Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:03:11 UTC

Tool: GodFather

Names	GodFather
Category	Malware
Type	Banking trojan, Reconnaissance, Info stealer, Credential stealer
Description	(Cyble) During our routine Open-Source Intelligence (OSINT) research, Cyble Research Labs came across a Twitter post wherein researchers mention an Android bankbot named GodFather with the name apkversion1.1.5.43 and an icon similar to the default Settings app. We found notable similarities with Cereberus and Medusa banking trojans upon analyzing the malware sample. GodFather malware acts on the commands from Threat Actor's (TA's) Command & Control (C&C) server to steal sensitive information from the victim's device. Upon successful execution, the malware can perform malicious activities such as transferring money, getting device information such as phone number, installed app list, battery info, etc. By further abusing the permissions on the affected device, the malware can also steal SMSs, control device screen using VNC, forward calls, and open URLs without the user's knowledge.
Information	<https://blog.cyble.com/2022/03/23/godfather-malware-under-the-lens/> <https://blog.cyble.com/2022/12/20/godfather-malware-returns-targeting-banking-users/> <https://www.darkreading.com/endpoint-security/godfather-banking-trojan-spawns-1k-samples-57-countries> <https://cyble.com/blog/godfather-malware-targets-500-banking-and-crypto-apps-worldwide/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.godfather>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool GodFather

Changed	Name	Country	Observed

Unknown groups

	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=922d749e-df19-477c-a88d-c0153df75733