Android Malware Analysis <your surname> <your name>

*Malware Sample Analysis*

# Sample Identification (3 points)

## Hash

## Application name

## Malware name

## Main Activity screenshot

Insert here a screenshot of the main Activity

# Static Analysis (4 points)

## Package name

## Certificate ownership

## Uses permission

## Activity

## Broadcast Receiver

## Service

# Behavioral Analysis (4 points)

*Every malware belongs to a family following its goals. In this exercise, the analyst has to figure out the behavior, enumerate and describe features of the malware sample.*

*How the malware sample persist on the infected host?*

*How the malware sample interact with devices (camera, microphone, file storage, …)?*

*Please try to answer these questions and answer in the summary below.*

## Summary of behavioral analysis

# Network Activity (4 points)

*Does the malware connect to an external endpoint?*

## Command-and-Control (CnC)

## Protocol used for communication

## Data format for communication

# Open Source Intelligence (3 points)

## What relevant information can you retrieve using OSINT?

## Any ester egg?

# Attribution (1 points)

## Who are targeted by the malware?

## What hypothesis can you make about the malware author?

# Congratulation! You finish, now follow these rules

## Save this report in PDF format.

## Don’t forget to append your name to the document and archive label. (Malware\_Analysis\_Report\_<your name>)

## Compress and encrypt this report with the password: [REDACTED]

## Send it to [toufik.airane@protonmail.com](mailto:toufik.airane@protonmail.com)

# Further resources

[Android Hackers Handbook by Joshua Drake](https://www.amazon.fr/Android-Hackers-Handbook-Joshua-Drake/dp/111860864X)

[Practical Malware Analysis](https://www.amazon.fr/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901/)

# The last point is for the care of the report