Impact, Tactic TA0034 - Mobile

Archived: 2026-04-05 18:42:45 UTC

The adversary is trying to manipulate, interrupt, or destroy your devices and data.

The impact tactic consists of techniques used by the adversary to execute his or her mission objectives but that do not cleanly fit into another category such as Collection. Mission objectives vary based on each adversary's goals, but examples include toll fraud, destruction of device data, or locking the user out of his or her device until a ransom is paid.

ID: TA0034

Created: 17 October 2018

Last Modified: 25 April 2025

Techniques

Techniques: 10

ID	Name	Description
T1640	Account Access Removal	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: credentials changed) to remove access to accounts.
T1616	Call Control	Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.
T1662	Data Destruction	Adversaries may destroy data and files on specific devices or in large numbers to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.
T1471	Data Encrypted for Impact	An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

ID	Name	Description
T1641	Data Manipulation	Adversaries may insert, delete, or alter data in order to manipulate external outcomes or hide activity. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.
.001	Transmitted Data Manipulation	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.
T1642	Endpoint Denial of Service	Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.
T1643	Generate Traffic from Victim	Adversaries may generate outbound traffic from devices. This is typically performed to manipulate external outcomes, such as to achieve carrier billing fraud or to manipulate app store rankings or ratings. Outbound traffic is typically generated as SMS messages or general web traffic, but may take other forms as well.
T1516	Input Injection	A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.
T1464	Network Denial of Service	Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth that services rely on, or by jamming the signal going to or coming from devices.
T1582	SMS Control	Adversaries may delete, alter, or send SMS messages without user authorization. This could be used to hide C2 SMS messages, spread malware, or various external effects.

Source: https://attack.mitre.org/tactics/TA0034