There are several fundamental problems that lead to the “botnet” phenomenon. These include:

- Imperfect programming practices: it’s nearly impossible to write highly complex code without bugs that can be exploited
- The “Grandma” effect: the overwhelming majority of Internet users are not tech savvy and will execute almost anything that comes their way

One of the original uses of computer bots was for moderating Internet Relay Chat (IRC) Channels.

- Eggdrop was one of the first bots developed in 1993
- Shortly after more malicious IRC bots emerged to attack other IRC users/servers
  - Flooding with packets (DoS attacks)
  - Hiding the origin of traditional DoS attacks and increasing the magnitude via Distributed Denial of Service (DDoS) attacks

In order to launch DDoS attacks more bots were needed and a distributed mechanism was required:

- Led to the creation of integration with existing trojans
  - Subseven Bot, Bionet Bot, AttackBot, GTBot, Evilbot, Slackbot
  - SDBot: 4,000+ known variants by Aug 2004!
  - Agobot: support for DDoS attacks, GRE tunneling, password sniffing, spam proxy

Utilize anti-virus, firewalls, and automated patching to prevent computers from being automatically infected with malware.

Problem: This reduces the problem but does not completely eliminate it. In addition, nearly all of these mechanisms can be defeated by more sophisticated malware.
New bots observed each day rose from less than 2,000 to more than 30,000 in less than 6 months
- 800,000-900,000 total number of bot infected systems
- Some botnets consisting of over 100,000 bots observed by CERT

Observation:
- The number of botnets is increasing yet the number of bots in each botnet is decreasing
  - Previously ~80-140K members in a botnet
  - Now typically several hundred to a few thousand members

Explanation:
- Harder to detect smaller botnets, and easier to sell/rent
- Additional bandwidth of each bot has increased as broadband use increases

There are very few overt characteristics to identify botnets
- Almost all rely on a successful propagation technique
  - Most bots spread via automated vulnerability scans
    - e.g. MyDoom, Bagle, etc
- Internet Motion Sensor Project
  - Network of sensors that monitors 60 unused address blocks at 19 organizations
- Honeynet
  - Monitor unpatched Windows systems and let them be exploited
  - Only 2 out of 12 were infected with non botnet malware

Detect the command and control structure
- Direct connection to controller
- Indirect connection via a proxy
- IRC - simple text based syntax, low latency, widely available and anonymity built in

Detect the secondary features of infection
- Monitor the well known IRC port 6667 and identify botnet string payloads
  - Problem: IRC can run on any port
    - Honeypot experiment detected 3 instances running on higher port numbers
  - Identify behavioral characteristics that are faster than human response times
    - Problem: High false positive rate
  - Utilize a honeypot to connect back and profile the IRC botnet server
Interesting Honeypot Results
- Connections from bots
  - Search engines
  - Bandwidth testers
  - Downloading posts from message boards to get server addresses
  - Transmission of comprehensive host profiles to other servers
    - Including detailed information on the operating system, host bandwidth, users, passwords, file shares, filenames and permissions for all files, and a number of other minute details about the infected host.

Conclusions
- There are no simple characteristics to identify the command and control traffic
- Time of connections vary from seconds to hours
- Number of bytes transferred varies
- Can inspect the payload of packets, but at a high price of computation
- Easily defeated by encrypting packets, sending random "noise" packets, changing communication topologies

Botnets of Tomorrow
- Move away from centralized botnets especially IRC
- Modification of existing p2p systems to incorporate botnet functionality
- Increase in "random" botnets
  - No bot knows information about only one other bot
  - High latency / no message delivery guarantee

Botnet Detection / Mitigation
- Use other "proven" detection systems
  - Host detectors (honeypots) / network detectors
    - Monitor for "noisy" behaviors (e.g. port scanning)
    - Identify bot programs by correlating their sending characteristics
    - Aggregate statistics together to determine source of attacks

Challenges in Killing Botnets
- Once a botnet has been detected there are a limited number of options to disrupt it
  - Becomes very legally complicated when the operators are in foreign countries
  - Killing individual bots vs. killing the botnet
- Automation and cooperation among ISPs

Questions?