# Malware analysis

Lecture 1
Introduction

# Whoami

Dorka Palotay - dpalotay@gmail.com

- Applied Mathematics BSc at ELTE
- Security and Privacy MSc at EIT Digital (UNITN and ELTE) - Advanced Cryptography Specialization
- Threat Researcher at Sophos
- Threat Engineer at Citibank
- SOC ACD Analyst at Citibank Fusion Center
  (Security Operations Center Advance Cyber Defense)

# Topics of the course

## 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

# Topics of the course

## Analyzing malicious Windows programs

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

# Topics of the course

## 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.

# Topics of the course

## Network analysis

- Faking a network for safe malware analysis.
- Introduction to Wireshark.
- Command and Control communication of malware.

## 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.

# Topics of the course

## 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.

# Topics of the course

## Ransomware analysis

- Cryptographic algorithms used by ransomware.
- Cryptographic flaws in ransomware.

## 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.

# Topics of the course

## 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.

# Recommended readings


A. 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
B. Monnappa K A: Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing. ISBN: 978-1788392501

# Course requirements

- Create teams of three - 09.19.
- Find a research project - 09.26.
- Present your findings (20 minutes) - 12.05. and 12.12.
- Create a paper of your project - 12.12.

# Do’s and Don’ts

- Do not run malware on your computer, only in VM
- Do not reverse engineer proprietary software
- Do not hack back
- Do not distribute malware

- Create a safe malware analysis environment
- Share malware in password protected archive
- Read blogs and research papers
- Try, play, have fun

# The cyber kill chain

| | | |
|---|---|---|
| 01 | Reconnaissance | Research, identification and selection of targets. |
| 02 | Weaponization | Coupling a remote access trojan with an exploit into a deliverable payload. |
| 03 | Delivery | The adversaries convey the malware to the targeted environment (e.g. email, website, USB). |
| 04 | Exploitation | Exploiting a vulnerability to execute code on victim's system (software, hardware or human vulnerability). |
| 05 | Installation | Installing malware (remote access trojan, backdoor) on the asset, escalate privileges, maintain persistence. |
| 06 | Command & Control | Command channel for remote manipulation of victim. |
| 07 | Actions on Target | Intruders accomplish their original goals (e.g. data exfiltration, identify new targets, destruction of data). |

Lockheed-Martin Corporation-Hutchins, Cloppert, and Amin-Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains-2011

# Malware

- Malicious Software
- Any software designed to cause damage to a computer, server or computer network.
- Malicious behavior:
  - allow unauthorized access
  - stealing sensitive information
  - encrypting files
  - using system resources
  - etc.

# Types of malware

- Virus / Worm
- Trojan
- RAT - Remote Access Trojan
- Ransomware
- Botnet
- Adware
- Spyware
- Downloader / Dropper
- Rootkit
- ...

# Malware analysis

Dissecting malware in a safe and isolated environment to understand it’s behavior.

Goals:

- Respond to malware incidents
- Understand how the system was compromised
- Identify host-based and network-based IOCs (indicator of compromise)
- Remediate infection
- Prevent/detect new attacks

# Types of malware analysis

Static Analysis - examining malware without executing it

- Basic static analysis
  - quick and simple tools
  - reveal some immediate static information about the sample
  - ineffective against sophisticated malware
- Advanced static analysis
  - disassembling the binary
  - requires in-depth expertise

# Types of malware analysis

Dynamic Analysis - run the maware and monitor it’s behavior

- Basic dynamic analysis
  - reveal behavioral information, e.g.  process, file, memory, registry and network activities
- Advanced dynamic analysis
  - debugging the binary
  - requires in-depth expertise

# Setting up a safe environment

Requirements

- Host machine: Linux, Windows, MacOS
- Virtual machines: Linux and Windows
- Virtualization software:
  - VirtualBox: https://www.virtualbox.org/wiki/Downloads
    - Install VirtualBox Guest Addition
    - Save you work by creating snapshots
  - VMware
    free version: https://www.vmware.com/products/workstation-player.html (limited features, e.g. no snapshots)
    linux, windows: https://www.vmware.com/products/workstation-pro.html
    mac: https://www.vmware.com/products/fusion.html

Useful sources: https://countuponsecurity.com/2015/01/13/dynamic-malware-analysis-with-remnux-v5-part-1/
Recommended readings

# Setting up a safe environment

Virtual Machines:

- Windows VM
  - victim machine - malware executed here
  - multiple VMs can be installed (Win7, Win10)
  - no internet connection
  - dynamic analysis
  - https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
- Linux VM
  - REMnux - A Linux Toolkit for Reverse-Engineering and Analyzing Malware https://remnux.org/ https://zeltser.com/remnux-malware-analysis-tips/
  - pre-installed tools for malware analysis
  - simulate network services (DNS, HTTP)
  - static analysis

# Setting up a safe environment

- host-only network on both VMs
- REMnux - set static ip
- Windows - default gateway and DNS is set to the IP address of REMnux

DEMO TIME