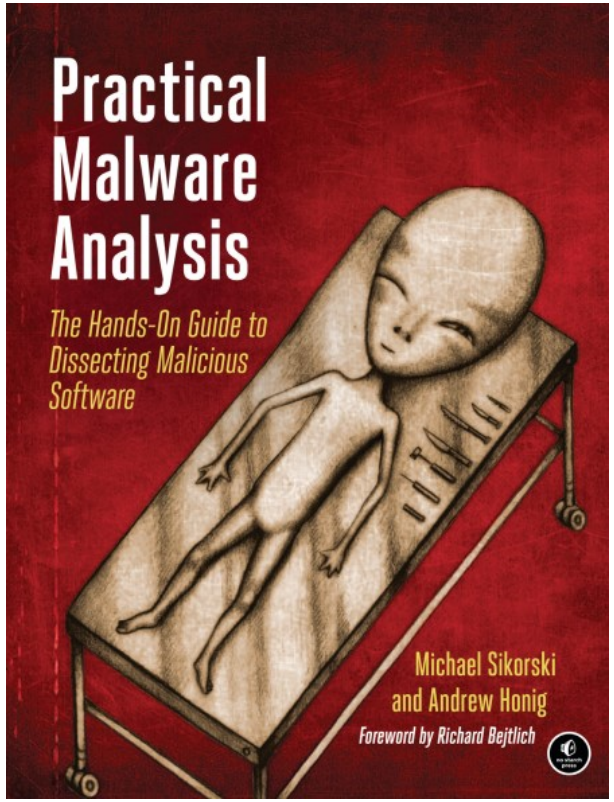
# CMT118 Malware Analysis

George Theodorakopoulos



# What is malware?

- **Mal**icious soft**ware**
- Software that harms the user, organisation, computer, network
- Virus, worm, trojan horse, rootkit, spyware, ransomware
- May steal, delete, modify information; execute actions (transfer money, open door, shut down alarm system); propagate to other computers and repeat

# Malware analysis

- Scenario:
  Malware is spreading through your organisation. You have identified the file with the malware. Your task is to find how to prevent it from spreading, stop it from delivering its payload (performing harmful actions), and find and disinfect all infected computers.
- You have to understand how it works

# Static and Dynamic Analysis

- Static analysis
  - Analyse malware without running it
  - Basic Static analysis: Do not even look at the (binary) instructions
  - Advanced Static analysis: Reverse-engineer the binary executable into assembly instructions and look at them to see exactly what the malware does
- Dynamic analysis
  - Run the malware and see what it does – **Dangerous!**
  - Basic Dynamic analysis: Run the malware and observe effects on the system
  - Advanced Dynamic analysis: Run the malware with a debugger to examine its internal state while running

# Our Focus

- Basic Static analysis
  - Strings/Icons in the file, File header, Imported libraries
  - PEView, DependencyWalker, ResourceHacker
- Basic Dynamic analysis
  - Registry/Filesystem modifications, Process creation, Network access
  - Regshot, ProcMon, FakeNet, Wireshark
- Advanced Dynamic analysis
  - How are resources (e.g. strings) used while the program is running?
  - OllyDbg

# In-class Task

- We will go through book examples and then labs
  - First for Static analysis (Ch. 1)
  - Then for Dynamic analysis (Ch. 3)
- Coursework (MA part): Apply static and dynamic tools on a piece of malware
- After CW submitted: Advanced Dynamic analysis (OllyDbg, Ch. 9)
  - We will apply OllyDbg (as well as all simpler tools from Ch.1 and Ch.3) on the CW malware