Monash University
FIT 5124: Advanced Topics in Security
Week 11 Tutorial Sheet

Ron Steinfeld, 22 April 2015

This week we will look at malware analysis in Windows.

– Download and run a virtual machine image for Windows XP. You can download VMs from the following Microsoft web site:

  `https://www.modern.ie/en-gb/virtualization-tools#downloads`

– Analyze the malware consisting of the files `Lab12-01.exe` and `Lab12-01.dll` from Lab 12-1 (page 266) of the book 'Practical Malware Analysis' (available on Moodle) in your Windows XP virtual machine, using techniques from this week's lecture. Answer the questions from Lab 12-1.
– Investigate the anti-disassembly techniques in the malware executable `Lab15-01.exe` (available on Moodle), and answer the questions from Lab 15-1 on page 350 of the 'Practical Malware Analysis' book. You can download an evaluation or free version of the IDA disassembler from the web site:

  `https://www.hex-rays.com/products/ida/support/download.shtml`