- Filename: eccouncil-ceh31250-v11-7-3-1-trojans.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Trojans
  ==

Trojans

Objectives:

- Define what a Trojan is
- Describe the common indicators of a Trojan infection
- Discuss how attackers commonly employ Trojans
- List and define the common types of Trojans used by attackers
- Discuss how to create and deploy a Trojan
- List and define the common channels used by attackers to infect targets with Trojans

---

- What is a trojan and are there different types?
  - Legitimate software with a hidden malicious payload
    - RATs
    - Mobile Trojans
    - IoT/Botnet
    - Banking
    - DoS/DDoS
    - Backdoor
  - The purpose of using Trojans
    - Control over target host
      - Disable firewalls/IDS/etc
      - Install more malware
      - C2
      - Spying on users
      - Storage
    - Destruction of target host
    - DDoS
    - Theft
      - PII, PHI, Financials,
- What are the methods of deploying trojans?
  - Droppers
    - Malware that downloads trojan
  - Downloaders
    - AV safe program that downloads trojan
      - Target: Downloads and runs `media-player_1.2_installer`
      - Parrot: serving up `.sysconfig` and listening with netcat on port *9999*
  - Wrappers
    - Safe program with trojan attached
      - When safe program runs, trojan is also executed

            - Made linux trojan binary using Metasploit and freesweep (a minesweep game)
            - Parrot: `use exploit/multi/handler ; set payload linux/x64/shell/reverse_tcp`
            - Target: `sudo dpkg -i /home/billy/Downloads/freesweep.deb`
                - Check for shell
    - Crypters
        - Obfuscations to make trojan FUD
- How do trojans infect targets?
    - Email
    - Covert Channels
    - Proxy Servers
    - Removable Media (USB)
- How do trojans evade AV?
    - Splitting the file
    - Changing file extension (windows hides known extensions by default)
    - Modify the trojan and you modify the known signature
    - Encryption
    - Don't use known trojans
        - Custom malware
- How are trojans made?
    - Off-the-shelf builder
        - DarkHorse Trojan Maker
        - ProRAT
        - Senna Spy Trojan Generator
    - Custom build