Practical Malware Analysis

Chapter 0: M A L W A R E A N A L Y S I S P R I M E R

Akbar Namin
Texas Tech University
Fall 2021

Reference:
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition
by Michael Sikorski (Author), Andrew Honig (Author)

What Is Malware Analysis?

- Malicious software(*malware):* Any software that does something that causes harm to a user, computer, or network can be considered malware, such as:
  - Viruses
  - trojan horses
  - worms
  - rootkits
  - Scareware
  - spyware

- Malware analysis: is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it.

The Goals of Malware Analysis

- Information required to respond to a network intrusion
  - Exactly what happened
  - Ensure you've located all infected machines and files
- How to measure and contain the damage
- Find signatures for intrusion detection systems

Signatures

- **Host-based signatures**
  - ➢ Identify files or registry keys on a victim computer that indicate an infection
  - ➢ Focus on what the malware did to the system not the malware itself
    - Different from antivirus signature

- **Network signatures**
  - ➢Detect malware by analyzing network traffic
  - ➢More effective when made using malware analysis

Malware Analysis Techniques

- **Static Analysis**
  - Examines malware without running it
  - Tools: VirusTotal, strings, a disassembler like IDAPro
- **Dynamic Analysis**
  - Run the malware and monitor its effect
  - Use a virtual machine and take snapshots
  - Tools: RegShot, Process Monitor, Process Hacker, CaptureBAT
  - RAM Analysis: Mandant Redline and Volatility

Basic Analysis

- **Basic static analysis**
  - View malware without looking at instructions
  - Tools: VirusTotal, strings
  - Quick and easy but fails for advanced malware and can miss important behavior

- **Basic dynamic analysis**
  - Easy but requires a safe test environment
  - Not effective on all malware

Advanced Analysis

- **Advanced static analysis**
  - Reverse-engineering with a disassembler
  - Complex, requires understanding of assembly code

- **Advanced Dynamic Analysis**
  - Run code in a debugger
  - Examines internal state of a running malicious executable

Types of Malware

- Backdoor
  - Allows attacker to control the system
- Botnet
  - All infected computers receive instructions from the same Command-and-Control (C&C) serve
- Downloader
  - Malicious code that exists only to download other malicious code
  - Used when attacker first gains access

Types of Malware

- Information-stealing malware
  - Sniffers, keyloggers, password hash grabbers
- Launcher
  - Malicious program used to launch other malicious programs
    - Often uses nontraditional techniques to ensure stealth or greater access to a system
- Rootkit
  - Malware that conceals the existence of other code
  - Usually paired with a backdoor

- **Scareware**

➢ Frightens user into buying something

- **Spam-sending malware**

➢ Attacker rents machine to spammers

- **Worms or viruses**

➢Malicious code that can copy itself and infect additional computers

Mass vs Targeted Malware

- Mass malware
  - Intended to infect as many machines as possible
  - Most common type

- Targeted malware
  - Tailored to a specific target
  - Very difficult to detect, prevent, and remove
  - Requires advanced analysis
  - Ex: Stuxnet

General Rules for Malware Analysis

- **Don’t Get Caught in Details**
  - ➢ You don’t need to understand 100% of the code
  - ➢ Focus on key features

- **Try Several Tools**
  - ➢ If one tool fails, try another
  - ➢ Don’t get stuck on a hard issue, move along

- **Malware authors are constantly raising the bar**