

# MALWARE CONFERENCE (MALCON) KNOW YOUR ENEMY

Research Track E Practical Solutions (Industry Track) The Law

# 12th IEEE International Conference on Malicious and Unwanted Software "MALCON 2017"

# **Call for Papers**

Theme: "It's about time law enforcement got as organized as organized crime"

Submission of papers	
Broad Spectrum Malware Track	July 7th, 2017, 23:59:59 EST
Industry Track	Aug 11th, 2017, 23:59:59 EST
Short Paper Track	Aug 11th,, 2017, 23:59:59 EST
Notification of Acceptance	September 1st, 2017, 23:59:59 EST
Camera ready paper:	September 8th, 2017: 23:59:59 EST
Conference dates	October 11-14, 2017

The 12th International Conference on Malicious and Unwanted Software (MALCON 2017) will be held at the Waldorf Astoria El Conquistador Resort, Fajardo, Puerto Rico, USA, October 11-14, 2017 (October 14, 2017 - optional). The Focus of the conference this year is twofold - (1) Evolving threat landscape, and (2) innovative system defense approaches. The topics are described in the paragraphs below.

# Evolving threat landscape

The Malware Criminal EcoSystem has become a vibrant sector of the dark economy in recent years. Innovation in this ecosystem is rampant at all levels - from the discovery of new vulnerabilities, to the introduction of new deployment mechanisms. This division of labor in the Malware Ecosystem has accelerated the deployment of new threats which often are deployed by multiple entities across platforms (often sloppily), but which certainly meet the business objectives. Current security approaches are often ineffective, since attackers quickly field test prototype attacks that dodge current defenses. The defenders reverse engineer the attacks, craft new defenses, which need to be tested to avoid harming the defender's clients. This cycle of new threats field tested, followed by the development of new defenses based on the new attacks represents an escalation that the defender industry cannot win. Therefore, the Anti-Malware industry

needs to evolve in at least two significant ways. First, the need for an Anti-Malware ecosystem, where researchers and companies collaborate instead of compete is needed. Second, the design and implementation of innovative Malware defenses must be based on knowledgeabout emerging threats gained through research. Within this context, the evolving threat landscape track is interested in exploring the current attacker's arsenal. Of particular interest are:

- Recent reverse engineering results of complex malware,
- Analysis of infection spread patterns,
- Advanced persistent threat (APT) designs,
- Botnet innovations, including domain name generation tools,
- Offensive use of BGP and DNS (along with defense innovations),
- Return oriented programming,
- Attacks with novel use of hardware/firmware,
- New forms of phishing,
- Online contraband networks,
- Malware use of darknet
- Identity theft,
- Malware obfuscation and encryption methods,
- Malicious network communications,
- Point-of-Sale malware
- Internet of Things and Mobile platforms, and
- Other innovations in this space.

#### Innovative system defense

While system defense requires technical innovations, we recognize that it depends equally on enterprise policies, after the fact forensics, and system monitoring. System defenders need to balance a number of conflicting factors:

- Users must be authenticated;
- Insider threats must be located; and
- Privacy must be safeguarded.

The enterprise depends on off-the-shelf products that are rarely secure. Sometimes security systems become attack vectors. Defense personnel are also forced to balance competing legal requirements.



# MALWARE CONFERENCE (MALCON) KNOW YOUR ENEMY

Research Track 🔳 Practical Solutions (Industry Track) 🔳 The Law

The defense track is soliciting papers with technical innovations, insights gained from practice, relevant legal expertise, and policy definitions. Topics of special interest include:

- Privacy preservation,
- Identity maintenance,
- Security policies,
- Online criminal enterprise identification/discovery,
- Advances in reverse engineering,
- Cloud security,
- Data forensics,
- Challenges of attribution in malware analysis
- Defense effectiveness evaluation methods
- Network monitoring, and
- Software defined network security.

#### Publication

The proceedings of the conference will be published in DVD form and 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:

#### https://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 2017 or if you are interested in contributing to the organization of the conference please contact Dr. Fernando C. Colon Osorio, General Program Chair, Malware 2017 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. Richard Brooks, Clemson University, USA - mailto:rrb@g.clemson.edu, and

- Dr. Alexander Volynkin, Computer Emergency Response Team <u>mailto:avolynkin@cert.org</u>.

#### Malware 2017 Program Committee General Program Chair:

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

#### **Technical Program Committee Co-Chairs:**

- Dr. Richard Brooks, Clemson University, and
- Dr. Alexander Volynkin, Computer Emergency Response Team, Carnegie Mellon University

#### **Technical Program Committee**

- Mr. Corrado Aaron Visaggio, University of Sannio, Italy
- Mr. Sebastien Bardin, CEA France, France
- Dr. Guillaume Bonfante, LORIA, France
- Dr. Seyit A. Camtepe, Technische Universität Berlin, Germany
- Dr, William Casey, CERT, Carnegie Mellon Univ., USA
- Dr. Andreas Clementi, AV Comparatives, Germany
- Prof. Arun Lakhotia, University of Louisiana at Lafayette, USA
- Dr. Ferenc Leitold, CheckVir Veszprog, Hungary
- George Kesidis, Penn State University, USA
- Prof. Spiros Mancoridis, Isaac L. Auerbach Cybersecurity Institute , Drexel University, USA
- Mr. Ivan Macalintal, Microsoft, USA
- Prof. Jean-Yves Marion, École des mines de Nancy, France
- Prof. Todd McDonald, Univ. of South Alabama, USA
- Dr. Jose Andres Morales, CERT, Carnegie Mellon Univ., USA
- Dr. Jose Ortiz-Ubarri, Universidad de Puerto Rico Rio Piedras Campus, USA
- Dr. Joshua Saxe, Invincea Labs, USA
- Dr. Aubrey-Derrick Schmidt, T-Systems Intnl, Germany
- Prof. Tony Skjellum, Auburn University, USA
- Prof. Natalia Stakhanova, Univ. New Brunswick, Canada
- Prof. Mark Stamp, Jose State University, USA
- Prof. Tayssir Toulli, Universite Paris 13, Paris, France



# MALWARE CONFERENCE (MALCON) KNOW YOUR ENEMY

Research Track 
Practical Solutions (Industry Track) 
The Law

- Mr. Jeff Williams, Dell SecureWorks, USA
- Ms. Sarah Zenou, Airbus, France
- Prof. Cliff C. Zou (Changchun Zou), Univ. Central Florida, USA
- Prof. Mohammad Zulkernine, School of Computing, Queen's University, Canada

## Malware 2017 Keynote, Panels & Tutorials:

• Dr. Jose A. Morales, CERT, Carniege Mellon University, USA

### Malware 2017 Local Program Chair

• Prof. Jose Ortiz, Universidad de Puerto Rico - Rio Piedras Campus, Puerto

### Malware 2017 Transportation & Accomodations

### Airlines<sup>1</sup>: - From the East Coast of the US:

Boston To SJU: JetBlue has three noon-stops a day ( 6:30 AM, 10:45 AM, and 11:55 PM, with a typical fare of \$ 432.00 round trip

NYC to SJU - JetBlue has 8 non-stop flights starting a 6:30 AM, with the last flight departing at 11:35 PM with a typical fare of \$ 356.00 round trip

Washington, DC to SJU - One daily flight non-stop with Jet Blue at 8 AM. Cost at about \$400 round trip.

Philadelphia to SJU - 3 Non-Stops a day with American Airlines, Cost at around \$420.00 round-trip

#### From the West Coast of the US:

San Francisco Area to SJU - Delta or American Airlines. Several 1-stop through NYC, Dallas or Miami. Cost around \$500.00 round trip.

## Hotel Transportation:

There are two Basic ways.

- 1. Namely using the hotel services at around \$85.00 round trip, or a
- private taxi (called "Publicos" in Puerto Rico) at around \$100 for 3-4 passengers.

1

Note: The fares quoted above are typical fares that can be found at Kayak.com and/or Travelocity.com.