Malware forensics
Endre Bangerter

The goal of this lecture is to develop an in-depth understanding of contemporary malware with a focus on malware code and its capabilities and behaviors. Students will be taught the necessary background and practical techniques to detect, identify and analyze malware.

Each session will consists of a lecture and lab parts. The labs play an important role and may require additional homework.

The course will focus on Windows malware, but many concepts apply to malware on other platforms as well.

The lecture will cover a selection (TBD) of the following topics:

- Windows OS specific background, like PE files and loading mechanisms, selected parts of the Windows API, which is used by malware.
- Malware techniques, such as code injections, hooking, root-kits.
- Memory forensics techniques to detect and analyze malware. Discussion of the limitations of memory forensics.
- Malware identification
- Malware analysis / malware reverse engineering, including static and dynamic analysis, at the code level and using so called "sandboxes".
- Binary obfuscation, protection, and anti-analysis techniques
- Infection vectors and exploits

<u>Pre-requisites:</u>

- Operating systems internals
- C and assembly basics