Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:43:22 UTC

Tool: Scotch

Names	Scotch
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Downloader
Description	(Citizen Lab) The ultimate spyware tool deployed by MOONSHINE, Scotch, is a modular Java application which uses the WebSocket protocol to communicate with its C2 server. The Scotch payload itself has limited espionage features, such as obtaining device information and uploading files from the infected device. However, as part of its initial contact with the C2, Scotch downloads additional plugins. During our analysis, we were able to acquire two plugin packages, named “Bourbon.jar” and “IceCube.jar” which added functionality including exfiltrating SMS text messages, address books, and call logs, and spying on the target through their phone’s camera, microphone, and GPS.
Information	<https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Scotch

Changed	Name	Country	Observed	
APT groups				
	Poison Carp, Evil Eye		2018-Jun 2023	

1 group listed (1 APT, 0 other, 0 unknown)