Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:58:49 UTC

Tool: Android RAT

Names	Android RAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Kaspersky) The first application on the list that is not installed on the system will be selected as the target application. The malware embeds multiple APK files, which are stored in a directory named “assets”. The analyzed sample includes the following packages: apk a20fc273a49c3b882845ac8d6cc5beac apk 53cd72147b0ef6bf6e64d266bf3ccafe apk bae69f2ce9f002a11238dcf29101c14f apk b8006e986453a6f25fd94db6b7114ac2 apk 4556ccecbf24b2e3e07d3856f42c7072 apk 6c3308cd8a060327d841626a677a0549 The selected APK is copied to /.System/APK/. By default, the application tries to save the file to external storage, otherwise it saves it to the data directory. Finally, the application tries to install the copied APK. The final malware is a modified version of the AhMyth Android RAT, open-source malware downloadable from GitHub, which is built by binding the malicious payload inside other legitimate applications. Basically, it provides the following features: • camera manager (list devices and steal screenshots) • file manager (enumerate files and upload these to the C2) • SMS manager (get a list of text messages or send a text) • get the call log • get the contact list • microphone manager • location manager (track the device location) The RAT that we analyzed is slightly different from the original. It includes new features added by the attackers to improve data exfiltration, whereas some of the core features, such as

	the ability to steal pictures from the camera, are missing.
Information	<https://securelist.com/transparent-tribe-part-2/98233/>

Last change to this tool card: 27 August 2020

Download this tool card in JSON format

All groups using tool Android RAT

Changed	Name	Country	Observed	
APT groups				
	Transparent Tribe, APT 36		2013-Mar 2025	

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