Training Topic

*Malware Reverse*

It’s time for us to learn how bad guys actually build their bad stuff. Students will learn how we the bad guys actually build/structure their malware and make enchantment along the way. Students will learn how to malware utilize various API gadgets/scripts. By learning the arts of the malware, awareness can be raise to make the future a bit better.

Disclaimer: This is for education purpose only

Detail Training Syllabus for 2 Days:

0 - Introduction to reverse engineering tools
  * Compilers
  * Assemblers
  * Disassemblers
  * Debuggers

1 - C programming crash course
  * Introduction
  * Using MSVC Compiler
  * Variables
  * Procedure Call/Function
  * Calling Convention
  * Strings
  * Structure
  * Pointer
  * Handle
  * Dynamic Memory
  * Exercises

2 - x86 assembly programming crash course
  * Registers
  * Memory and Addressing
  * Instructions
  * Calling Convention
  * Exercises

3 - Disassembly tools
  * IDA Pro
  * Basic usage
  * Common reversing techniques
  * Rewrite simple asm functions in C
* Exercises

4 - Debugging tools
* OllyDBG
* Basic usage
* Common debugging techniques
* Exercises

Required Software:
   - https://www.visualstudio.com/downloads/

2 - IDA Freeware

3 - OllyDBG 2.0
   - http://ollydbg.de/version2.html

4 - Hiew32 Demo version
   - http://www.hiew.ru/#hiew

About Trainers – Azlam Mukhtar

Azlan Mukhtar is a Co-Founder of Eraxen PLT, a cybersecurity startup company, trying to solve malware attack problems. For the past 9 years, he was working for F-Secure, Symantec, and Blue Coat as malware analyst and reseacher fighting malware. As a reverse engineering enthusiast, he loves sharing knowledge, doing training for the communities (sometimes for free), and occasionaly participate reverse engineering challenges such as Flare-On by FireEye. Previously experience as Malware Analyst at F-Secure, Symantec, and Blue Coat.