When the FIRE BURNs

Visualizing and Exploring Rogue Autonomous Systems

Federico Maggi <fmaggi@elet.polimi.it
POLITECNICO DI MILANO

Outline

- Finding Rogue Networks
- Baring Unknown Rogue Networks
- Demo of FIRE
- Demo of BURN

Finding Rogue nEtworks (FIRE)

- Rogue AS = friendly AS, with hosts that do
  - Malware hosting
  - Botnet traffic (C&C)
  - Phishing
  - Spamming
- Collects data from:
  - Anubis (malware, C&C traffic)
  - PhishTank (phishing)
  - SpamHaus (spamming)

Baring Unknown Rogue Networks (BURN)

- Built on top of FIRE
- Visualization system
- Meant for both
  - End-users (visual exploration)
  - Experts (overview, knowledge discovery before using FIRE)
- Prototype currently in beta phase

DEMOs

When the FIRE BURNs

Visualizing and Exploring Rogue Autonomous Systems

http://www.syssec-project.eu
http://twitter.com/syssecproject

Federico Maggi
Politecnico di Milano