BrainTest, Software S0293 | MITRE ATT&CK®

Archived: 2026-04-05 14:06:04 UTC

Domain	ID	Name	Use
Mobile	T1645	Compromise Client Software Binary	BrainTest uses root privileges (if available) to copy an additional Android app package (APK) to /system/priv-app to maintain persistence even after a factory reset.[2]
Mobile	T1407	Download New Code at Runtime	Original samples of BrainTest download their exploit packs for rooting from a remote server after installation.[2]
Mobile	T1404	Exploitation for Privilege Escalation	Some original variants of BrainTest had the capability to automatically root some devices, but that behavior was not observed in later samples.[2]
Mobile	T1643	Generate Traffic from Victim	BrainTest provided capabilities that allowed developers to use compromised devices to post positive reviews on their own malicious applications as well as download other malicious applications they had submitted to the Play Store.[2]
Mobile	T1406	Obfuscated Files or Information	BrainTest stores a secondary Android app package (APK) in its assets directory in encrypted form, and decrypts the payload at runtime.[2]