Lab 8: Malware family

Objective

This lab focuses on exploring a sample of real mobile malware and looking for malicious behaviors in its source code.

Table: Some examples of malware families and their behaviors.

Malware family	Malware type	Privacy stealing	SMS / CALL	Remote control	Bank stealing	Stealthy download	Ransom	Privilege escalation
ZNIU	Rooting	×	×	×				×
ROOTSTV	Exploit			×		×		×
Slocker	Ransomware						×	
XLoader	Trojan - banker	×	×	×	×	×		×

Task: Exploring malicious codes

Write a script or a program that allows you to explore each APK and automatically detect the corresponding malicious codes of their behaviors.

Feel free to write a script or program for each APK.

Submission Requirements

- The complete source code of your scripts or programs.
- A short report (max 2 pages) with:
    - A description of your implementation.
    - A sample output from analyzing an APK.