MALWARE CONFERENCE (MALCON)

KNOW YOUR ENEMY

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

13th IEEE International Conference on Malicious and Unwanted Software "MALCON 2018"

Call for Papers

Theme: "In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters" – Jeff Jarmoc

"Any sufficiently advanced bug is indistinguishable from a feature" – Rich Kulawiec

Submission of papers	
Research Track (Abstract))	**July 17th, 2018, 23:59:59 EST**
Research Track Full Manuscript	July 17th, 2018, 23:59:59 EST
Industry Track	July 17th, 2018, 23:59:59 EST
Notification of Acceptance	August 20th, 2018, 23:59:59 EST
Camera ready paper:	September 7th, 2018: 23:59:59 EST
Conference dates	October 22-24, 2018

The 13th International Conference on Malicious and Unwanted Software (MALCON 2018) will be held at the Nantucket Hotel & Resort, Nantucket, Massachusetts, USA.
The Focus of the conference this year is twofold - (1) Future vulnerabilities and attacks, and (2) secure system implementation and design. The topics are described in the paragraphs below.

Future vulnerabilities and attacks

The dark economy now relies on the Internet. 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. The underground economy relies on computing infrastructure. Crypto-currencies are starting to replace cash as the preferred specie for remuneration. This specie can even be generated by malicious web activity.
As Internet of Things devices rapidly gain online presence, they also become an attractive target for malware. Lack of important security features of Internet enabled devices with questionable provenance invite new types of malware and eventually result in a large scale compromise. Vulnerable networks of IoT devices are then further leveraged to conduct targeted attacks. Defending such a diverse environment requires new analysis and detection paradigms.
Current security approaches are often ineffective, since attackers quickly field test prototype attacks that dodge current defenses. Defenders reverse engineer 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. Within this context, the future vulnerabilities and attacks explores the next steps we expect to see in the 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 analysis and training to conter social engineering,
- Online contraband networks,
- Malware use of darknet
- Identity theft,
- Malware obfuscation and encryption methods,
- Malicious network communications,
- Point-of-Sale malware,
- Hardware assisted malware detection,

MALWARE CONFERENCE (MALCON)

KNOW YOUR ENEMY

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

- Use of crypto-currency infrastructure for distributing malware,
- Malicious crypto-currency mining,
- Ransomware detection and reversing,
- Deep learning tools for malware detection (GAN?),
- Internet of Things and Mobile platforms, and
- Other innovations in this space.

Secure system implementation and design

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.

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,
- Physical unclonable functions
- Fingerprinting,
- Money laundering using crypto-currencies,
- Computer criminal profiling and motivation,
- Malware detection in large scale, heterogeneous IoT networks
- 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 2018 or if you are interested in contributing to the organization of the conference please contact Dr. Fernando C. Colon Osorio, General Program Chair, Malware 2018 at fcco@wssrl.org 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 mailto:avolynkin@cert.org.

Hotel:

The Nantucket Hotel & Resort, Nantucket, Massachusetts. For reservations call 866-807-6011 (USA, toll-free) or 508-310-1734. Mention the Malware conference for the preferred rate.

Airlines[1]: - From the East Coast of the US:

Boston To Nantucket: Cape Air has 16 noon-stops a day starting at 7:10 AM, with a typical fare of $ 99.00 each way.

NYC to Nantucket - JetBlue has a daily non-stop flights starting 10:38 AM, with a typical fare of $ 491.00 round trip.