

Data Destruction, Technique T1662 - Mobile

Archived: 2026-04-05 18:37:42 UTC

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.

To achieve data destruction, adversaries may use the `pm uninstall` command to uninstall packages or the `rm` command to remove specific files. For example, adversaries may first use `pm uninstall` to uninstall non-system apps, and then use `rm (-f) <file(s)>` to delete specific files, further hiding malicious activity.^{[1][2]}

Source: <https://attack.mitre.org/techniques/T1662>