Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:08:52 UTC

Tool: TsarBot

Names	TsarBot
Category	Malware
Type	Banking trojan, Backdoor, Credential stealer
Description	(Cuble) Cyble Research and Intelligence Labs (CRIL) discovered a new Android banking trojan that uses an overlay attack to target over 750 applications, including banking, finance, cryptocurrency, payment, social media, and e-commerce applications, across multiple regions. While the malware mainly utilizes overlay attacks to steal credentials, it also carries out various other malicious actions. It is capable of recording and remotely controlling the screen, enabling attackers to monitor and manipulate the device. Additionally, it employs lock-grabbing techniques, keylogging, and intercepting SMS messages.
Information	<https://cyble.com/blog/tsarbot-using-overlay-attacks-targeting-bfsi-sector/>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool TsarBot

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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