Android Malware Analysis <your surname> <your name>

*Malware Sample Analysis*

# Sample Identification

* Hash:
* Application name:
* Malware signature:

# Static Analysis

* Package name:
* Certificate ownership:
* Uses permission:
* Activity:
* Broadcast Receiver:
* Service:

# Behavioral Analysis

*Every malware belongs to a family following its objective. Compared to your sample, enumerate and describe few features.*

* Enumerate and describe few characteristics:

*Does the Malware Implement Persistence? If yes, explain which technique the malware use.*

* Description of the technique used for Persistence:

*Does the Malware interact with data stocked on the device? If yes, tell us what kind of data is retrieved.*

* Kind of data accessed:

# Network Activity

*Does the malware connect to an external endpoint? If yes, provide useful information.*

* Address of the CnC:
* Protocol used for communication:
* Data format of the communication:

# Attribution

* For you, from what origin is the malware? Who targets it?

# Open Source Intelligence

* What useful information can you find about this sample?
* Any ester egg?

# Congratulation! You finish, now follow these rules:

1. Save this report in PDF format
2. Rename the document: Malware\_Analysis\_Report\_<your name>.pdf
3. Compress and encrypt this report with the password: XXXXXXXX
4. Rename the archive: Malware\_Analysis\_Report\_<your name>.zip (rar or 7z)
5. 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/)