CHEMISTGAMES, Software S0555 | MITRE ATT&CK®

Archived: 2026-04-05 16:33:32 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	CHEMISTGAMES has used HTTPS for C2 communication.[1]
Mobile	T1623	.001	Command and Scripting Interpreter: Unix Shell	CHEMISTGAMES can run bash commands.[1]
Mobile	T1533		Data from Local System	CHEMISTGAMES can collect files from the filesystem and account information from Google Chrome.[1]
Mobile	T1407		Download New Code at Runtime	CHEMISTGAMES can download new modules while running.[1]
Mobile	T1521	.002	Encrypted Channel: Asymmetric Cryptography	CHEMISTGAMES has used HTTPS for C2 communication.[1]
Mobile	T1430		Location Tracking	CHEMISTGAMES has collected the device's location.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	CHEMISTGAMES has masqueraded as popular South Korean applications.[1]
Mobile	T1575		Native API	CHEMISTGAMES has utilized native code to decrypt its malicious payload.[1]

Domain	ID		Name	Use
Mobile	T1406		Obfuscated Files or Information	CHEMISTGAMES has encrypted its DEX payload. [1]
Mobile	T1474	.003	Supply Chain Compromise: Compromise Software Supply Chain	CHEMISTGAMES has been distributed as updates to legitimate applications. This was accomplished by compromising legitimate app developers, and subsequently gaining access to their Google Play Store developer account.[1]
Mobile	T1426		System Information Discovery	CHEMISTGAMES has fingerprinted devices to uniquely identify them.[1]
