Dvmap, Software S0420 | MITRE ATT&CK®

Archived: 2026-04-05 16:20:24 UTC

Domain	ID		Name	Use
Mobile	T1407		Download New Code at Runtime	Dvmap can download code and binaries from the C2 server to execute on the device as root.[1]
Mobile	T1404		Exploitation for Privilege Escalation	Dvmap attempts to gain root access by using local exploits.[1]
Mobile	T1625	.001	Hijack Execution Flow: System Runtime API Hijacking	Dvmap replaces `/system/bin/ip` with a malicious version. Dvmap can inject code by patching `libdmv.so` or `libandroid_runtime.so`, depending on the Android OS version. Both libraries are related to the Dalvik and ART runtime environments. The patched functions can only call `/system/bin/ip`, which was replaced with the malicious version.[1]
Mobile	T1629	.003	Impair Defenses: Disable or Modify Tools	Dvmap can turn off `VerifyApps`, and can grant Device Administrator permissions via commands only, rather than using the UI.[1]
Mobile	T1406		Obfuscated Files or Information	Dvmap decrypts executables from archive files stored in the `assets` directory of the installation binary.[1]
Mobile	T1632	.001	Subvert Trust Controls: Code Signing Policy Modification	Dvmap can enable installation of apps from unknown sources.[1]
Mobile	T1426		System Information Discovery	Dvmap checks the Android version to determine which system library to patch.[1]

Source: https://attack.mitre.org/software/S0420