Malware & Reversing

- Interesting Malware
    - Conficker.
    - Morris worm.
    - Zeus malware.
    - Stuxnet.
    - Wannacry.
    - CookieMiner.
    - Sunburst.
- Malware Features
    - Various methods of getting remote code execution.
    - Domain-flux.
    - Fast-Flux.
    - Covert C2 channels.
    - Evasion techniques (e.g. anti-sandbox).
    - Process hollowing.
    - Mutexes.
    - Multi-vector and polymorphic attacks.
    - RAT (remote access trojan) features.
- Decompiling and Reversing
    - Obfuscation of code, unique strings (you can use for identifying code).
    - IdaPro, Ghidra.
- Static and Dynamic Analysis
    - Describe the differences.
    - Virus total.
    - Reverse.it.
    - Hybrid Analysis.