UNIVERSITÀ DI PISA

Malware Analysis

for the DSS course

2024/2025

Andrea Mugnai, Jacopo Tucci

Index

1. Introduction

The purpose of this report is to provide a comprehensive analysis of the malware using different tools and techniques. The analysis will cover the following aspects:

- Static analysis
- Dynamic analysis

The main goal was to identify the malicious payload inside the APK files of the provided samples.

1.1. Tools used

During this project, we used three main analysis tools to identity the malicious behavior of the samples:

- **VirusTotal** (Antimalware Analysis)
  - It's a web tool that allows to submit samples and analyze them with several antivirus or antimalware programs
  - This tool was used to gain a starting insight on the already existing knowledge about the specific malicious sample.
- **MobSF** (Static and Dynamic analysis)
  - This tool let the analyst to automatically highlight interesting features of the application (e.g. Android permissions, API calls, remote URLs), but also to extract the Java code from the APK file. In this way we can gain a strong insight of the potential malicious behavior of the application and then manually analyze it by examining the code.
  - Moreover, it allows to perform a dynamic analysis, by executing the application inside a virtual environment and by monitoring it.
- **JD-GUI** (Java Decompilation)
  - This tool allows to decompile the Java code extracted from the APK file and to analyze it in a more user-friendly way.
  - It is useful to understand the logic behind the code and to identify potential malicious behavior.

We found that 4 out of 5 samples belong to the same malware family, **FakeBank**, which consists of trojans designed to steal sensitive banking and SMS information. The remaining sample is a ransomware disguised under the name of the popular game **Clash Royale**.