SECURITY

Mobile SDKs - iOS & Android

1. Security SDK

The Security SDK checks the device and allows to know how secure it is to run certain applications. Constantly, the security SDK will be updated in order to avoid that its security becomes obsolete if new hacking techniques are developed in the market.

The security SDK have different functionalities and features depending on the platform used.

1.1. iOS security SDK

Four different steps are performed when the security SDK is run from iOS platform.

- **Apps en black list**: The security SDK checks if the iOS device have implemented applications whose function is to hack the device. This applications are among others: Cydia, RockApp, Icy, WinterBoard, SBSettings, MxTube, IntelliScreen, FakeCarrier, Blackra1n...
- **Use of certain directories**: The security SDK checks if the iOS device have data in directories that normally are used to hack devices. For instance: /var/lib/cydia or /var/tmp/cydia.log
- **Access to certain directories:** If any directory has more accesses than desired, the security SDK detects that the device has been hacked.
- **VPN Connection:** The security SDK detects if the iOS device is connected to a VPN connection and determine by analysing the other steps if the iOS device is hacked.

This steps have been developed to iOS 11 but they are compatible from iOS 9 to iOS 11

1.2. Android security SDK

Seven different steps are performed when the security SDK is run from Android platform.

- **Apps en black list**: The security SDK checks if the Android device have implemented applications whose function is to grant superuser permission to other malicious applications. These applications are among others:
  - SuperSU - eu.chainfire.supersu
  - Phh's superuser - me.phh.superuser
  - Kingroot - com.kingroot.kinguser
  - Magisk - com.topjohnwu.magisk

• **Use of certain directories**: The security SDK checks for the presence of files in certain directories. These files may indicate that the user has hacked the device.
The analyzed directories are:

- "/system/app/Superuser.apk"
- "/sbin/su"
- "/system/bin/su"
- "/system/xbin/su"
- "/data/local/xbin/su"
- "/data/local/bin/su"
- "/system/sd/xbin/su"
- "/system/bin/failsafe/su"
- "/data/local/su"
- "/su/bin/su"

• **Access to certain directories:** The security SDK checks the applied permission of all the applications deployed by the user, determining if any of them use dangerous permission. A list with the applications that apply this permission is returned.

• **Install applications from unknown origins:** The security SDK detects if the user has activated this option and can install external applications to Google Play.

• **Development options activated:** If this option is activated to develop applications other functionalities can be modify and consequently, the device can be hacked.

• **Debug mode activated:** If this mode is activated, the user can access to a certain functionalities of the device from the computer. This access could be used to hack the Android device.

• **Encrypted device:** The security SDK checks if the device is encrypted. In this case, the device's security increases and it is more difficult to hack it.

• **VPN Connection:** The security SDK detects if the Android device is connected to a VPN connection and determine by analysing the other steps if the Android device is hacked.

This steps are compatible from Android 4.0 onwards