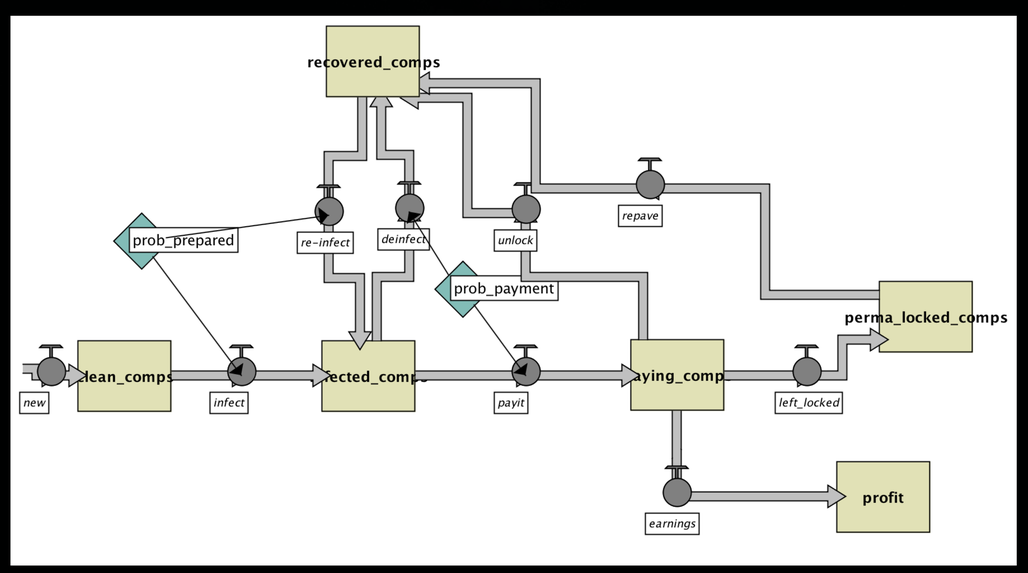
Understanding the Ransomware Landscape through System Dynamics Modeling

Galois, Inc. – Jem Berkes, David Burke, Andrey Chudnov

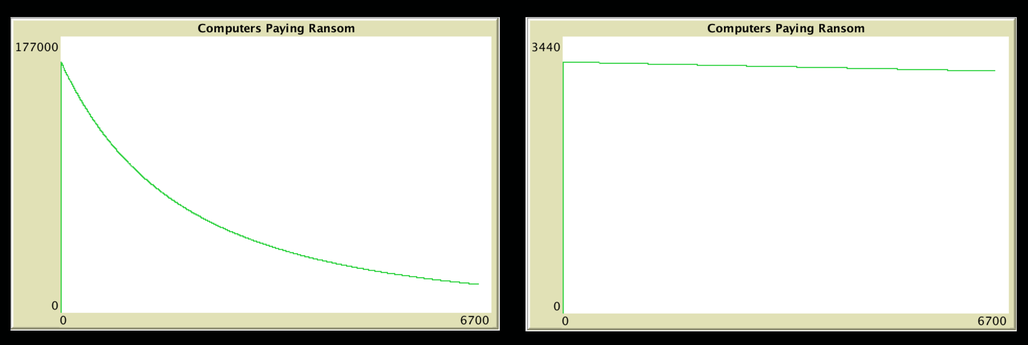
Objectives

- Ransomware as a business: understand the ecosystem
- System Dynamics models and experiments
- Identify areas for further research



Approach

- Experiments using System Dynamics models
- Enables modeling of complex feedback loops
- Can reveal emergent behavior over time
- Our initial models focus on the target space
- Model flows are *people* and *money*



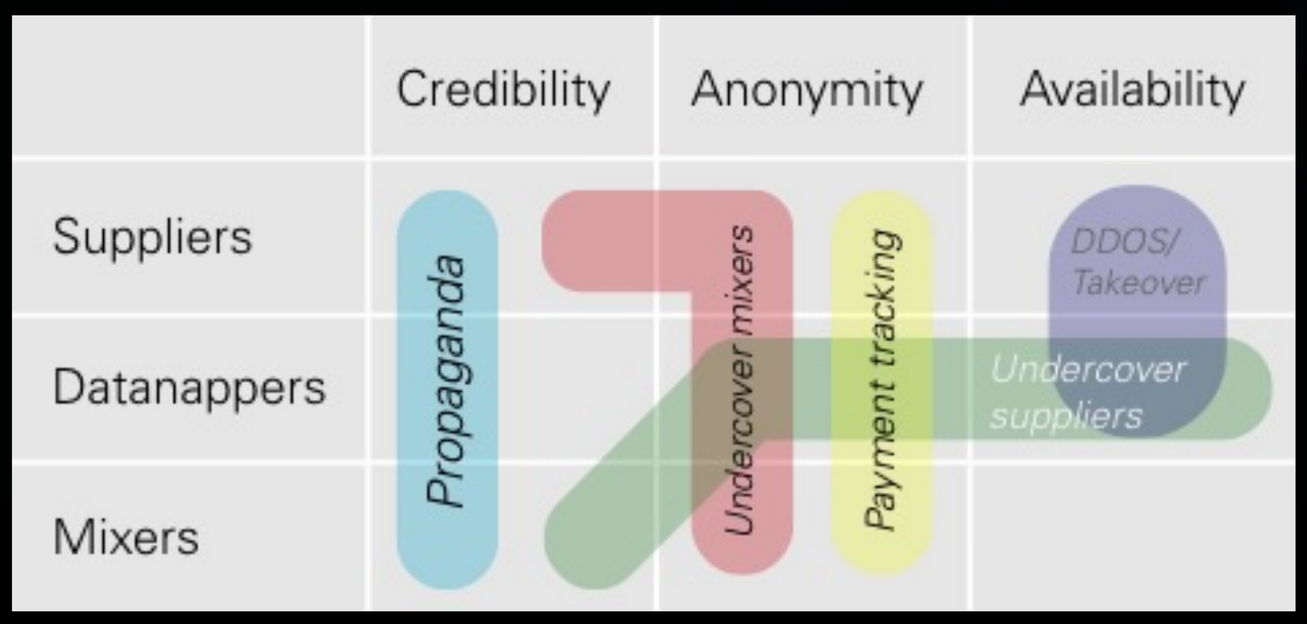
Simulations: WannaCry (left) and CryptoWall (right)

Initial results

- Qualitatively, output matches real attacks
  - CryptoWall lasts much longer than WannaCry
  - CryptoWall raises more profit than WannaCry
  - WannaCry has much higher peak # of infections
- Iterative refinement and validation of models

Future Research

- Ransomware “market research”
- Refine/extend the models: identify leverage points
- Counter-intelligence: methods to disrupt ransomware ecosystem



SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING

Computational Cybersecurity in Compromised Environments
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia