Malware Analysis (CS6038)

Week 04.1 Dynamic & Hybrid Analysis

Scott Nusbaum
nusbausa@ucmail.uc.edu

February 5, 2019

University of CINCINNATI

Overview

- Homework
- Ask Class do they want to continue with the x86 reversing?
  - Show demos of some simple compiled programs and walk through the assembly
- Dynamic Analysis
  - Definition
  - Tools
  - Demo

University of CINCINNATI

Homework

- Homework 1:
  - Due Thursday
- Homework 2:
  - Due Feb 19, 2019
  - See here for the assignment

University of CINCINNATI

Demo

- Continue the demo from last week add in
  - Mathematic operations
  - Rotation Cipher
  - Xor
  - Structures

University of CINCINNATI

Dynamic Analysis

- **Dynamic malware analysis**: Dynamic or Behavioral analysis is performed by observing the behavior of the malware while it is actually running on a host system. This form of analysis is often performed in a sandbox environment to prevent the malware from actually infecting production systems; many such sandboxes are virtual systems that can easily be rolled back to a clean state after the analysis is complete. The malware may also be debugged while running using a debugger such as GDB or WinDbg to watch the behavior and effects on the host system of the malware step by step while its instructions are being processed. Modern malware can exhibit a wide variety of evasive techniques designed to defeat dynamic analysis including testing for virtual environments or active debuggers, delaying execution of malicious payloads, or requiring some form of interactive user input [4]. WIKI

University of CINCINNATI

Dynamic Tools

- Sandboxing
- Microsoft SysInternals
- X64debug
- Ollydbg
- Windbg
- Volatility
- Regedit

University of CINCINNATI

Sandboxing

- Cuckoo Sandbox
- VirusTotal
- Hybrid Analysis
- JoeSandbox

University of CINCINNATI

Dynamic Demo

- TrickBot
  - Show procexp, procmon,
  - TcpDump

University of CINCINNATI