

# A Taxonomy of Botnets

# Introduction

Botnets:

- networks of compromised machines/ networks of victims machines to attack other machines
- Botnets are used to spread new bots

→ to protect from these attacks the creation of new response strategies are required

# Botnets Background

Origin of botnets:

- use of email
- instant messaging
- remote software vulnerabilities

Applications running on botnet platforms:

- Spam
- identity theft
- key cracking

# Botnets Command and Control

Ways of communication between the bots and the victims

→ weakest link is about the C&C box (command and control)

Organizational techniques:

1. Decentralized Naming Resolution  
→ botnets act as their own DNS cloud
2. Tor botnets  
→ using a proxy network
3. Tunneling bots  
→ bots that tunnel through existing protocols

# Botnet Taxonomie

## Taxonomy of possible botnet topologies

- will help researchers identify what types of responses are most effective against botnets
- assist the defender in identifying possible types of botnets,
- describe key properties of botnet classes

## Metrics for botnet performance

- evaluate and compare response strategies
- important measures of botnets: size, network diameter, and redundancy

# Empirical Analysis of Responses to Scale-Free Botnets

Analysis of characteristics of botnets shows that targeted responses work best against scale-free networks.

For Confirmation:  Targeted Response Using DDNS Sinkholing

Result: In general, the experiment showed that, for scale-free botnets, particularly those using star-topologies, targeted responses such as DNS manipulation can be effective in capturing most of an infectious network.

# Conclusion

- Botnets present significant new challenges for researchers
- The fluid nature of the topic requires researchers anticipate future botnet strategies and design effective response techniques
- Analysis showed that targeted removals on scale free botnets offer the best response

## Future Work

- Future Work will investigate the potential of honeypots to measure local transitivity in botnets, including P2P botnets.