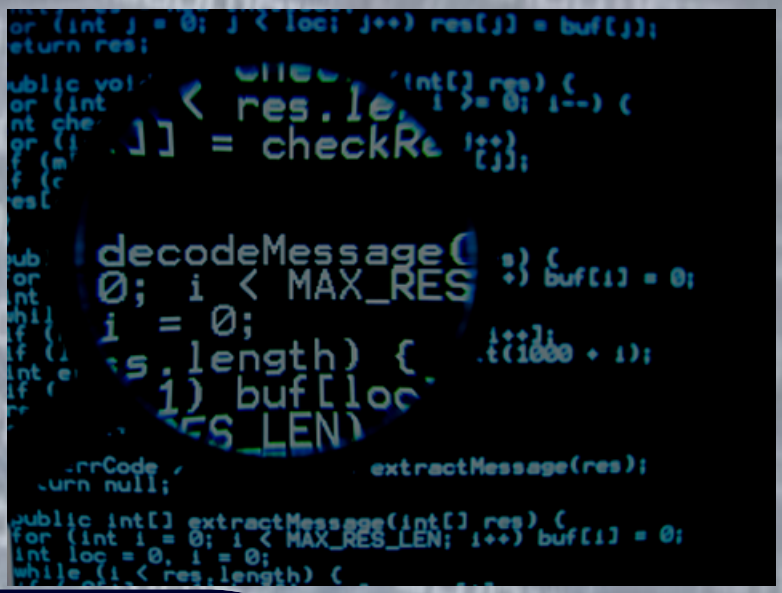
Intended Audience:

Proficient computer users who need to learn malware reverse engineering.

Individuals who desire to gain or further their reverse engineering skills.

Those who need or desire to learn how to perform in-depth capability analysis of malware.

EXPERIENCED, FOCUSED, OPERATIONAL CNO SUPPORT



Malware Capability Assessment & Reverse Engineering (MalCARE)

CSRgroup LLC

Prerequisites:

Proficiency using Windows.

Willingness to perform challenging reverse engineering labs.

Experience with C and Assembly helpful but not required.

Malware is one of the greatest threats facing computer security today but not all malware is created equal. Time spent analyzing malware means time away from conducting other mission relevant jobs. What sets the MalCARE course apart from other malware analysis courses being offered is that we teach a unique method of capability analysis via pattern recognition, allowing you to rapidly determine if the malware is a threat to your operations.

CSRgroup LLC

Phone: 410-609-3157
Fax: 410-697-3260
E-mail:inquiry@csr-group.com

CSRgroup
computer security consultants

Malware Capability Assessment & Reverse Engineering - Module Descriptions

Module 1 –Malware Reverse Engineering Methodology

In this module, students will learn a unique methodology for reverse engineering malware by thorough pattern recognition. The focus will be on rapidly determining which capabilities the malware possesses. Students will focus on rapid capability identification with a target time of one hour per malware specimen. Students will also be taught common behaviors that malware exhibits and how to rapidly identify those behaviors in disassembled code.

Module 2 – Assembly Language

Students will learn the basics of assembly language. Rather than being inundated by a multitude of different assembly instructions, students will be taught those instructions necessary to reverse engineer the code flow of most malware.

Module 3 – Tool Familiarization

Before diving head-first into malware, students will be taught the basics of **Immunity Debugger and IDA Pro**. Unlike other malware courses, this course isn't a "tool-fest" where students are inundated with multiple tools that accomplish the same tasks. This course focuses on a scriptable user mode debugger and IDA Pro for performing malware RE. After learning the basics of both tools in this module, students will be introduced to various **advanced features and plugins** throughout the hands on labs, putting these tools to use solving real-world RE problems. While a couple of other tools are used throughout the course, most of the emphasis is placed on IDA and Immunity Debugger.

Module 4 – Identifying Malware Capabilities through Reverse Engineering

Students will learn about Windows APIs and how malware authors use the APIs to write malware. This module is taught as a series of "lightning round" lectures covering a specific malware capability (i.e. registering a service). After each lecture, students gain **hands-on** experience using the tools to Reverse Engineer **real-world** malware, specifically looking at capabilities covered in the lecture. We understand that assembly language is **hard** to wrap your head around. Our instructors have Reverse Engineered the malware and provide C/C++ source code for the functions being examined. This allows students to see source code and assembly **side by side** and burns the code into the neurons for later recollection (**pattern recognition**).

Module 5 – De-Obfuscation of malware

Malware authors obfuscate their programs (using packers and cryptors) to bypass antivirus and make reverse engineering tasks more difficult. Students will study several common techniques for de-obfuscating malware so it can be analyzed using conventional reverse engineering techniques. Additionally, students will learn how to locate and defeat VMware® and debugger detection routines commonly used in malware.

Module 6 – Capstone Exercises

Students will put skills gained throughout the course to the test as they rapidly analyze malware and perform capability assessments in an instructor proctored environment. These exercises offer students an opportunity to reinforce knowledge learned during the course. All malware analyzed in the capstone is real malware found in live incident response environments.

CSRgroup
computer security consultants