Malware Analysis

Malware is the concern of cyber security experts across the globe. Everyday new variants of malware emerge in the cyber world, that are more sophisticated and dangerous than their previous versions. Given to this fact the work of malware analysts is equally challenging and interesting.

As malware analysts, we have a core set of tools and techniques at our disposal for analyzing malware.

What is Malware Analysis?

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

Goal of Malware Analysis

- To understand the type of malware.
- To understand the capabilities of malware functions.
- How the system will be affected.
- How it communicates with the attacker.
- To check if it is a targeted or commodity attack
- To exfiltrate useful indicators like registry keys and filenames for the purpose of generating signatures that can be used to detect future detection

Malware Analysis Techniques

- Most often, when performing malware analysis, you'll have only the malware executable, which won't be human-readable. In order to make sense of it, you'll use a variety of tools and tricks, each revealing a small amount of information.
- You'll need to use a variety of tools in order to see the full picture.
- There are two fundamental approaches to malware analysis: **static and**
- **dynamic**.
- *Static analysis* involves examining the malware without running it.
- *Dynamic analysis* involves running the malware.
- Both techniques are further categorized as **basic or advanced.**

Basic Static Analysis

- Examining the executable file without viewing the actual instructions.
- Can confirm whether a file is malicious, provide information about its functionality, and sometimes provide information that will allow you to produce simple network signatures.
- Basic static analysis is straightforward and can be quick, but it's largely ineffective against sophisticated malware, and it can miss important behaviors.

Techniques:

- Includes running it through antivirus, analyzing strings, functions, headers.
- Websites such as VirusTotal (www.virustotal.com) allows you to upload a file for scanning using multiple antivirus engines.
- Although this could tip off the malware writers that the malware is being analyzed causing them to begin developing new and stealthier versions.
- Create an MD5 or SHA1 hash of the malware and search the hash to see if any information is available online.
- Search the executables for strings to reveal hints about functionality. It may give url or ip address, libraries used, functional and error messages.
- Legitimate programs almost always include many strings. If it has few strings, it is probably obfuscated or packed, suggesting that it may be malicious. You must unpack it to analyze.
- Don't forget to analyze the PE file to analyze which functions have been imported, exported and what type of linking is there i.e. runtime, static or dynamic.

Basic Dynamic Analysis

- Actually, runs malware to observe its behavior, understand its functionality and identify technical indicators which can be used in detection signatures, where the system is setup in a close and isolated environment.
- The lab environment is the totally isolated and if the malware is sending any network requests and is expecting a response, the response is usually simulated.
- Technical indicators revealed with basic dynamic analysis can include domain names, IP addresses, file path locations, registry keys, additional files located on the system or network.
- Additionally, it will identify communication with an attacker-controlled external server for command and control purposes or in an attempt to download additional malware files.

Techniques:

❖ Sandbox:

- A *sandbox* is a security mechanism for running untrusted programs in a safe environment without fear of harming "real" systems. Sandboxes comprise virtualized environments that often simulate network services in some fashion to ensure that the software or malware being tested will function normally.

- Such systems execute an unknown malware program in an instrumented environment and monitor their execution, used as the core of automated detection processes.

Some well-known automated sandboxes:

- Cuckoo – Open source and Automated Dynamic Malware analysis tool
- www.hybrid-analysis.com
- www.joesandbox.com

❖ ProcMon:

- Process Monitor, or procmon, is an advanced monitoring tool for Windows that provides a way to monitor certain registry, file system, network, process, and thread activity.
- It combines and enhances the functionality of two legacy tools: FileMon and RegMon.
- Procmon generates thousands and lakhs of events, so its not easy to find information. For that we have to use filter option for filtering events by Registry, File System, Process activity, and Network activity.