Protected User Data, Technique T1636 - Mobile

Archived: 2026-04-05 15:44:33 UTC

Adversaries may utilize standard operating system APIs to collect data from permission-backed data stores on a device, such as the calendar or contact list. These permissions need to be declared ahead of time. On Android, they must be included in the application's manifest. On iOS, they must be included in the application's `Info.plist` file.

In almost all cases, the user is required to grant access to the data store that the application is trying to access. In recent OS versions, vendors have introduced additional privacy controls for users, such as the ability to grant permission to an application only while the application is being actively used by the user.

If the device has been jailbroken or rooted, an adversary may be able to access Protected User Data without the user's knowledge or approval.

Source: https://attack.mitre.org/techniques/T1636