

CALL FOR PAPERS for Ransomware and its social impacts

The IEEE Transaction on Computational Social Systems is accepting paper submissions from industry, government and academe for a Special Issue focused on formal methods and models to address ransomware and its threat to critical infrastructure. Ransomware is the malicious software that locks a computer until an extorted fee or ransom is paid for the key to unlock it. Extortionists are becoming more sophisticated in their attacks, and successful attacks are creating disruptive effects on their victims' systems. WannaCry and NotPetya were attacks on critical infrastructure that cascaded onto broader populations.

This Special Issue seeks modeling approaches that provide insight into the potential consequences that can result from ransomware attacks on critical infrastructure. Additionally, it seeks techniques to identify non-obvious features of malicious activity that could be used to distinguish threats who employ very similar methods and procedures.

Areas of Particular Interest

Researchers can choose any critical infrastructure as a use case or focus for models/model approaches. Full-length Research Papers are sought that address solutions to problems in all areas of ransomware, including but not limited to the following:

- Modeling approaches into the consequences of ransomware attacks on critical infrastructure
- Analytics for attribution of attacks on critical infrastructure
- Analytics for preventing attacks on critical infrastructure
- Analytics for mitigating attacks on critical infrastructure
- Emerging crimeware
- Human factors in ransomware attacks
- Geo-political or socio-economic dependencies
- Strategies to reduce the utility of crimeware, specifically ransomware on the critical infrastructure
- Specific critical infrastructures most at risk from a ransomware attack
- Avoiding misattribution
- Attack disruption

Guest Editors:

(Main) Peter Chin, PhD, Dept. of Computer Science, Boston University and STR

Email: spchin@cs.bu.edu

Angelos Keromytis, PhD, DARPA and Columbia University

Email: angelos.keromytis@darpa.mil

George Cybenko, PhD, Dorothy and Walter Gramm Professor of Engineering Dartmouth College

Email: george.cybenko@dartmouth.edu

Daniel G. Wolf, Cyber Pack Ventures, Inc.

Email: [dewolf@cyberpackventures.com](mailto:dwolf@cyberpackventures.com)

Donald L. Goff, PhD, Cyber Pack Ventures, Inc.

Email: dgoff@cyberpackventures.com

Rui Qin, PhD, Qingdao Academy of Intelligent Industries, China

Email: rui.qin@ia.ac.cn

Important dates

Paper submission Deadline: 10/15/2018

Acceptance Notification: 11/15/2018

Final Submissions Due: 12/31/2018