Malware Analysis

Abhinandan Kainth | Anuneet Anand | Mayank Rawat | Rakshit Singh | Tejas Dubhir

Motivation

Malware has always posed a threat to computer users. In recent years, malware has become more invasive and challenging to detect. There is a growing need to study the working of the malware to identify vulnerabilities in our systems and using this knowledge to make our systems resilient to their attacks.

Objective

The purpose of this study is to analyse the structure and working of key-loggers and ransomware. We aim to examine the malware with sandboxing, identify its API calls, and reverse engineer its mechanism.

Methodology

We will first start with some basic malware from *CTF challenges* and provide solutions for the same. We will follow *Practical Malware Analysis* by Sikorski, Hoing for reference. After gaining some insights and experience in reversing we will look into two specific malware types :-

- Keyloggers
- Ransomware

We will make a virtual machine sandbox for them and conduct the following:-

1. Static analysis using tools like Radare and or IDA pro.
2. The dynamic analysis which contains Network analysis via Wireshark and analysing process creation using procmon.
3. Drawing parallels between Static and Dynamic Analysis to create a reverse engineering code for the given malware binary.
4. The analysis and insights will be presented in a report

Deliverables

- Possible solutions for the CTF challenges.
- A report containing the analysis, working, decoding of the malware and the results obtained.
- Reversed Engineered Code of the respective Key-logger and Ransomware used.