Cybersecurity

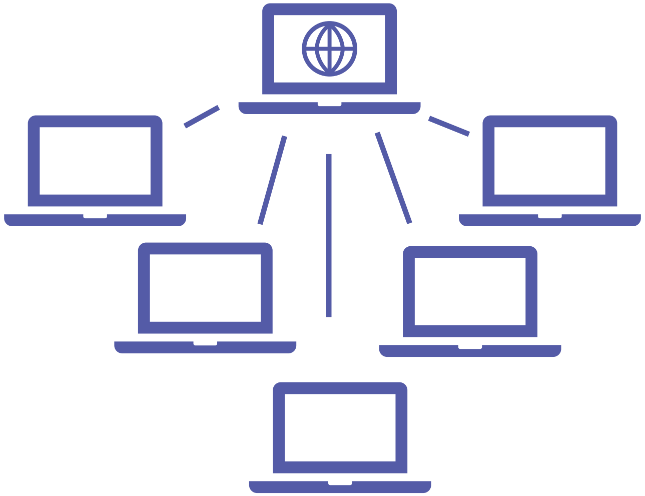
Bots and Botnets

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

CYBER.ORG

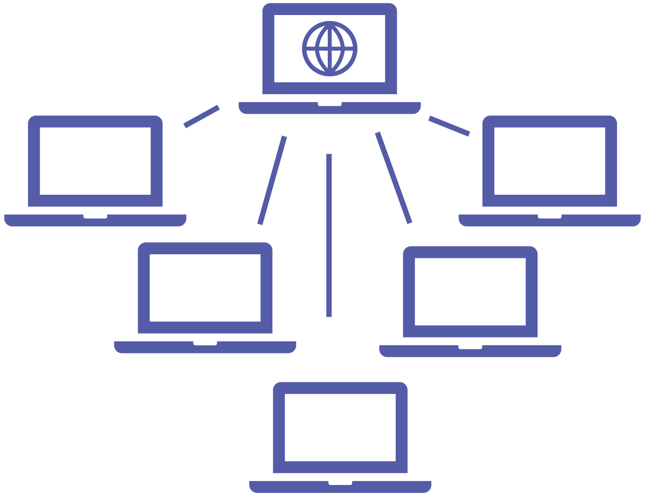
Botnets



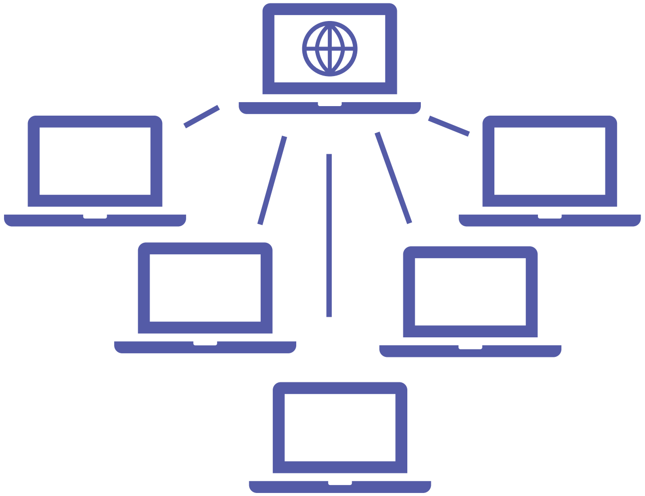
- Robot networks
  - Collection of computers able to act as one
- Once infected,
  host computer becomes a “bot”
- How does it get on your computer?
  - Trojan Horse (“Check out this attachment!”) or
    you run a program or click an ad you THOUGHT was legit
  - Exploited OS or application vulnerability
- Command and Control (C&C)
  - Bots sit and wait, phone home (C&C), see if there are any jobs given by the botmaster
    - “Ping this person”, “Spam these people”, “Visit this site”, “Do this”

Botnets

- Group of bots working together
- Distributed Denial of Service (DDoS)
  - Thousands/millions of machines acting as one
- Botnets are leased/for sale
  - Botmasters rent time on botnet
- Often used to send spam



Stop the bot



- Prevent initial infection
  - Update OS and application
  - Update anti-virus/anti-malware
- Identify an existing infection
  - Scan regularly
  - Network monitoring, abnormal traffic?
- Prevent access to Command and Control (C&C)
  - Identify with host-based firewall
  - Block host(s) at the firewall
    - CVEs will usually provide IP addresses/domain names of C&C servers to block