



UNIVERSITÀ DI PISA

Malware Analysis

for the DSS course

2024/2025

Andrea Mugnai, Jacopo Tucci

Index

1. Introduction	3
1.1. Tools used	3
2. FakeBank family	4
2.1. Analyzed Samples	4

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 identify 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*.

2. FakeBank family

FakeBank is an Android trojan that disguises itself as a legitimate banking application in order to steal sensitive information from the user, such as their phone number and banking credentials. It also intercepts all incoming SMS messages.

The analyzed samples are connected to multiple remote servers, to which they transmit the collected data over HTTP connections.

2.1. Analyzed Samples

During the project, we were tasked with analyzing four different variants of the **FakeBank** malware. Their SHA-256 hash values are as follows:

- b9cbe8b737a6f075d4d766d828c9a0206c6fe99c6b25b37b539678114f0abffb
- 1ef6e1a7c936d1bdc0c7fd387e071c102549e8fa0038aec2d2f4bffb7e0609c3
- 4aeccf56981a32461ed3cad5e197a3eedb97a8dfb916affc67ce4b9e75b67d98
- 191108379dccd5dc1b21c5f71f4eb5d47603fc4950255f32b1228d4b066ea512

For the sake of readability, we will refer to each sample using the first four characters of its hash.

Since the structure, behavior, Java code, and general characteristics of the four samples are largely identical (or at least very similar), we will begin by analyzing the **4aec** sample in detail. Afterwards, we will highlight the key differences found in the other three samples in comparison to this one.