Foreground Persistence, Technique T1541 - Mobile

Archived: 2026-04-05 15:02:30 UTC

Adversaries may abuse Android's `startForeground()` API method to maintain continuous sensor access. Beginning in Android 9, idle applications running in the background no longer have access to device sensors, such as the camera, microphone, and gyroscope.[1] Applications can retain sensor access by running in the foreground, using Android's `startForeground()` API method. This informs the system that the user is actively interacting with the application, and it should not be killed. The only requirement to start a foreground service is showing a persistent notification to the user.[2]

Malicious applications may abuse the `startForeground()` API method to continue running in the foreground, while presenting a notification to the user pretending to be a genuine application. This would allow unhindered access to the device's sensors, assuming permission has been previously granted.[3]

Malicious applications may also abuse the `startForeground()` API to inform the Android system that the user is actively interacting with the application, thus preventing it from being killed by the low memory killer.[4]

Source: https://attack.mitre.org/techniques/T1541