Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:39:09 UTC

Tool: KevDroid

Names	KevDroid
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Talos) Variant 1: The purpose of the application is to steal information stored on the device. Here is the list of stolen information: • Installed applications • Phone number • Phone Unique ID • Location (the application tries to switch on the GPS), this information is collected every 10 seconds, which is aggressive for this kind of spying tool • Stored contacts information (name, phone numbers, emails, photos, etc.) • Stored SMS • Call logs • Stored emails • Photos • Recording calls Variant 2: The variant contains the same features than the previous version with some additional: • Camera recording • Audio recording • Web history stealing • File stealing • Root access on the device
Information	<https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.kevdroid>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:KevDroid>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool KevDroid

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=322aa827-1bf8-4d95-b773-dc6488aea1b8