- Filename: eccouncil-ceh31250-v12-7-1-1-malware-concepts-and-components.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Malware Concepts and Components ==

Malware Concepts and Components

Objectives:

- Define Malware
- List the common malware types
- Explain how malware spreads
- List and define common components that make up, or are used by Malware

---

- We hear a lot about Malware these days, but I have trouble understanding that term. Can you help me out by defining malware and how that differs from other harmful software?
  - Malware Definition
    - Umbrella term for any malicious software
  - Types of malware
    - Trojans
    - Viruses
    - Worms
    - Ransomware
    - Adware
      - PUA (Potentially Unwanted App)
    - Other PUAs
      - Spyware
      - Browser Hijacker
    - Malware Collections
      - https://github.com/abuisa/MalwareZoo
- It seems that malware does a pretty good job of spreading. Why is that? What are the methods malware use to spread?
  - Email attachments/links
  - Software installs from untrusted sources
    - Torrents
  - OS/Software vulnerabilities
- What are some of the components that are common to malware?
  - Downloaders
    - No malware
  - Droppers
    - Contains malware
  - Obfuscators and Crypters
  - Payloads
  - Exploits
- OK, so what is the purpose of malware? Are hackers just bored and looking to cause chaos, or are there more tangible reasons?
  - Chaos? Yes
  - Cyber-crime ($$MONEY$$)
    - Stealing intellectual property

    - Destruction of data
    - Spam
  - Use compromised systems for DDoS or as a 'patsy' or a pivot