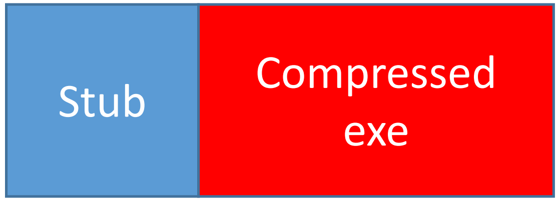
Malware Analysis Terminology

Basic Terminologies

- Packed
- Obfuscated
- Disassemblers
- Debuggers
- IOCs

Packed/Packer

- A packed malware contains part of itself compressed or encrypted



- The Stub would unpack this compressed part and then executes it either by injecting it into another process memory or runs it by itself as a separate process.

Obfuscation

- Using meaningless strings for variables
- Encodes strings in base64
- Break ups strings into multiple parts and uses some operations to concatenate them
- Used in powershell or javascript
- Malware also can be obfuscated, or, encrypted

Disassemblers

- For analyzing a file without executing it
- Known as static analysis
- Eg: Ghidra, IDA Pro
- Ghidra is also a Decompiler
- Cannot analyze memory regions

Debuggers

- Allows you to execute a program and step through it
- Examine memory regions
- Known as Dynamic Analysis
- Eg. xdbg, win dbg
- Can unpack a packed malware by dumping memory
- Behaviour Analysis

IOCs

- Indicators of Compromise
- eg:
    - File Hashes
    - File Names
    - Email Address
    - URLs
    - Dropped Files
    - Added or Modified Registry Keys

Malware Artifacts

- Items left over from malware infection
- Includes Indicators of Compromise (IOCs)

Thank you