SCORE

Special Cyber Operations
Research & Engineering

Computational Cybersecurity in
Compromised Environments

C3E

Modeling Consequences of Ransomware on Critical Infrastructures

C3E Cybersecurity Problems

- Identity Discovery Challenge (2012)
- APT Infection Discovery Using DNS Data (2013)
- Metadata-based Malicious Cyber Discovery (2014)
- Novel Approaches to Avoid Misattribution of Malicious Cyber Activity (2015)
- **Modeling Consequences of Ransomware on Critical Infrastructures (2016)**

Modeling Consequences of Ransomware on Critical Infrastructures

- Modeling approaches are sought for the 2016 challenge problem to provide insight into potential consequences that might result from crimeware attacks, specifically ransomware, on the critical infrastructure

Ransomware & Critical Infrastructures

- Adversaries in cyberspace continues to grow and become more sophisticated in their practices
  - Use of crimeware, especially ransomeware is increasing
  - Crimeware has more Advanced Persistent Threat (APT) like characteristics
- Institute for Critical Infrastructure Technology (ICIT) recent report warns that ransomware in 2016 could hold America hostage

Ransomware & Critical Infrastructures

- Ransomware attacks, unlike other crimeware, create disruptive effects on victim systems
  - An associated attack on critical infrastructure has the potential to increase the risk of unintended and possibly catastrophic consequences.

- Ransomware as a service availability means the skill level for entry is low resulting in the likelihood of a significant disruptive event occurring

- Nation state actors could use the ransomware disruptive effects to mask an information warfare attack while providing some level of deniability.

Specific Research Questions

- Are there modeling approaches for gaining insight into the consequences of ransomware attacks on critical infrastructure?
  - Could these be used to inform a risk framework?
  - Could these produce mitigation strategies?

- What novel methods/techniques or behavioral analytics exist to attribute attacks?
  - How would you apply these specifically to Advanced Persistent Threats?
  - Could these reveal possible nation-state instigation?
  - How would these minimize the possibility of misattribution?

Specific Research Questions

- Is there any other emerging crimeware that could cause significant disruptive events or other unintended consequences?

- Are there any geo-political or socio-economic dependencies that might reveal the perpetrator's true identity?

- What is a strategy to reduce the utility of crimeware, specifically ransomware on the critical infrastructure?

Worksheet Questions

- Are these the right questions to ask the researchers for the Challenge Problem? Are there others that need attention?
- Are there other emerging crimeware or ransomware potential threats that need more research attention?
- Do you know of any on-going research in the areas of crimeware or ransomware?

Worksheet Questions

- Are there any suggested data sources, reports, or examples?

- Would you be interested in submitting a short proposal for approaches to stimulate research in this area?

- Do you have any suggestions to improve the Challenge Problem process?

QUESTIONS