Course Project

T-110.6220: Reverse Engineering Malware // Spring 2015

General Notes

- Project is 40% of total grade
- Deadline: 27.04.2015 23:59:59
- 4 tasks that cover different aspects of the course
  - More free form than homework
  - Focus on the reports
  - Still a clear goal for all tasks, but majority of points will be awarded based on your reports on how you reached the goal
- 1400 points total

Individual Work

- Final project is individual work
- Violation of this will be handled according to Code of Academic Integrity
  - https://into.aalto.fi/display/enregulations/Aalto+University+Code+of+Academic+Integrity+and+Handling+Violations+Thereof

Clustering (200 points)

- Given 9 samples, describe how you would cluster them into a set of 3x3
- Distinct features in each sample, no need to have a “other” cluster
- No need to do automatic clustering with algorithm xy
- Focus on the analysis of the samples at hand and the feature extraction
- Free to use whatever language/tool to automatically extract features but note that all features should be extractable with Python pefile module

Reversing I + II (300 + 200 points)

- Focus on the report, not just finding the password
- Recommended to use both static and dynamic analysis
- Reversing II: Helpful to look at the bigger picture

Volatility (700 points)

- Memory forensics using the Volatility Framework
- Given a memory dump, use Volatility to find out:
  - What kind of system is it? (OS, amount of RAM, …) (100 points)
  - How is the system infected? (200 points)
  - What is the malware doing? (200 points)
  - How is the malware trying to evade detection? (200 points)
- Focus on the report, not on worrying whether you've found everything
- Volatility Malware Command Reference https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal

Questions?

SWITCH ON FREEDOM