Cerberus, Software S0480 | MITRE ATT&CK®

Archived: 2026-04-05 13:22:00 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	Cerberus communicates with the C2 server using HTTP.[2]
Mobile	T1407		Download New Code at Runtime	Cerberus can update the malicious payload module on command.[1]
Mobile	T1628	.001	Hide Artifacts: Suppress Application Icon	Cerberus hides its icon from the application drawer after being launched for the first time.[1]
Mobile	T1629	.003	Impair Defenses: Disable or Modify Tools	Cerberus disables Google Play Protect to prevent its discovery and deletion in the future.[1]
Mobile	T1630	.001	Indicator Removal on Host: Uninstall Malicious Application	Cerberus can uninstall itself from a device on command.[1]
Mobile	T1417	.001	Input Capture: Keylogging	Cerberus can record keystrokes.[1]
		.002	Input Capture: GUI Input Capture	Cerberus can generate fake notifications and launch overlay attacks against attacker-specified applications.[1]
Mobile	T1516		Input Injection	Cerberus can inject input to grant itself additional permissions without user interaction and to prevent application removal.[1][2]

Domain	ID		Name	Use
Mobile	T1430		Location Tracking	Cerberus can collect the device's location.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	Cerberus has pretended to be an Adobe Flash Player installer.[3]
Mobile	T1509		Non-Standard Port	Cerberus communicates with the C2 using HTTP requests over port 8888.[2]
Mobile	T1406		Obfuscated Files or Information	Cerberus uses standard payload and string obfuscation techniques.[1]
Mobile	T1636	.003	Protected User Data: Contact List	Cerberus can obtain the device's contact list.[1]
		.004	Protected User Data: SMS Messages	Cerberus can collect SMS messages from a device.[1]
Mobile	T1582		SMS Control	Cerberus can send SMS messages from a device.[1]
Mobile	T1418		Software Discovery	Cerberus can obtain a list of installed applications.[1]
Mobile	T1426		System Information Discovery	Cerberus can collect device information, such as the default SMS app and device locale.[1][2]
Mobile	T1633	.001	Virtualization/Sandbox Evasion: System Checks	Cerberus avoids being analyzed by only activating the malware after recording a

Domain	ID		Name	Use
				certain number of steps from the accelerometer.[1]

Source: https://attack.mitre.org/software/S0480