Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:16:31 UTC

Tool: AndroRAT

Names	AndroRAT
Category	Tools
Type	Backdoor
Description	(Trend Micro) RATs have long been a common Windows threat, so it shouldn't be a surprise that it has come to Android. A RAT has to gain root access — usually by exploiting a vulnerability — in order to have control over a system. Discovered in 2012, the original authors intended AndroRAT — initially a university project — as an open-source client/server application that can provide remote control of an Android system, which naturally attracted cybercriminals.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/new-androrat-exploits-dated-permanent-rooting-vulnerability-allows-privilege-escalation/> <https://github.com/DesignativeDave/androrat>
MITRE ATT&CK	<https://attack.mitre.org/software/S0292/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.androrat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:androrat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool AndroRAT

Changed	Name	Country	Observed	
APT groups				
	Patchwork, Dropping Elephant		2013-Jun 2025	

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