Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:05:28 UTC

Tool: SandroRAT

Names	SandroRAT
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(McAfee) Just as any other Android RAT (such as AndroRAT), the malware can remotely execute several commands to perform any of the following actions: • Steal sensitive personal information such as contact list, SMS messages (inbox, outbox, and sent), call logs (incoming, outgoing, and missed calls), browser history (title, link, date), bookmarks and GPS location (latitude and longitude). • Intercept incoming calls and record those in a WAV file on the SD card to later leak the file. • Update itself (or install additional malware) by downloading and prompting the user to install the file update.apk. • Intercept, block, and steal incoming SMS messages. • Send MMS messages with parameters (phone number and text) provided by the control server. • Insert and delete SMS messages and contacts. • Record surrounding sound and store it in an adaptive multi-rate file on the SD card to later send to a remote server. • Open the dialer with a number provided by the attacker or execute USSD codes. • Display Toast (pop-up) messages on the infected device. A novel functionality of this threat is its ability to access the encrypted Whatsapp chats (available in the path /WhatsApp/Databases/msgstore.db.crypt5 on the SD card) and obtain the unique encryption key using the Google email account of the device to get the chats in plain text and store them in the file waddb.sr
Information	<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sandrorat-android-rat-targeting-polish-banking-users-via-e-mail-phishing/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:SandroRAT>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SandroRAT

Changed	Name	Country	Observed	
APT groups				
	Syrian Electronic Army (SEA), Deadeye Jackal		2011-Aug 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=08636d6f-1a0d-46ee-bc95-1586b9995db3