



# The Emerging Threat of Peer-to-Peer Worms

Nassima KHIAT, Yannick CARLINET and Nazim AGOULMINE

**MonAM 2006 Workshop**

# AGENDA



- ▶ Introduction
- ▶ Peer-to-Peer worms
- ▶ Modeling of Peer-to-Peer worms
- ▶ Solutions to Peer-to-Peer worms
- ▶ Conclusion and future works

# Introduction

▶ **Worm: program that self-propagates across a network exploiting security or policy flaws in widely-used services [N. Weaver et al.]**

▶ **Impact on individual users and companies**

- ▶ SQL Slammer (January 2003): more than 750 millions dollars of damages in the world (Computer Economics)

| Worldwide Impact (US \$) |                |
|--------------------------|----------------|
| 2005                     | \$14.2 Billion |
| 2004                     | 17.5 Billion   |
| 2003                     | 13.0 Billion   |
| 2002                     | 11.1 Billion   |
| 2001                     | 13.2 Billion   |
| 2000                     | 17.1 Billion   |
| 1999                     | 13.0 Billion   |
| 1998                     | 6.1 Billion    |
| 1997                     | 3.3 Billion    |
| 1996                     | 1.8 Billion    |
| 1995                     | 500 Million    |

Source: Computer Economics, 2006 Figure 1

▶ **Propagation ways of worms**

- ▶ Random scan
- ▶ Hit-list based
- ▶ Topological
- ▶ Passive

# Peer-to-Peer worms

- ▶ **Peer-to-Peer worm: worm that uses a P2P system to spread from one machine to another**
  
- ▶ **Two classes:**
  - ▶ Topological scan based P2P worms
  - ▶ Passive P2P worms (e.g. Benjamin)
  
- ▶ **Importance of P2P worms detection**
  - ▶ Devastating impact on ISP's networks and customer hosts
  - ▶ Potentially more harmful than non-P2P worms (fast, furtive)
  - ▶ P2P systems will be used to distribute legal content

# Modeling of Peer-to-Peer worms



## ▶ Utility of worms modeling :

- ▶ Get information about worm propagation characteristics and impact on the network
- ▶ Test detection and mitigation systems

## ▶ Interesting studies

- ▶ W. Yu, C. Boyer, S. Chellappan and D. Xuan, IEEE ICC 2005.
  - Modeling the propagation of topological scan based P2P worms
- ▶ R. Thommes and M. Coates, IEEE INFOCOM 2006
  - Modeling passive scan based P2P worms
- ▶ K. Ramachandran and B. Sikdar, Hot-P2P, 2006
  - Modeling worm attacks in Gnutella-type P2P systems

# Solutions to Peer-to-Peer worms



- ▶ **Guardian nodes, L. Zhou et al.**
  - ▶ Nodes with detection capabilities
  - ▶ Alarms triggered to warn non-guardian nodes
  
- ▶ **Peer Pressure, P. Keyani et al.**
  - ▶ Against fragmentation attacks
  - ▶ Addition of virtual neighbors to each peer
  
- ▶ **Credence, K. Walsh and E. G. Sirer**
  - ▶ Reputation system
  - ▶ Assessment of files authenticity

# Conclusion & future works



- ▶ P2P worms: a serious threat
- ▶ Still an active research area
- ▶ Problem of similarity between P2P worms traffic and legitimate P2P network activity
- ▶ Possible use of honeypot technology in a detection solution
- ▶ When a worm is detected: necessity of a containment system to avoid further propagation of this worm
  - At ISP level
  - Distributed



# Questions?