Remote Access Software, Technique T1663 - Mobile

Archived: 2026-04-05 14:50:17 UTC

Adversaries may use legitimate remote access software, such as `VNC`, `TeamViewer`, `AirDroid`, `AirMirror`, etc., to establish an interactive command and control channel to target mobile devices.

Remote access applications may be installed and used post-compromise as an alternate communication channel for redundant access or as a way to establish an interactive remote session with the target device. They may also be used as a component of malware to establish a reverse connection to an adversary-controlled system or service. Installation of remote access tools may also include persistence.

Source: https://attack.mitre.org/techniques/T1663