- Filename: eccouncil-ceh31250-v12-10-5-1-botnets.md
- Show Name: CEHv12 (312-50)
- Topic Name: Network and Perimeter Hacking: Denial of Service
- Episode Name: Botnets
  ==

Botnets

Objectives:

- Define Botnets and their attributes
- Describe what a typical botnet setup looks like
- Explain how a botnet attack network is built

- What is a botnet?

    - A dispersed group of compromised and remotely controlled systems

        - Could be any device

    - A portmanteau of roBOT + NETwork
    - Live botnet threats map: https://www.spamhaus.com/threat-map/

- What is their purpose?

    - Typically employed to do...

        - Cypto-mining
        - Attack platform for cybercrime
        - Spread malware
        - Influencing online games and polls
        - DDoS attacks

    - Affiliate Networks

        - Botnets joining forces

            - More effective

    - https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/

- How do hackers choose targets to become bots?

    - Scan networks for vulnerabilities

        - Random hits
        - Pseudo-random permutation list of IPs
        - Local Subnets

            - Already infected devices scan their local networks for other vulnerable targets

                - Infected bots can scan for internet facing targets as well

- Common ways compromised hosts download attack toolkits

    - Autonomously

        - Attacker copies it directly to target

            - Target scans for more targets and repeats the cycle

    - No intermediary source required
    - Back-Chaining

        - Attacker exploits target

            - Target then requests toolkit from Attacker

                - Repeat

    - Central Source

        - Intermediary server acts as toolkit repository for bots