Asacub, Software S0540 | MITRE ATT&CK®

Archived: 2026-04-05 13:20:55 UTC

Domain	ID		Name	Use
Mobile	T1626	.001	Abuse Elevation Control Mechanism: Device Administrator Permissions	Asacub can request device administrator permissions.[1]
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	Asacub has communicated with the C2 using HTTP POST requests.[1]
Mobile	T1532		Archive Collected Data	Asacub has encrypted C2 communications using Base64-encoded RC4.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	Asacub has masqueraded as a client of popular free ads services.[1]
Mobile	T1575		Native API	Asacub has implemented functions in native code.[1]
Mobile	T1406		Obfuscated Files or Information	Asacub has stored encrypted strings in the APK file.[1]
Mobile	T1636	.003	Protected User Data: Contact List	Asacub can collect the device’s contact list.[1]
		.004	Protected User Data: SMS Messages	Asacub can collect SMS messages as they are received.[1]
Mobile	T1582		SMS Control	Asacub can send SMS messages from compromised devices.[1]

Domain	ID		Name	Use
Mobile	T1426		System Information Discovery	Asacub can collect various pieces of device information, including device model and OS version.[1]
Mobile	T1422		System Network Configuration Discovery	Asacub can collect various pieces of device network configuration information, such as mobile network operator.[1]
		.001	Internet Connection Discovery	Asacub can collect various pieces of device network configuration information, such as mobile network operator.[1]