Intro to Malware Sample 3

Learning Objectives

- File identification (Lokibot Trojan)
- Unpacking and decompiling using Exe2Aut
- Using Ghidra Disassembler/Decompiler
- Using xdbg debugger to defeat anti-debugging
- Using xdbg debugger set breakpoints on VirtualAlloc
- Using xdbg debugger to set hardware breakpoints on memory
- Using Process Hacker to dump memory