Data Manipulation: Transmitted Data Manipulation, Sub-technique T1641.001 - Mobile

Archived: 2026-04-05 12:43:35 UTC

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity. By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity to deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system, typically gained through a prolonged information gathering campaign, in order to have the desired impact.

One method to achieve Transmitted Data Manipulation is by modifying the contents of the device clipboard. Malicious applications may monitor clipboard activity through the `ClipboardManager.OnPrimaryClipChangedListener` interface on Android to determine when clipboard contents have changed. Listening to clipboard activity, reading clipboard contents, and modifying clipboard contents requires no explicit application permissions and can be performed by applications running in the background. However, this behavior has changed with the release of Android 10.

Adversaries may use Transmitted Data Manipulation to replace text prior to being pasted. For example, replacing a copied Bitcoin wallet address with a wallet address that is under adversarial control.

Transmitted Data Manipulation was seen within the Android/Clipper.C trojan. This sample was detected by ESET in an application distributed through the Google Play Store targeting cryptocurrency wallet numbers.[1]

Source: https://attack.mitre.org/techniques/T1641/001