Malware:MAL

This room is for the study of malware analysis

Process of malware attack
- Delivery
- Execution
- Maintaining persistence
- Propagation

Type of malware analysis
- Static analysis
- Dynamic analysis

Tools Used:
- Static:
  - Dependency Walker
  - PeID
  - PE Explorer
  - PEview
  - ResourceHacker
- Disassembly:
  - IDA Freeware
  - WinDbg
- Dynamic:
  - Debugging
    - OLLYDBG
    - ghidraRun
  - Monitoring Registry Changes
    - Regshot-Unicode
  - Network Analysis
    - apateDNS
    - Tcpview
    - Wireshark
  - Process Exploring
    - Autoruns
    - procexp64
    - Procmon64

Identifying the hash of file by md5sum
- Virustotal
- file properties
- Hashtab

Packing, Obfuscation

Tool Usage:
- PEiD : Able to identify the compiler or packer of a file
- IDA freeware : Used to disassembly and analyze the code
- Strings : To collect the ascii characters
- PE Explorer : Can analyse the file in abetter way. Able to identify the imports