S.O.V.A., Software S1062 | MITRE ATT&CK®

Archived: 2026-04-02 12:31:05 UTC

Domain	ID		Name	Use
Mobile	T1517		Access Notifications	S.O.V.A. can silently intercept and manipulate notifications. S.O.V.A. can also inject cookies via push notifications.[1]
Mobile	T1638		Adversary-in-the-Middle	S.O.V.A. has included adversary-in-the-middle capabilities.[1]
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	S.O.V.A. can use the open-source project RetroFit for C2 communication.[1]
Mobile	T1471		Data Encrypted for Impact	S.O.V.A. has code to encrypt device data with AES.[2]
Mobile	T1641	.001	Data Manipulation: Transmitted Data Manipulation	S.O.V.A. can manipulate clipboard data to replace cryptocurrency addresses.[1]
Mobile	T1628	.001	Hide Artifacts: Suppress Application Icon	S.O.V.A. can hide its application icon.[1]
Mobile	T1629	.001	Impair Defenses: Prevent Application Removal	S.O.V.A. can resist removal by going to the home screen during uninstall.[1]
Mobile	T1630	.001	Indicator Removal on Host: Uninstall Malicious Application	S.O.V.A. can uninstall itself.[1]
Mobile	T1417	.001	Input Capture: Keylogging	S.O.V.A. can use keylogging to capture user input.[1]

Domain	ID		Name	Use
		.002	Input Capture: GUI Input Capture	S.O.V.A. can use overlays capture banking credentials and credit card information, and can open arbitrary WebViews from the C2.[1]
Mobile	T1516		Input Injection	S.O.V.A. can programmatically tap the screen or swipe.[2]
Mobile	T1464		Network Denial of Service	S.O.V.A. has C2 commands to add an infected device to a DDoS pool.[1]
Mobile	T1406	.002	Obfuscated Files or Information: Software Packing	S.O.V.A. has been distributed in obfuscated and packed form.[1]
Mobile	T1636	.004	Protected User Data: SMS Messages	S.O.V.A. can intercept and read SMS messages.[1]
Mobile	T1513		Screen Capture	S.O.V.A. can take screenshots and abuse the Android Screen Cast feature to capture screen data.[2]
Mobile	T1582		SMS Control	S.O.V.A. can send SMS messages.[1]
Mobile	T1418		Software Discovery	S.O.V.A. can search for installed applications that match a list of targets.[2]
Mobile	T1409		Stored Application Data	S.O.V.A. can gather session cookies from infected devices. S.O.V.A. can also abuse Accessibility Services to steal Google Authenticator tokens.[1] [2]
Mobile	T1426		System Information Discovery	S.O.V.A. can gather data about the device.[1]

Source: https://attack.mitre.org/software/S1062