CRDFGLOBAL
INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

Introduction to malware analysis

Mykola **ILIN**,
Dmytro **YAKOBCHUK**,
Igor Sikorsky KPI

Course outline

Introduction to malware analysis

Basic course in modern malicious software reverse engineering, dynamic analysis and incident response to malware attacks

- BSc curriculum of 2-3 year (3-4 semester)
- Ukrainian specialty
  - 125 “Cybersecurity”
  - 113 “Applied mathematics”

Course objectives

1. Demonstrate an understanding of malware design, implementation and functions used by malicious entity to compromise system security
2. Apply methods of static, dynamic and behavioral analysis for understanding of malware algorithms
3. Use modern automatic analysis tools (sandboxes, honeypots) for analysis of malware algorithms and malicious entity behavior
4. Demonstrate an understanding of digital forensics for live malware analysis and incident response
5. Use modern threat intelligence systems for exchange of Indicators of Compromise (IoC) of targeted attacks

Learning outcomes

1. Understand malware taxonomy, common tactics and techniques according to MITRE ATT&CK
2. Perform malware analysis using static analysis tools (without running malware)
3. Analyze malware behavior using dynamic analysis tools (debugging and monitoring of active malware)
4. Extract IoC from static and dynamic analysis results, exchange IoCs with threat intelligence community using Malware Information Sharing Platform (MISP) framework
5. Understand malicious entity attack techniques using simulation of malware attack in secure environment
6. Understand malicious entity behavior using honeypot analysis techniques

Course structure

- **Lectures**
  - 8 lectures, 16 hours total
- Seminars
  - 8-16 hours
- **Laboratory assignments**
  - 8 labs, 16 hours total
- **Rating** – total 100
  - Labs 8 x 5 = 40, CTF 2 x 20 = 40, Exam 20
  - Additional points for TOP-3 places in international competitions (up to 20 points)

Course Materials

- **Syllabus**
  - syllabus.pdf (in English)
- **Lecture notes, slides**
  - slides.pdf (in Ukrainian)
- **Lab assignments, training manual**
  - main.pdf (in Ukrainian)

Tests

- **CTF1: continuous jeopardy**
  - **Time**: from first lecture to last week of semester
  - Dynamic scoring with CTFd
  - Gamified learning tasks are combined with open problems, without known solutions
  - Talent selection for R&D on higher courses
- **CTF2: king of the hill**
  - **Time**: last week of semester
  - Offensive security exercise in malware analysis defenses bypass and automation
- **Final exam**
  - Oral, questions from lecture topics and lab assignments

Course Materials

- Demonstration (in Ukrainian)
  - Lecture notes
  - Laboratory assignments

CRDFGLOBAL
INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

Instructor

Mykola ILIN

Email: m.ilin@kpi.ua

Telegram: @mykola_ilin

Threema: 2SS7EYDB

Teaching assistant

Dmytro YAKOBCHUK

Email: d.yakobchuk@kpi.ua

Threema: TADKETKX