Malware analysis workshop

This workshop gives an introduction to memory analysis for the purposes of digital forensics and malware analysis. It relates to selected topics of Cyber Security Body of Knowledge version 1.1 (CyBOK) knowledge areas “Forensics”, “Security Operations & Incident Management”, and “Malware and Attack Technologies”[1].

The workshop intends to introduce memory analysis and related necessary topics such as data storage in memory and properties of memory-resident data. The workshop will also describe when memory analysis can provide valuable results for forensic investigations and incident response processes. The workshop begins with an introduction to the theoretical concepts and continues with a hands-on lab.

The workshop incorporates liberating structures to facilitate discussion and reflection. It is planned to allow students plenty of time for discussions with peers and reflections. The idea time for the workshop is about three hours but it can be adapted for anything between two and four hours.

The following resources are included in the workshop:

- Instructor slide deck: Contains slides that can be used as is or adapted as needed.
- Student compendium: Contains what the students need to follow the workshop; note pages for discussion and reflection sessions, lab instructions, and summary of theoretical concepts.
- Memory dump infected with the Malware Cridex
- Additional tools linked from the student compendium

The resources are available at: https://github.com/kavrestad/MalwareAnalysis.

Developed by Joakim Kävrestad at the university of Skövde - Joakim.kavrestad@his.se

---

[1] https://www.cybok.org/knowledgebase1_1/