Intro to Malware Sample 4 (TeslaCrypt Ransomware)

Learning Objectives

- Analysis of Tesla Crypt Ransomware
- File identification
- Custom packer detection using PEStudio
- Using xdbg debugger to unpack
- Using Process Hacker to dump memory
- Analysing unpacked file using Ghidra