Exobot, Software S0522 | MITRE ATT&CK®

Archived: 2026-04-05 15:11:25 UTC

Domain	ID		Name	Use
Mobile	T1626	.001	Abuse Elevation Control Mechanism: Device Administrator Permissions	Exobot can request device administrator permissions.[1]
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	Exobot has used HTTPS for C2 communication.[1]
Mobile	T1642		Endpoint Denial of Service	Exobot can lock the device with a password and permanently disable the screen.[1]
Mobile	T1624	.001	Event Triggered Execution: Broadcast Receivers	Exobot has registered to receive the `BOOT_COMPLETED` broadcast intent.[1]
Mobile	T1417	.001	Input Capture: Keylogging	Exobot has used web injects to capture users' credentials.[1]
		.002	Input Capture: GUI Input Capture	Exobot can show phishing popups when a targeted application is running.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	Exobot has used names like WhatsApp and Netflix.[1]
Mobile	T1636	.003	Protected User Data: Contact List	Exobot can access the device's contact list.[1]
		.004	Protected User Data: SMS Messages	Exobot can intercept SMS messages.[1]

Domain	ID		Name	Use
Mobile	T1604		Proxy Through Victim	Exobot can open a SOCKS proxy connection through the compromised device.[1]
Mobile	T1582		SMS Control	Exobot can forward SMS messages.[1]
Mobile	T1418	.001	Software Discovery: Security Software Discovery	Exobot can obtain a list of installed applications and can detect if an antivirus application is running, and close it if it is.[1]
Mobile	T1426		System Information Discovery	Exobot can obtain the device's country and carrier name.[1]
Mobile	T1422		System Network Configuration Discovery	Exobot can obtain the device's IMEI, phone number, and IP address.[1]
		.001	Internet Connection Discovery	Exobot can obtain the device's IMEI, phone number, and IP address.[1]

Source: https://attack.mitre.org/software/S0522/