Android Malware Analysis <your surname> <your name>

Malware Sample Analysis

# Sample Identification (3 points)

* Hash of the Malware
* Name of the Application
* Malware’s Family
* Screenshot of the Main Activity

Insert a picture

# Static Analysis (4 points)

* Package Name
* Certificate Ownership
* Uses Permission
* Activity
* Broadcast Receiver
* Service

# Behavioral Analysis (4 points)

Every malware is following a goal (spyware, ransomware, …). In this exercise, the analyst has to figure out the behavior of the malware by enumerating and describing each features of the sample. Ask you these questions:

* How the malware sample persist on the infected host?
* How the malware sample interact with devices (GPS, camera, microphone, file storage)?

# 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 have finished, now follow these rules:

1. Save this report in PDF format.
2. Don’t forget to append your name to the document.
3. (Malware\_Analysis\_Report\_<your name>.pdf)
4. Send it to toufik.airane@gmail.com

The last point is for the care of the report

# 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/)