Study options and time estimates

LAST REVISION DATE: 2022-05-16

Malware analysis boot camp

- ► Fundamentals of x86 platform and Windows internals
  - ► Essentials of informatics (1 class)
  - ► x86 (i386/x64) architecture and assembly (2-4 classes)
  - ► PE structure and WinAPIs (2 classes)

- ► Basic analysis of Windows malware
  - ► Writing a professional malware report (1/2 class)
  - ► Behavioural analysis (1/2 class)
  - ► Analysing malicious network activity (1 class)
  - ► 101 of Unpacking (1 class)
  - ► Handling encryption in malware (1 class)
  - ► Reversing bytecode-based threats (2 classes)
  - ► Examining malicious scripts and macros (2 classes)

Professional development

- Advanced analysis of Windows malware
  - Understanding process injections and API hooking (1 class)
  - Bypassing anti-debugging tricks (2 classes)
  - Handling exploits and shellcode (2 classes)
  - Dealing with kernel-mode threats (2 classes)

- Malware analysis for non-Windows platforms
  - Analyzing Linux and IoT threats (2 classes)
  - Introduction to Android threats (2 classes)
  - Exploring macOS malware (2 classes)

- Extras
  - Basics of digital forensics for Windows (2 classes)
  - YARA threat hunting (1 class)