Malware Analysis

Syllabus

1. Introduction
    - The cyber kill chain
    - Definition of malware and its role in the kill chain
    - Different types of malware
    - The goal of malware analysis
    - Types of malware analysis
    - Setting up a safe environment for malware analysis

2. Analyzing malicious Windows programs
    - The Portable Executable file format, PE header and sections
    - The Windows loader, Windows API, Import Address Table, Import functions, Export functions
    - System architecture, processes, threads, memory management, registry
    - PE files on disk and in memory

3. Basic analysis
    - Basic static analysis
        - Introducing concepts and tools for basic static analysis: hash functions, VirusTotal, strings, PEiD, PE Explorer, CFF Explorer, and Resource Hacker.
        - Identifying file obfuscation techniques: packers and cryptors.
        - Introduction to Yara.
    - Basic dynamic analysis
        - Introducing concepts and tools for basic dynamic analysis: Sysinternals tools, sandboxes.
        - Persistence techniques.
    - Network analysis
        - Faking a network for safe malware analysis.
        - Introduction to Wireshark.
        - Command and Control communication of malware.

4. Advanced analysis
    - Introduction to x86 architecture
        - Memory, instructions, opcodes, operands, registers, functions, stack.
        - The difference between source code and compiled code. Examining simple examples using different compilers.
    - Advanced static analysis
        - Introduction to disassemblers and decompilers.
        - Static code analysis with IDA/Ghidra.
        - Obfuscation techniques.
    - Advanced dynamic analysis
        - Introduction to debuggers.
        - Dynamic analysis with OllyDbg.
        - Process injection techniques and hooking.
        - User mode and kernel mode debugging.
    - Ransomware analysis
        - Cryptographic algorithms used by ransomware.
        - Cryptographic flaws in ransomware.

5. Analysis of malicious documents
    - File formats: OLE2, OOXML, RTF and PDF.
    - Malicious macro.
    - Document exploits, e.g. exploit example for Equation editor vulnerability (CVE-2017-11882).
    - Introduction to oletools.

6. Defeat malware
    - Examples of how to use the information we got during malware analysis to defend against malware attacks.
    - Threat Intelligence, IOCs.
    - Security solutions.
    - Open source tools: Yara, Snort/Suricata.

Ajánlott irodalom:

- Michael Sikorski and Andrew Honig: **Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software**. No Starch Press. ISBN: 978-1-593-27290-6
- Monnappa K A: **Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware**. Packt Publishing. ISBN: 978-1788392501
- Michael Hale Ligh, Steven Adair, Blake Hartstein and Matthew Richard: **Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code**. Wiley. ISBN: 978-0-470-61303-0
- Chris Eagle: **The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler** Second Edition. No Starch Press. ISBN: 978-1-59327-289-0