

# Automated Worm Detection and Response

Dan Ellis

703-983-5807 • [ellisd@mitre.org](mailto:ellisd@mitre.org)

MITRE Sponsored Research



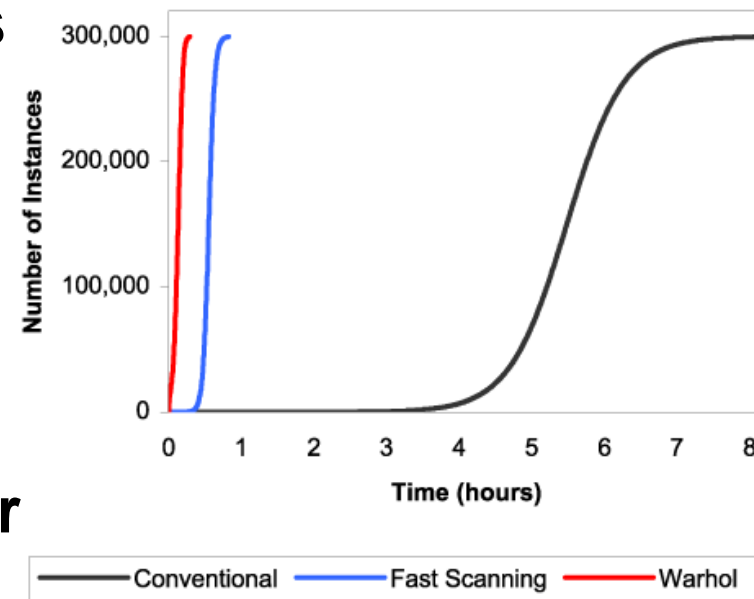
# Problem

- **Worms can infect enterprises in seconds to minutes.**
- **Current intrusion detection and response technologies are not sensitive, accurate, or fast enough.**
- **Can worms be detected quickly enough to respond in real time?**
- **Can effective countermeasures be deployed automatically to minimize spread?**

# Background

- Worms are *weaponizable*
  - Fast spread!
  - Arbitrary payloads
- Current intrusion detection & response is measured in hours
- Contemporary research focuses on Internet-scale response or perimeter defenses

$$a = \frac{e^{K(t-T)}}{1 + e^{K(t-T)'}}$$



# Objective

- To develop real-time worm detection and response capabilities for enterprise networks
  - Develop sensitive and accurate detection capability
  - Develop ability to execute realistic, repeatable tests on a *production network*
  - Refine and distribute **techniques** for near-real-time detection
  - Evaluate different response strategies triggered by detection

# Activities

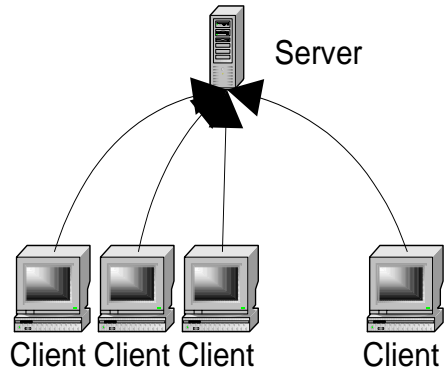
## Done

- **Developed patterns and signatures for worm attacks**
- **Developed benign test capability (Message Relay System)**
- **Deployed sensors on MITRE corporate network to validate and discover signatures**

## Current

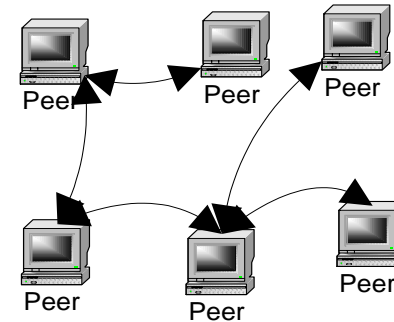
- **Evaluating detection**
  - **Accuracy, sensitivity, performance**

# Highlight

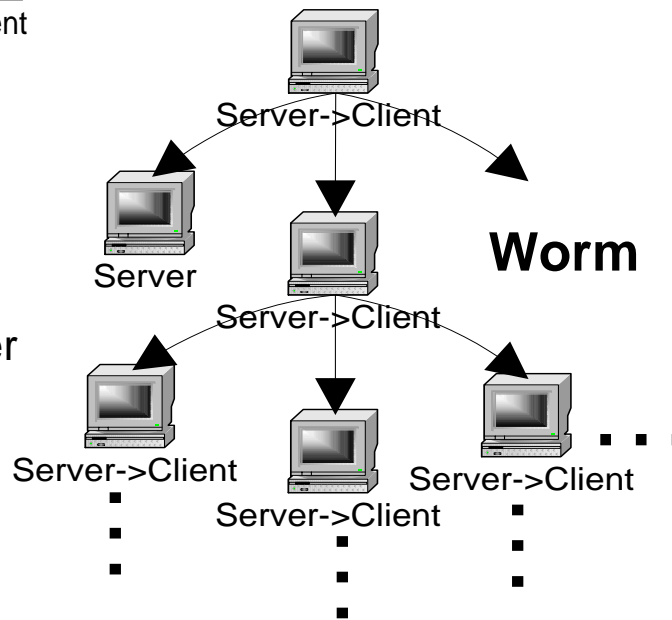


**Normal  
Client-Server**

Worm traffic looks  
different from other  
types of network  
traffic



**Normal P2P**



**Worm**



# Impacts

- **Improve state of the art of enterprise security management**
  - **Push industry to develop adaptive defense support capabilities**
- **Technology transfer to:**
  - **MITRE sponsors (DoD, Intel Community, IRS, etc.)**
  - **Community as a whole**
  - **MITRE operations**

# Future Plans

