Germany
- Dr. Seyit A. Camtepe, Technische Universität Berlin
- Prof. José M. Fernandez, Ecole Polytechnique de Montréal, Canada
- Mr. Richard Ford, Pyratech Security Systems, Inc, USA
- Dr. Olivier Festor, INRIA Nancy Grand-Est, France
- Mr. Brian Hay, Security Works, USA
- Prof. Xuxian Jiang, North Carolina State University, USA
- Mr. Bill McGee, Trend Mcro, USA
- Prof. Jean-Yves Marion, Nancy Université, France, TPC
- Mr. Rachit Mathur, McAfee, USA
- Dr. Jose Andres Morales, CERT - Carnegie Mellon University, USA
- Dr. Kara Nance, Security Works, USA
- Dr. Jose Nazario, Invincea, Inc, USA
- Prf. Mark Stamp - San Jose State University, USA
- Prof. Natalia Stakhanova, University of South Alabama
- Prof. Andrew Walenstein, Lafayette University, USA
- Mr. Jeff Williams, Microsoft, USA
- Prof. Cliff C. Zou (Changchun Zou), University Central Florida, USA

Malware 2013 Keynote, Panels & Tutorials :

- Mr. Neil Rubenking, President & CEO, AppNeta, Inc., USA
- Vic Phatak - NSS Labs

Local Conference Chair

- Prof. Jose Ortiz, Computer Science, Universidad de Puerto Rico, USA