Project 1 - Android Reversing

Description

This assignment is focused on the analysis of one Android application, from the two proposed. We offer two approaches as both objectives are different but still relevant to this course. Students should select one application and present a report of its analysis. The specific objectives of analyzing an application are related to identification of features, structure and other relevant findings.

The OLB Application

Location: https://play.google.com/store/apps/details?id=pt.sincelo.oliveiradobairro

This application is not malicious and will allow students to address the reversing of a common Android Application, mostly from a Application Security perspective. It refers to the Oliveira do Bairro Municipality sports facilities, providing functionality related to the use of the sports facilities.

The following aspects should be covered:

- characterization of the technologies used, as well as their versions, update status.
- characterization of the main logic blocks/processes/activities of the application, with focus on the ones responsible for data persistence, communication and authentication
- characterization of the APIs, communication methods, and message structure
- identification of potential issues, vulnerabilities and bad practices

The output should be composed of a report and a series of files, code snippets and related documentation supporting the report. If allowed by the authors, a subset of the reports may be sent to the product developers. We wish that with your knowledge we can validate the application, and find issues requiring some attention.

In the end, someone reading the report should have information about the overall structure of the application, how the main functionalities are implemented, and which potential vulnerabilities or issues are present.

The PDF Reader: File Manager

Location: PDF_Reader_File_Manager.zip

This application **is MALICIOUS** and refers to a PDF Reader, which was available in the Google Play Store until recently. It was removed together with other similar, after it was found it to be compromised. Therefore, if you wish to analyze this application, **NEVER install it in a real phone!**

The ZIP file contains the APK together with some additional files that are part of the attack chain. They are included because the original location may become offline at any moment. Start with the main APK and analyze it. If some file is not available, check if it is in the ZIP.

The following aspects should be covered:

- characterization of the main logic blocks/processes/activities of the application, with focus on the ones responsible for malicious behavior
- characterization of the APIs, communication methods, and message structure used for malicious purpose
- analysis of further payloads
- identification of potential issues and impact to users

The output should be composed of a report and a series of files, code snippets and related documentation supporting the report. If the students allow it, the reports will be made available in a public github repository. For this purpose, it is advised to use Markdown. We wish that with your knowledge we can help others that were victim of this malware.

In the end, someone reading the report should have information about the overall structure of the application, how the main malicious functionalities are implemented, what is the impact to users and to an organization, which indicators of compromise can be used (IP addresses, file hashes, domains), and what is the general operation of the attack.

Rules

The use of automated tools to scan the application is accepted. However, grading will mostly consider your work, your strategy, and your analysis, not on the raw results.

This project is expected to be authored by the students enrolled in the course. The use of existing code snippets, applications, or any other external functional element without proper acknowledgement is strictly forbidden. If any content lacking proper acknowledgment is found in other sources, the current rules regarding plagiarism will be followed.

References and tools

- Frida: https://frida.re/
- APKTool: https://ibotpeaches.github.io/Apktool/
- Android Studio: https://developer.android.com/studio
- Dex2Jar: https://github.com/pxb1988/dex2jar
- JD-Gui: https://github.com/java-decompiler/jd-gui
- OWASP ZAP: https://www.zaproxy.org/

2024

PREVIOUS

Obfuscation

NEXT

Project 2 - Suspicious Deb package

Last updated on 27 Feb 2024

(c) 2024 Me. This work is licensed under {license}

Published with Hugo Blox Builder — the free, open source website builder that empowers creators.