Malware Analysis Bootcamp

Learning Malware Analysis The Right Way

What is Malware?

- Malware is an executable or a binary that is malicious in nature.
- Malware is used by attackers to perform a variety of malicious actions like:
  - Spying on the target through:
    - RAT’s
    - Keyloggers
  - Data Exfiltration
  - Data encryption and destruction
    - Ransomware

Types Of Malware

Malware refers to any binary or executable that is malicious, however Malware is sorted in to further denominations based on its functionality. Here are the various types of Malware:

- Trojans - Type of malware that disguises itself as a legitimate program for social engineering purposes. It can destroy and exfiltrate data and can also be used for spying.
- RAT's - Type of malware that allows the attacker to remotely access and execute commands on the system. It's functionality can be extended with modules like keyloggers.
- Ransomware - Type of malware that encrypts all files on the system and holds the system and its data for ransom.
- Dropper - Type of malware whose purpose is to download/drop additional malware.

What Is Malware Analysis?

Malware analysis is the process of analyzing a malware sample/binary and extracting as much information as possible from it. The information we extract helps us understand the scope of the functionality of the Malware, how the system was infected with the malware and how to defend against similar attacks in the future.

Objectives of malware analysis:

- To understand the type of malware and the entire scope of what it can do (functionality). Is it a Keylogger, RAT or Ransomware.
- How the system was infected with the malware. Is it a targeted attack or a phishing attack?
- How it communicates with the attacker.
- To exfiltrate useful indicators like registry entries/keys and filenames for the purpose generating signatures that can be used to detect future detection.

Types Of Malware Analysis

- Static analysis - Is the process of analyzing malware without executing or running it. The objective is to extract as much metadata from the malware as possible. Example; strings, PE headers.
- Dynamic analysis - Is the process of executing malware and analyzing it's functionality and behaviour. The objective is to understand exactly how and what the malware does during the execution. This is done in a debugger.
- Code Analysis - Is the process of analyzing/reverse engineering assembly code. This can be both statically and dynamically done (Static and dynamic code analysis)
- Behavioural analysis - Is the process of analyzing and monitoring the malware after execution. It involves monitoring the processes, registry entries and network monitoring to determine the workings of the malware.

Next up: Setting up our environment