11-More C Code Constructs and Malware Analysis Project

Case Statements
Disassembling Arrays
Identifying Structures
Case Statements

- Small case statements are compiled like if-then-else constructs.
- Case statements with large numbers of cases are compiled using a jump table which stores the addresses of the code for the cases in memory and jumps to the appropriate address by jumping to the location referenced by the appropriate element of the table.
- Compile a program and debug it in gcc using `stepi` to step one instruction at a time, `info registers` to see register contents, and `x/i $eip` to see the current instruction (or `x/20i $eip` to see more, i.e. 20, instructions.)
Disassembling Arrays

- Arrays stored globally are addressed more simply than arrays stored in local storage.
  - Global arrays require at most \([\text{displacement} + \text{offset register} \times \text{scalar multiplier}]\)
  - Local arrays require \([\text{base register} + \text{displacement} + \text{offset register} \times \text{scalar multiplier}]\)
Identifying Structures

- Inspection of the Code shows the offsets to the field objects contained therein.
Things for Next Time

● Chapter 7
● Read the Rovnix WriteUp