TriangleDB, Software S1216 | MITRE ATT&CK®

Archived: 2026-04-05 16:55:00 UTC

Domain	ID		Name	Use
Mobile	T1634	.001	Credentials from Password Store: Keychain	TriangleDB has extracted the device's keychain.[1]
Mobile	T1533		Data from Local System	TriangleDB has collected and exfiltrated files.[1]
Mobile	T1521	.001	Encrypted Channel: Symmetric Cryptography	TriangleDB has encrypted data using 3DES.[1]
		.002	Encrypted Channel: Asymmetric Cryptography	TriangleDB has encrypted data using RSA.[1]
Mobile	T1420		File and Directory Discovery	TriangleDB has obtained a list of files using the `fts` API and has obtained files that match a specified regular expression.[1]
Mobile	T1630	.002	Indicator Removal on Host: File Deletion	TriangleDB has deleted an implant module or specified files.[1]
Mobile	T1544		Ingress Tool Transfer	TriangleDB has loaded additional modules stored in memory.[1]
Mobile	T1430		Location Tracking	TriangleDB has monitored the device's geolocation, which includes coordinates, altitude, bearing and speed.[1]
Mobile	T1644		Out of Band Data	TriangleDB has used the Protobuf library for command and control communication.[1]

Domain	ID	Name	Use
Mobile	T1424	Process Discovery	TriangleDB has collected a list of running processes.[1]
Mobile	T1418	Software Discovery	TriangleDB has obtained a list of installed applications.[1]
Mobile	T1422	System Network Configuration Discovery	TriangleDB has collected and sent information on the device's IMEI, MEID, serial number and other device information.[1]
