Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:20:10 UTC

Tool: BADSIGNAL

Names	BADSIGNAL
Category	Malware
Type	Backdoor
Description	(Volexity) In contrast to BadBazaar and BADSOLAR, BADSIGNAL does not download a second-stage payload. Instead, all capabilities are included in the main APK. The malicious code is loaded by extending the legitimate PassPhraseRequiredActivity class in org.thoughtcrime.securesms.MainActivity. BADSIGNAL uses a REST API on port 4432 as part of its C2 communication.
Information	<https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-mobile-devices-in-multi-year-campaign/>

Last change to this tool card: 12 October 2023

Download this tool card in JSON format

All groups using tool BADSIGNAL

Changed	Name	Country	Observed	
APT groups				
	Poison Carp, Evil Eye		2018-Jun 2023	

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