SEC 530 / CS48008 Malware Analysis and Detection

Dr. Orçun Çetin

Course Information

- https://sucourse.sabanciuniv.edu/plus/
  - All class materials will be uploaded to sucourse
  - You are responsible to check your e-mails and sucourse for announcements
- Instructor: Dr. Orçun Çetin
  - office: FENS L015
  - e-mails: orcun.cetin@sabanciuniv.edu
- TA: Recep Yıldırım
  - e-mails: recep.yildirim@sabanciuniv.edu
- Lectures: Thu 10:40-13:30 FENS L063

Course Information

Tentative Grading:

- 20% Labs
- 40% Projects & Assignments
  - 2 or 3 projects
  - Typically, group projects
  - Compose of multiple parts
- 40% Final Exam (Quite simple exam)
    - At least 20 points need to pass the exam
      - Otherwise you will get an F

Labs

- Composed of instructions that serve as hands-on exercises on course topics.
  - most of the samples are from training materials.
  - only few samples will be real malware samples.
  - Typically, done under the supervision of the instructor.
- Students are required to submit their lab results via sucourse.

Exam and Project

- Exam
  - No mid-term
- Project
  - Typically includes coding and collecting data from samples
  - Compose of multiple parts
- Assignments
  - More complex samples will be shared with students

Ethics and Cheating

- Plagiarism is not tolerated, homeworks are to be done personally
  - cooperation is not an excuse;
    - if you do not know how to cooperate, don’t do it.
- Students are assumed to agree that they will not use the knowledge they gain in this class to perform cybercrime.

Tentative Syllabus

- Introduction to Malware Analysis
  - Classification of Malware
  - Environment Setup for Safe Analysis
  - Malware Analysis in Virtual Machines
- Basic Analysis
  - Basic Static analysis
  - Basic Dynamic analysis
- Advanced Static Analysis (Reverse engineering basics)
  - Review of x86 assembly
  - Disassembly with IDA Pro & other tools
  - Recognizing C Code Constructs in Assembly
  - Analyzing Malicious Windows Programs
- Advanced Dynamic Analysis
  - Debugging with OllyDbg & x32dbg
- More hands on malware analysis practice
  - Analyzing Java Binaries and Malware
  - Analyzing .NET Malware
  - Malware Analysis with Ghidra
- Malware Functionality
  - Malware Behavior & Covert Malware Launching
  - Malware Obfuscation
- Malicious document analysis
  - PDF, docs, macros

Optional : OT malware