Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:14:06 UTC

Tool: BadBazaar

Names	BadBazaar
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Lookout) We named this malware family BadBazaar in response to an early variant that posed as a third-party app store titled “APK Bazar.” Bazar is a lesser known spelling of Bazaar. Lookout has since acquired 111 unique samples of the BadBazaar surveillanceware dating back to late 2018. Over 70% of these apps were found in Uyghur-language communication channels within the second half of 2022. The malware primarily masquerades as a variety of Android apps, such as battery managers, video players, radio apps, messaging apps, dictionaries, and religious apps. We also found instances of apps pretending to be a benign third-party app store for Uyghurs.
Information	<https://www.lookout.com/blog/uyghur-surveillance-campaign-badbazaar-moonshine>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.badbazaar>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool BadBazaar

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b95c1027-bd3f-4a1f-beb9-778daa89388f