"Botnet" is a network of computers that are compromised and controlled by an attacker (botmasters). Botnets are one of the most serious threats to today's Internet. Most current botnets have centralized command and control (C&C) architecture. However, peer-to-peer (P2P) structured botnets have gradually emerged as a new advanced form of botnets. Without C&C servers, P2P botnets are more resilient to defense countermeasures than traditional centralized botnets.

In this dissertation, we first systematically study P2P botnets along multiple dimensions: bot candidate selection, network construction and C&C mechanisms and communication protocols.

As a further illustration of P2P botnets, we then present the design of an advanced hybrid P2P botnet, which could be developed by botmasters in the near future. Compared with current botnets, the proposed botnet is harder to be shut down, monitored, and hijacked. It provides robust network connectivity, individualized encryption and control traffic dispersion, limited botnet exposure by each bot, and easy monitoring and recovery by its botmaster. We suggest and analyze several possible defenses against this advanced botnet.

Besides P2P botnet design, we investigate honeypot detection as well, in order to show the limitations in deploying honeypots in botnet defense systems and the importance of building covert honeypots. A hardware and software independent honeypot detection methodology is proposed based on the assumption: security professionals deploying honeypots have liability constraint such that they cannot allow their honeypots to participate in real attacks that could cause damage to others, while attackers do not need to follow this constraint. We present honeypot detection techniques that can be used in both centralized botnets and P2P botnets. Our experiments show that current standard honeypot and honeynet programs are vulnerable to the proposed honeypot detection techniques. In the meantime, we discuss some guidelines for defending against general honeypot-aware attacks.

Upon our understanding of P2P botnets, we finally turn our focus to P2P botnet mitigation. We provide mathematical analysis of two P2P botnet defense approaches --- index poisoning defense and Sybil defense, and one monitoring technique - passive monitoring. According to the common idea shared by index poisoning defense and Sybil defense, we are able to give analytical results to evaluate their performance. And simulation-based experiments show that our analysis is accurate. For P2P botnet monitoring, we provide mathematical analysis of passive monitoring based on infiltrated honeypots or captured bots. The analysis shows how many bots will contain an infiltrated node in their routing tables, which is a lower bound for the number of bots that an infiltrated node can monitor. Simulation results also confirm the accuracy of our analysis.
Approved for distribution by Cliff C. Zou, Committee Chair, on June 23, 2010.

The public is welcome to attend.