Malware Analysis
Week 1

Joshua Reynolds

Malware Analysis Deliverables

Get answers to tough questions (fast!):

- Is this program malware?
- How could I detect this malware running on my computer?
- How could I detect if this malware ran on my computer in the past?
- How could I detect if this malware is talking over my network?
- What can this malware do?
- How does this malware evade virus detectors?
- How does this malware start running?
- What could you do to stop this malware from spreading?

Malware Analysis Tools

A reverse engineer has a toolkit of techniques you will learn:

- **Static Analysis**
  - Decompilation
  - Strings
  - Libraries
  - Symbolic Analysis
- **Dynamic Analysis**
  - Debugging
  - Concolic Execution

Because you need answers fast, you don’t actually need to learn how everything works. You can make some initial educated conclusions, and then investigate further.

“Know thine enemy” - Sun Tzu

Malware

A malicious program

Virus

A malicious program whose spread requires human help (running a program, opening a PDF, etc.)

Worm

A malicious program whose spread is automatic (like Mirai)

“Know thine enemy” - Sun Tzu

Potentially Unwanted Programs (PUPs)

Programs of dubious value, which may be annoying, but are not seriously malicious

“Know thine enemy” - Sun Tzu

Backdoor:

A program listening to the network for an attacker to remotely control the victim computer

“Know thine enemy” - Sun Tzu

Remote Access Trojan (RAT)

A subclass of backdoors which targets personal computers and often is capable of spying on or interacting with the user using the camera, microphone, and speakers. Creepy. A reason people cover their webcams.

“Know thine enemy” - Sun Tzu

Botnet:

A collection of machines with backdoors which can be controlled together to perform coordinated attacks (like DDoS)

“Know thine enemy” - Sun Tzu

Dropper/Downloader:

A program designed to download malware.

“Know thine enemy” - Sun Tzu

Cryptor:

A program designed to decrypt malicious code that has been disguised as nonsense using cryptography.

“Know thine enemy” - Sun Tzu

Keylogger or Info theft:

A program that steals information or user interactions.

“Know thine enemy” - Sun Tzu

Launcher:

A program that stealthily launches other programs, making it harder to detect that they are running. They may use tricks such as process injection to hijack an existing benign process and add a thread running malware code

“Know thine enemy” - Sun Tzu

Rootkit:

A malicious replacement or modification of a benign program, such as your operating system. Because antivirus programs are run by the operating system, a rootkit can hide from them and pretend it doesn’t exist.

“Know thine enemy” - Sun Tzu

Spam email sender

A program that sends out spam emails. IP addresses that send too many spam emails eventually get blocked, so attackers would much rather use other people’s IP addresses until they get banned.

Basis Static Analysis

Static analysis means analyzing malware *without* running it.

Such as:

- AV Scanners
- Hash Fingerprints
- String Scanning
- Binary Analysis
- Library Dependency Trees

Let’s Reverse!

Week 1 Lab 1