

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:26:51 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool DroidJack

Tool: DroidJack

Names	DroidJack
Category	Malware
Type	Backdoor
Description	DroidJack is an Android remote access tool that has been observed posing as legitimate applications including the Super Mario Run and Pokemon GO games.
Information	< https://www.fortinet.com/blog/threat-research/analyzing-android-malware-using-a-fortisandbox.html > < https://www.stratosphereips.org/blog/2021/1/22/analysis-of-droidjack-v44-rat-network-traffic >
MITRE ATT&CK	< https://attack.mitre.org/software/S0320/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidjack >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:droidjack >

Last change to this tool card: 29 December 2022

Download this tool card in [JSON](#) format

All groups using tool DroidJack

Changed	Name	Country	Observed
APT groups			
	Group5		2015
	↳ Subgroup: Pat Bear, APT-C-37		2015

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.eta-da.or.th/cgi-bin/listgroups.cgi?u=f830ab0f-1edc-4f98-9a38-ccc57909215c>