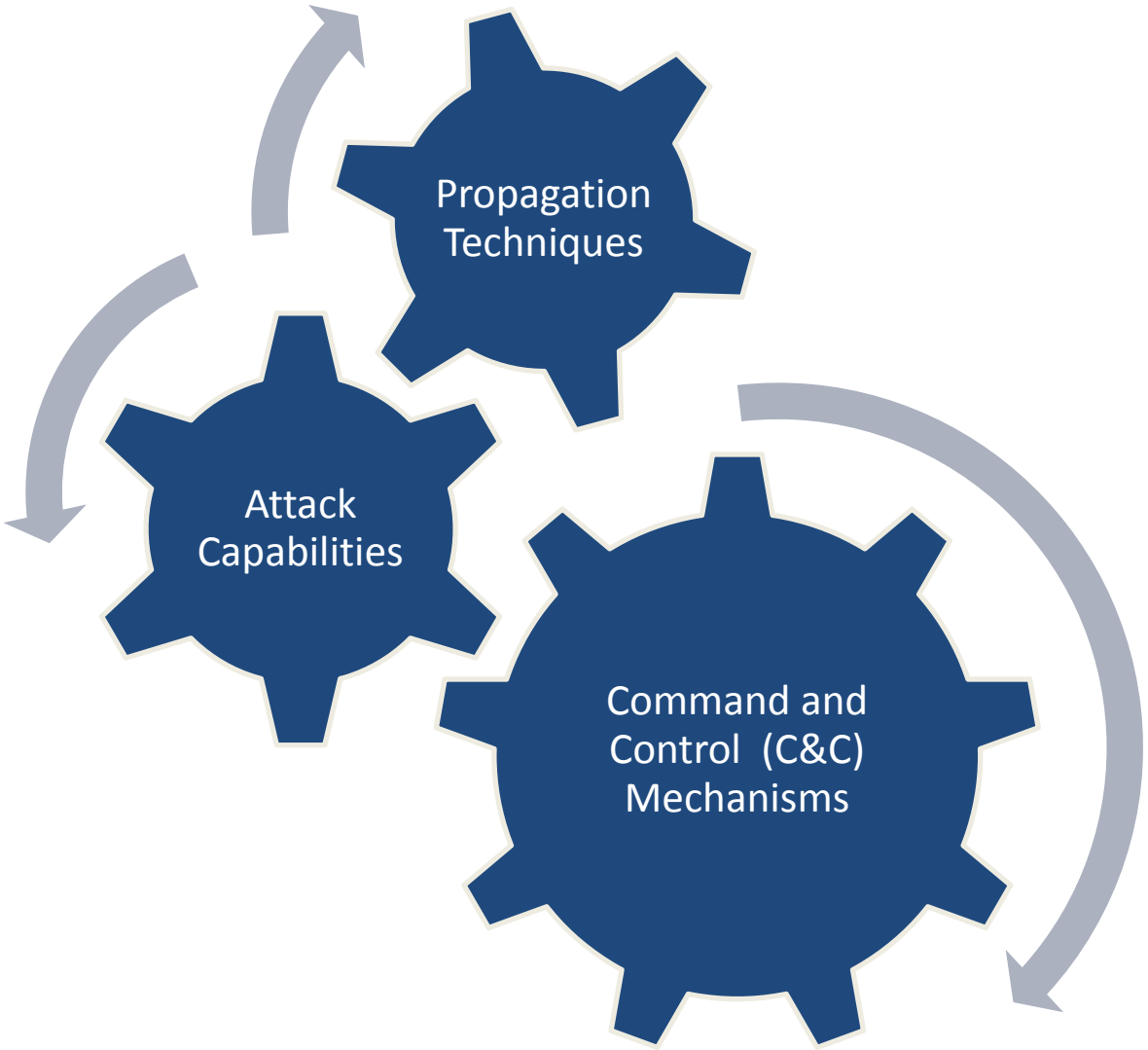
Next-Generation Botnets

Lenny Zeltser

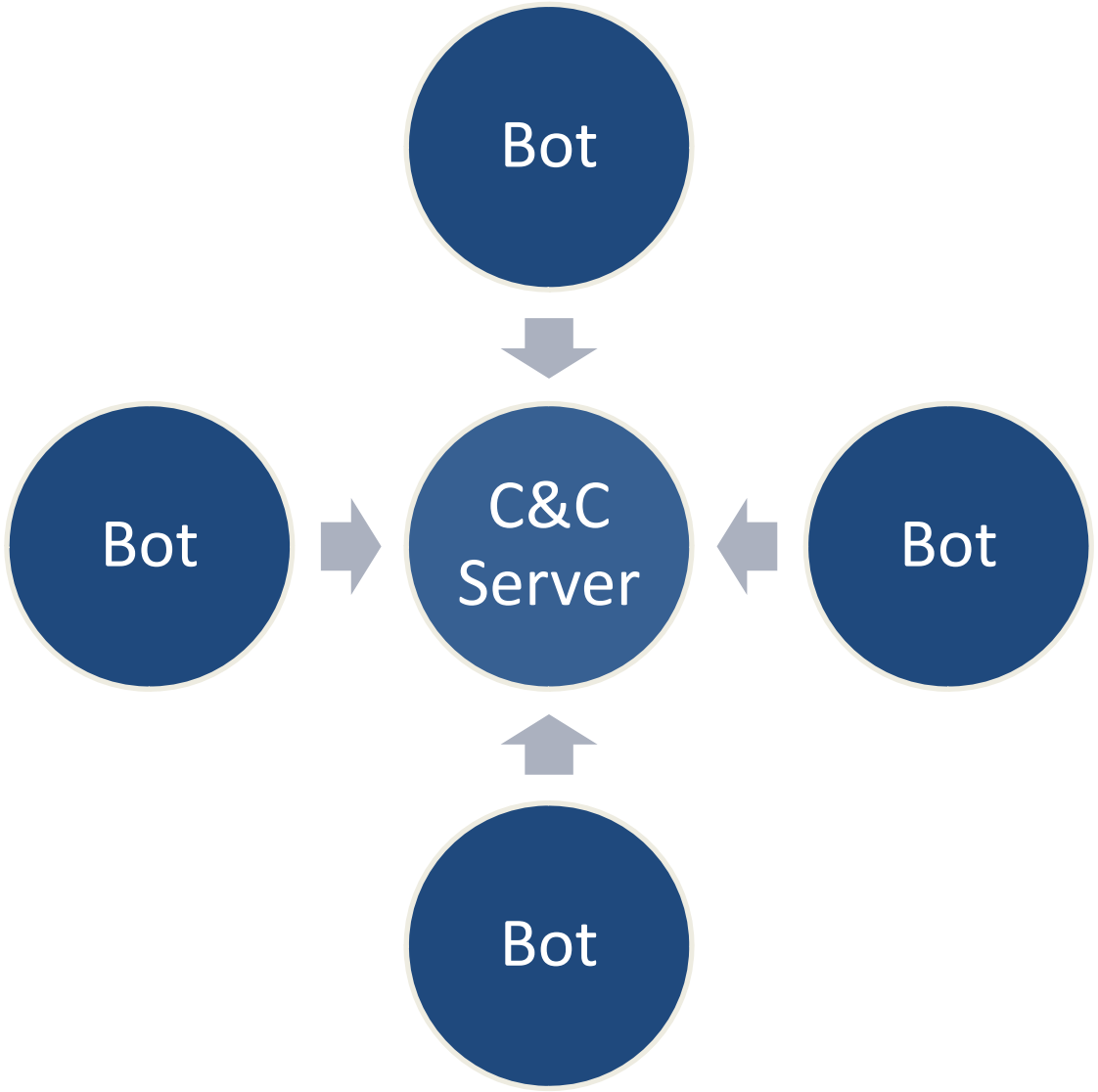
February 2008

Key Slides

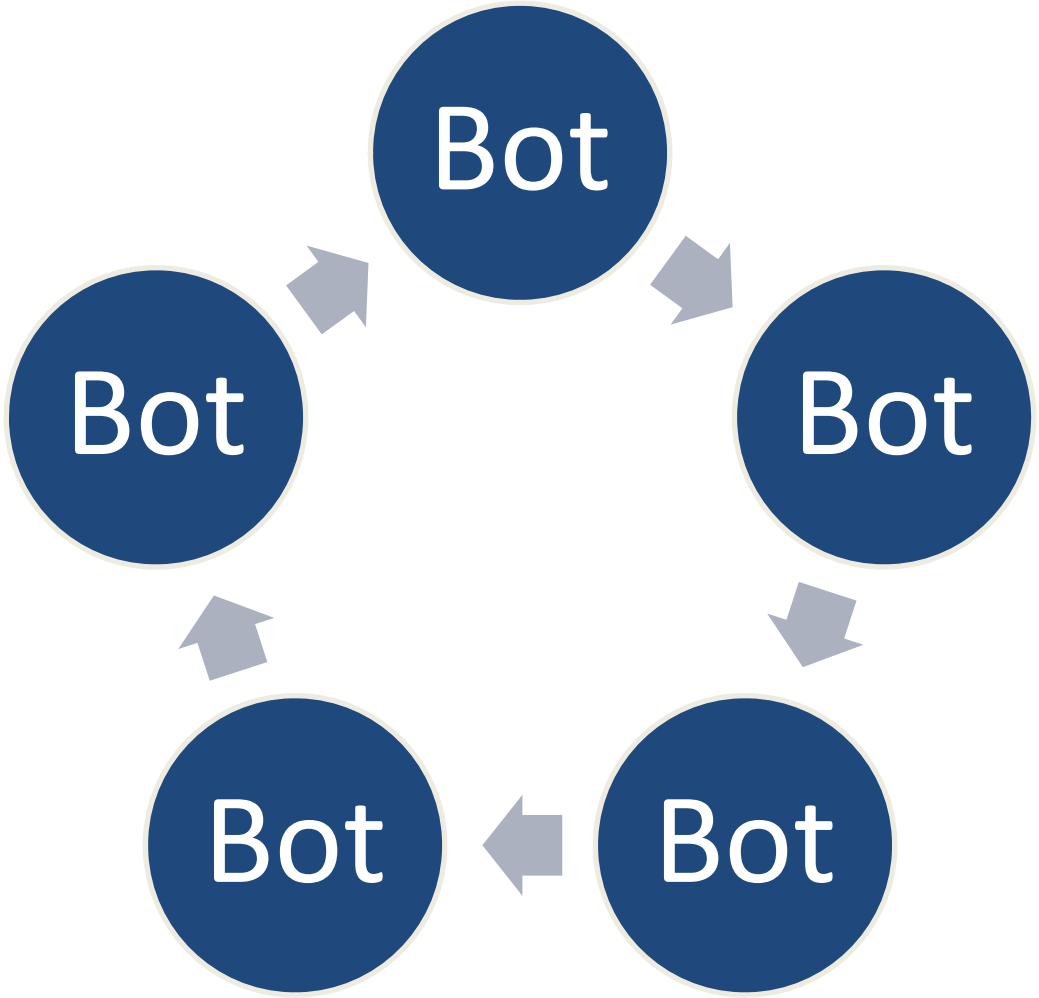
To understand the threat of botnets, consider how they spread, how they are controlled, and what they can do



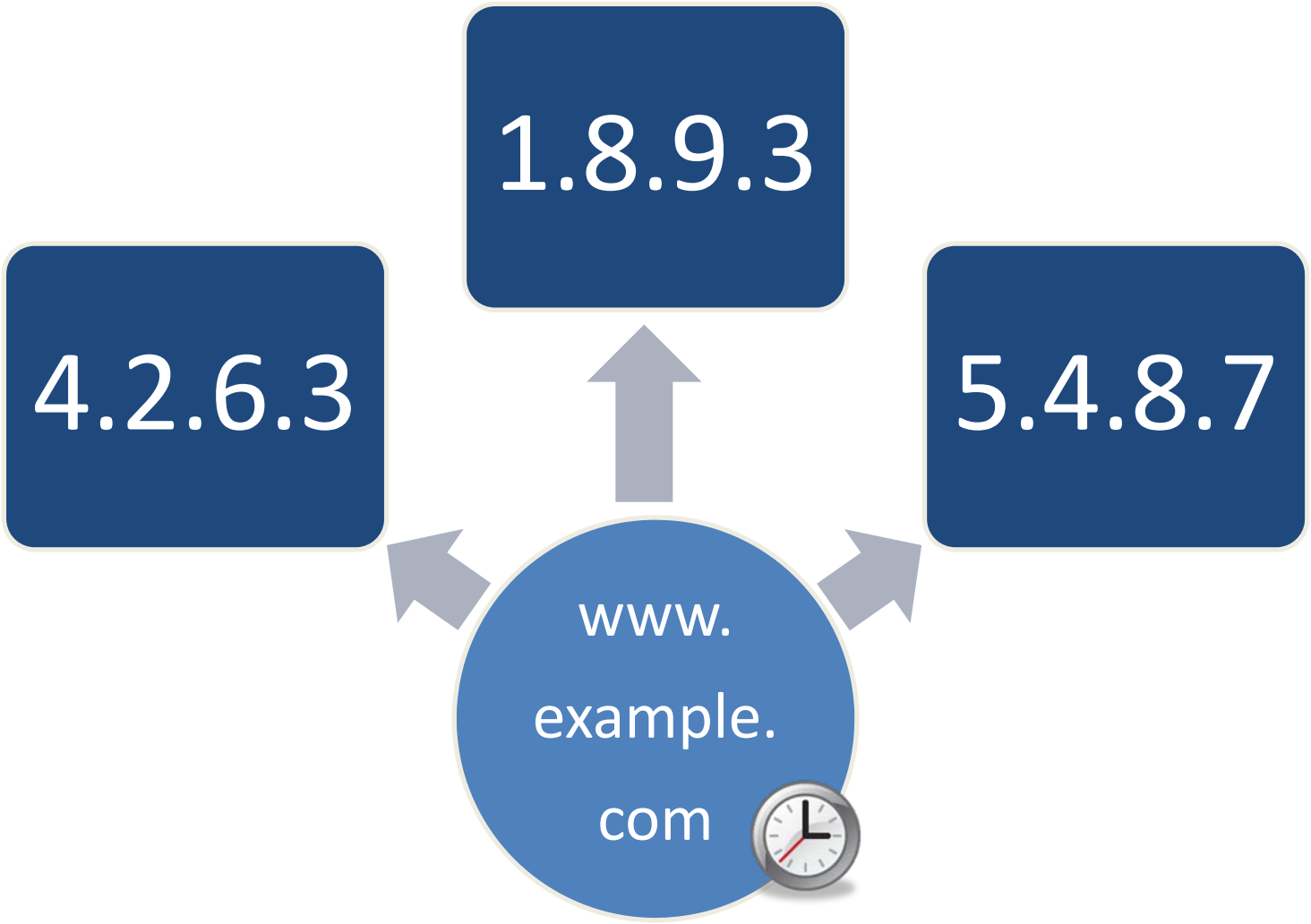
In traditional command and control methods, the bots connect to a central server to obtain their instructions.



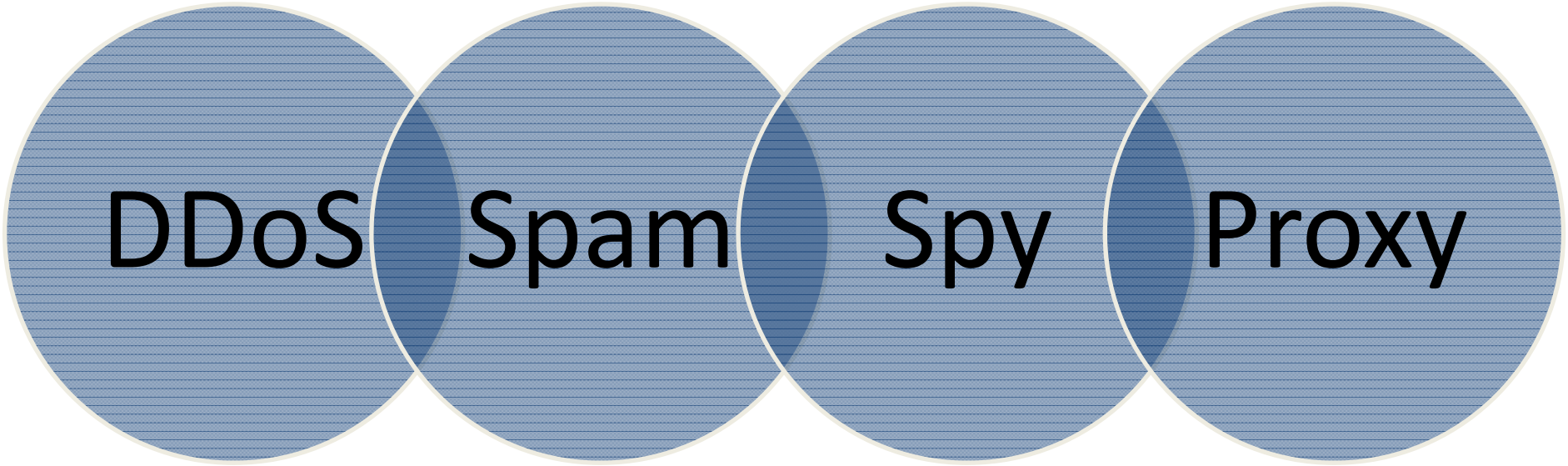
If a botnet uses a peer-to-peer mechanism for its command and control channel, bots communicate with each other and with the attacker without a central server.



In fast-flux DNS, a hostname resolves to many IP addresses. These mappings change every few minutes. Sometimes authoritative DNS servers change as well.



Capabilities of a botnet include the ability to launch distributed denial-of-service (DDoS) attacks, relay spam, leak data via spyware, proxy attackers' connections, etc.



Standard “defense in depth” principles apply to protecting against the various aspects of botnet threats.