Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:36 UTC

Tool: Rana

Names	Rana
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(ReversingLabs) In today's world, the most valuable source of such information are smartphones. You carry a smartphone almost the entire time, and, besides being the main tool for everyday communication, smartphones also provide a large set of secondary functionalities, including visual and audio recording and location services. Because of all these capabilities, gaining control over someone's smartphone provides the malicious actor with a powerful espionage tool. For these reasons, we decided to take a better look at the information and IOCs provided in the referenced report to see if there is anything more to be found about this Android malware.
Information	<https://blog.reversinglabs.com/blog/rana-android-malware>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.rana>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Rana

Changed	Name	Country	Observed	
APT groups				
	Chafer, APT 39		2014-Sep 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3292c11b-11db-4b78-8347-c6f341127ff1