**INTENTS**

**SEND\_SMS Intent**: This intent allows apps to send SMS messages. Malicious apps can use this to send premium rate SMS messages without the user's consent, leading to unexpected charges.

**DIAL Intent:** This intent can be used to initiate a phone call. Malicious apps may use it to make calls without the user's knowledge or permission, potentially leading to unwanted phone charges.

**SEND\_EMAIL Intent**: While this intent is generally used to launch email applications, malicious apps might exploit it to send unauthorized emails or spam.

**READ\_SMS and READ\_CONTACTS Intent**: These intents allow apps to access SMS messages and contact information. Malicious apps can abuse these intents to steal sensitive user data.

**WRITE\_EXTERNAL\_STORAGE and READ\_EXTERNAL\_STORAGE Intent:** These intents grant apps access to external storage, including the SD card. Malicious apps can misuse them to steal, modify, or delete user files.

**RECEIVE\_BOOT\_COMPLETED Intent**: Apps can register to receive this intent to execute code when the device boots up. Malicious apps can use this to start in the background and perform harmful actions without user interaction.

**PACKAGE\_ADDED and PACKAGE\_REPLACED Intent**: These intents are broadcasted when an app is installed or replaced. Malicious apps may monitor these events to track app installations and potentially interfere with legitimate app installations.

**ACTION\_SHUTDOWN Intent**: This intent is sent when the device is shutting down. Malicious apps can register to receive this intent to perform actions before the device powers off, potentially causing data loss or instability.

**ACTION\_SCREEN\_ON and ACTION\_SCREEN\_OFF Intent**: These intents can be used to monitor the device's screen state. Malicious apps may use them to track when the device is in use or idle, which can raise privacy concerns.

**ACTION\_USER\_PRESENT Intent**: This intent is sent when the user unlocks the device. Malicious apps can use it to perform actions when the user unlocks their device.

**ACTION\_POWER\_CONNECTED and ACTION\_POWER\_DISCONNECTED Intent**: These intents are sent when the device is connected or disconnected from a power source. Malicious apps might use them to perform actions when the device is charging.

**ACTION\_HEADSET\_PLUG Intent**: This intent is sent when a headset is plugged in or removed. Malicious apps can listen for these events to perform actions related to audio playback or recording.

**android.intent.action.NOTIFY** - To receive notifications

**BIND\_NOTIFICATION\_LISTENER\_SERVICE** - To access details of the notifications

c