FakeSpy, Software S0509 | MITRE ATT&CK®

Archived: 2026-04-05 13:56:44 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	FakeSpy exfiltrates data using HTTP requests. [1]
Mobile	T1624	.001	Event Triggered Execution: Broadcast Receivers	FakeSpy can register for the `BOOT_COMPLETED` broadcast Intent.[1]
Mobile	T1628	.001	Hide Artifacts: Suppress Application Icon	FakeSpy can hide its icon if it detects that it is being run on an emulator.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	FakeSpy masquerades as local postal service applications.[1]
Mobile	T1406		Obfuscated Files or Information	FakeSpy stores its malicious code in encrypted asset files that are decrypted at runtime. Newer versions of FakeSpy encrypt the C2 address.[1]
Mobile	T1636	.003	Protected User Data: Contact List	FakeSpy can collect the device's contact list. [1]
		.004	Protected User Data: SMS Messages	FakeSpy can collect SMS messages.[1]
Mobile	T1582		SMS Control	FakeSpy can send SMS messages.[1]
Mobile	T1418		Software Discovery	FakeSpy can collect a list of installed applications.[1]

Domain	ID		Name	Use
Mobile	T1409		Stored Application Data	FakeSpy can collect account information stored on the device, as well as data in external storage.[1]
Mobile	T1426		System Information Discovery	FakeSpy can collect device information, including OS version and device model.[1]
Mobile	T1422		System Network Configuration Discovery	FakeSpy can collect device networking information, including phone number, IMEI, and IMSI.[1]
		.001	Internet Connection Discovery	FakeSpy can collect device networking information, including phone number, IMEI, and IMSI.[1]
Mobile	T1421		System Network Connections Discovery	FakeSpy can collect the device's network information.[1]
Mobile	T1633	.001	Virtualization/Sandbox Evasion: System Checks	FakeSpy can detect if it is running in an emulator and adjust its behavior accordingly. [1]

Source: https://attack.mitre.org/software/S0509