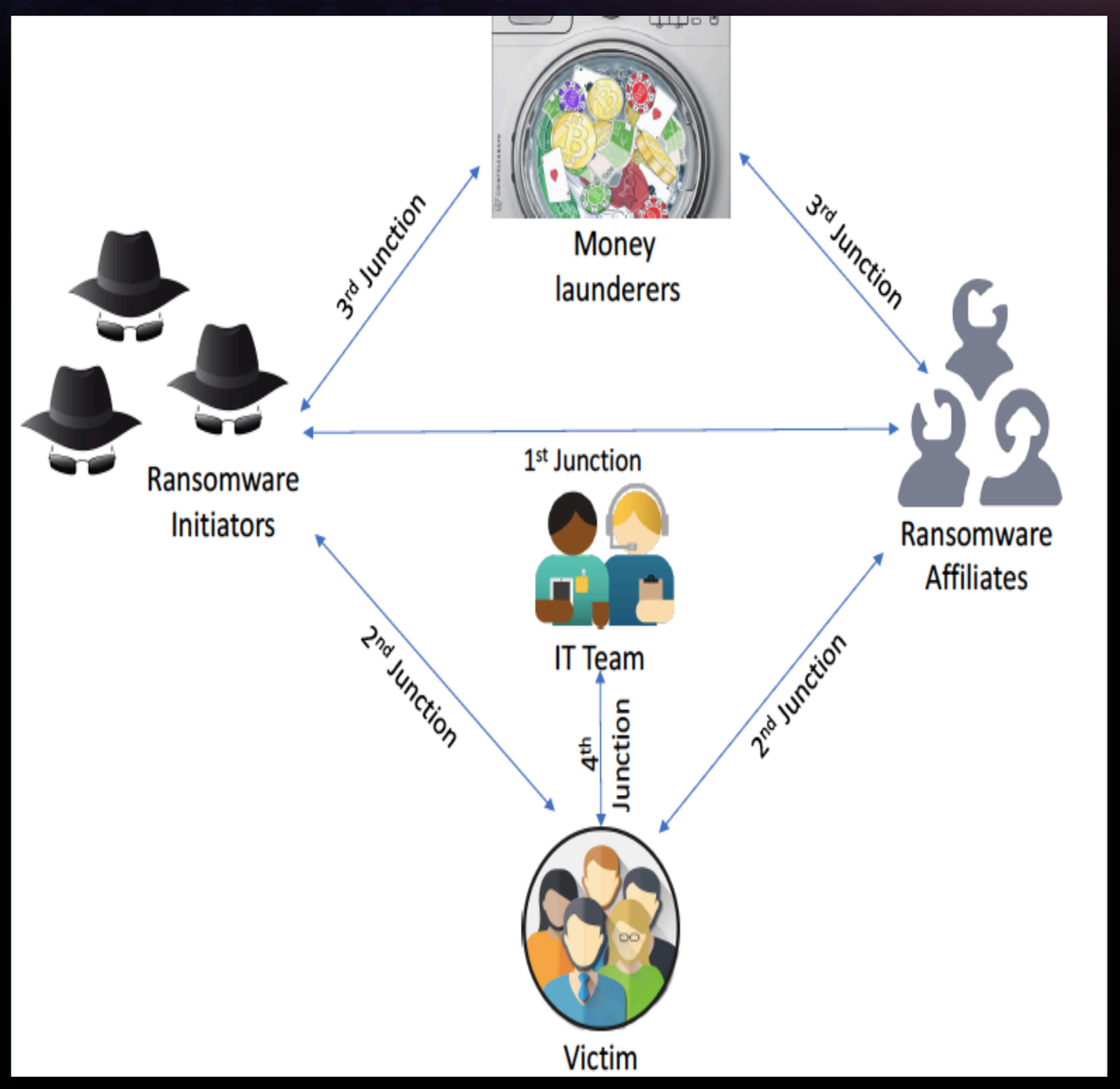
An Evidence-Based Ecological Approach for Disrupting Ransomware Spread

David Maimon, PhD– University of Maryland
Department of Criminology and Criminal Justice

Theoretical Framework

- Human Ecology views all forms of organization (whether biological or communal/social) as context-specific
  - Ecology encourages us to think of the situational environments that provide the structural resources and social opportunities for cybercrime to emerge.
  - While ecology is often seen as downplaying agency, it provides for agency as it is socially and collectively produced.
- An evidence-based ecological perspective provides an ideal framework for conceptualizing and understanding an interdisciplinary problem like ransomware since it draws on the assumption that solutions to human behaviors may be affected by the interconnected behavior of victims, offenders and law enforcement agencies operating within the cyber realm.
- Drawing on the ecological perspective we can identify key junctures in which research and policy efforts should be focused in aim to influence key players' online behaviors and reduce the probability of successful ransomware.

The Ecology of Ransomware



Key Junctures

- **1st Junction -** The intersection of online offenders who write the malicious software and propagate it and online offenders who are mainly involved in the distribution of the malicious software (*the ransomware initiators - ransomware affiliates juncture*)
- **2nd Junction**– the intersection of ransomware offenders and online computer users who are infected by the ransomware and required to send ransom money in order to decrypt their files (*the Online Offender-Victim juncture*)
- **3rd Junction -** the intersection of ransomware offenders and money launders services that are available to criminals who seek to disguise the origin of ransomware money (the online offenders-money launderers junction
- **4th Junction -** The intersection of online computer users and Information Technology Officer who are in charge on protecting and educating computer users (*the IT Managers-online computer users juncture*)

Potential Interventions

- **Deploying ransomware honeypots** - deploying fake ransomware and flooding the market with it will allow 1) identifying ransomware affiliates, and 2) mitigate the distribution of real ransomware.
- **Infiltrating ransomware campaigns by joining as a "legitimate" ransomware affiliate** - posing as an interested ransomware affiliate and initiate business relationships with ransomware initiators could reveal some of the communication patterns and financial relationships between ransomware initiators and affiliates, assist in identifying ransomware initiators intentions and allow the development of preventive efforts against such campaigns.
- **Increasing awareness practices among potential victims-** develop cyber security awareness programs that are designed to educate commuter users about the hazard of ransomware
- **Encouraging victims' reports on ransomware victimization.**
- **Build fake Bitcoin mixers-** Setting up mixing services and attracting criminals can be a way to track ransomware offenders and deter them.
- **Monitor Bitcoin exchange markets.**

Potential Research Initiatives

- There is a need to develop acceptable and consistent matrices to support empirical investigations of the effectiveness the proposed interventions in preventing ransomware campaigns
- Scholars should explore the progression of ransomware infections by focusing on the interaction between offenders and victims and their decision making during the progression of the criminal event