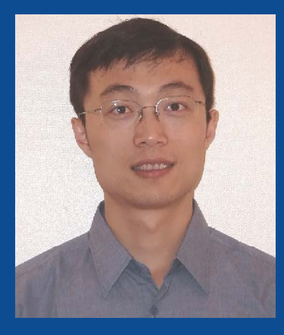
Collaborative Research: CT-ISG:

Modeling and Measuring Botnets

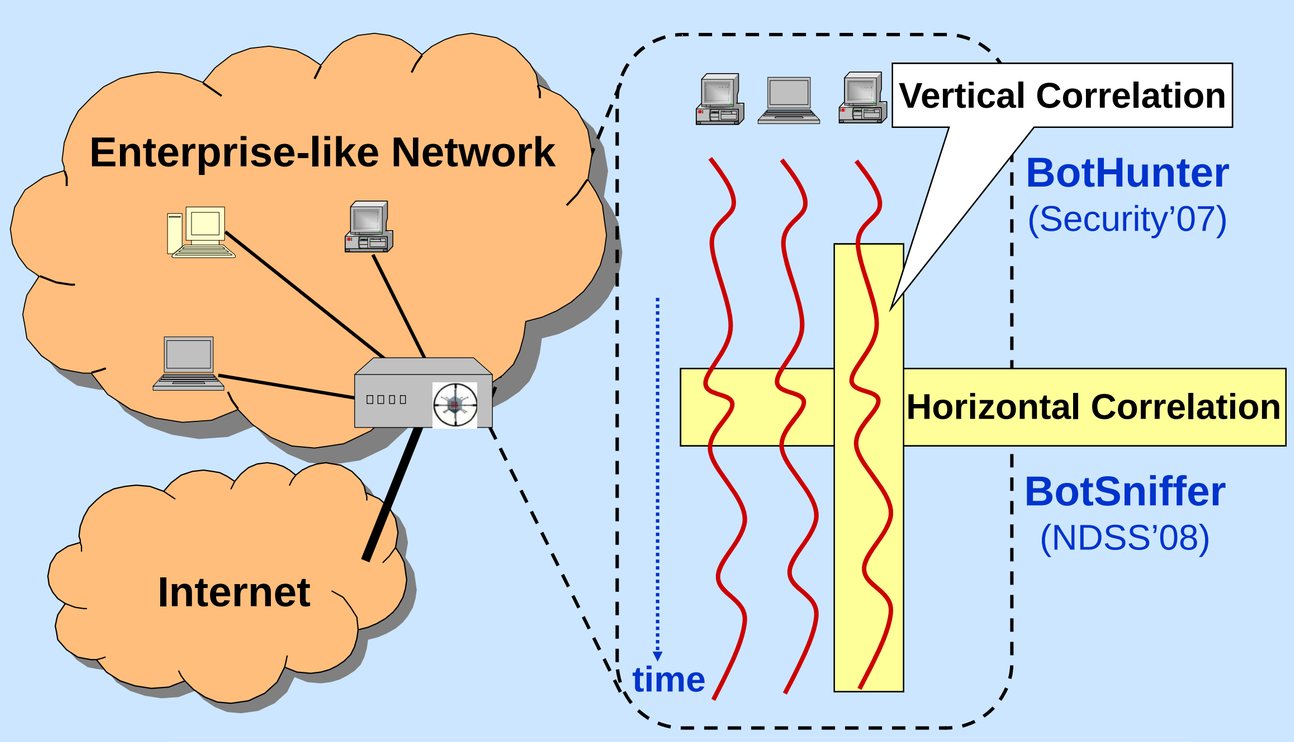



Wenke Lee, Georgia Tech. http://www.cc.gatech.edu/~wenke/
Cliff C. Zou, Univ. Central Florida http://www.cs.ucf.edu/~czou/

SUMMARY

A ***botnet*** is a network of compromised computers, or bots, commandeered by an adversarial botmaster. Botnets are responsible for many Internet attacks, including spam, phishing, key logging, and denial of service.

This project aims to develop techniques to botnet modeling, measuring, and detection techniques. Knowing the dynamics, trend, size, and locations of the population of a botnet enables us assess the threat and prioritize the appropriate response actions; Detecting a botnet in a local area network with low false negative helps us eliminate botnet threat.



Botnet Detection based on the Correlation in Botnet Traffic

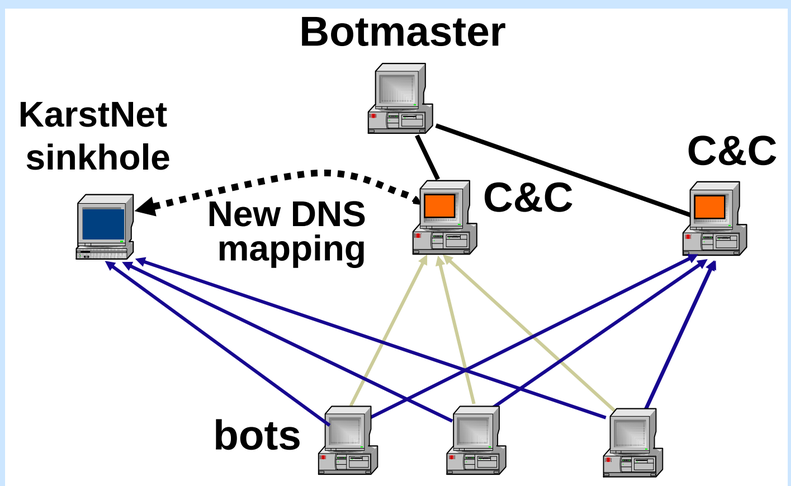
Approach and Impact

New approach

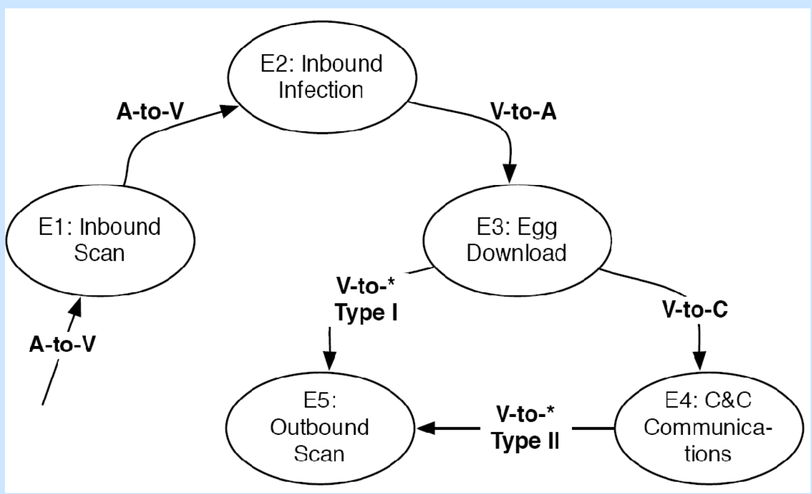
- A DNS hijack-based botnet monitor
- Novel model and measurement
- Two botnet detection approaches

Research Impact

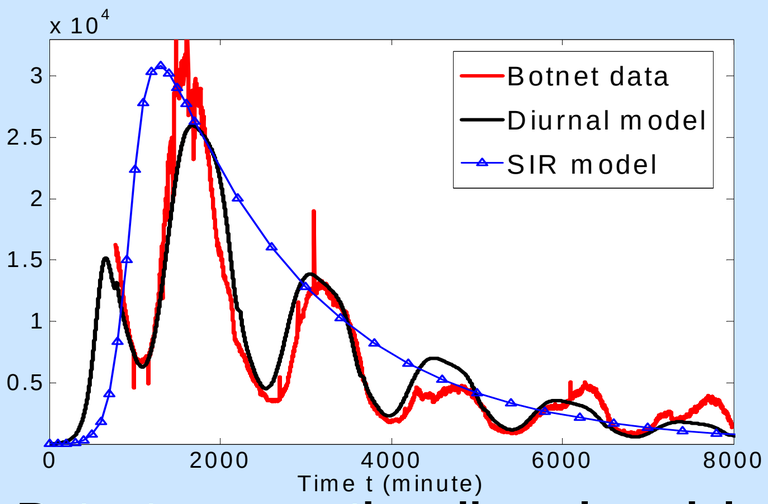
- Deeper understanding of botnets
- Effective/practical botnet detection
- Help secure military/civil networks



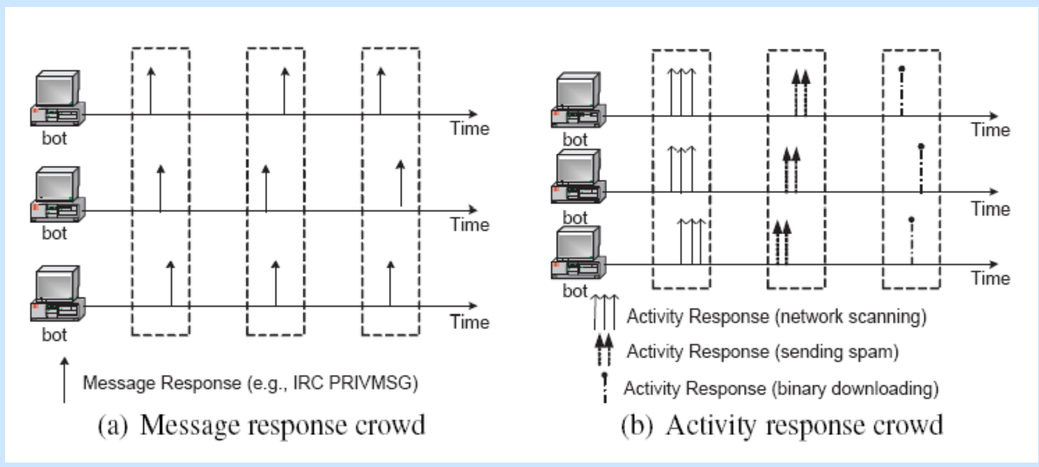
KarstNet: DNS hijack-based botnet monitor



Bothunter: botnet infection lifecyle model



Botnet propagation diurnal model



Botsniffer: spatial-temporal similarity

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

Georgia Tech
UCF