Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:43:37 UTC

Home > List all groups > List all tools > List all groups using tool MysteryBot

Tool: MysteryBot

Names	MysteryBot
Category	Malware
Type	Banking trojan
Description	(Threat Fabric) While processing our daily set of suspicious samples, our detection rule for the Android banking t LokiBot matched a sample that seemed quite different than LokiBot itself, urging us to take a closer look at it. Lo at the bot commands, we first thought that LokiBot had been improved. However, we quickly realized that there i more going on: the name of the bot and the name of the panel changed to 'MysteryBot', even the network communication changed. During investigation of its network activity we found out that MysteryBot and LokiBot Android banker are both running on the same C&C server. This quickly brought us to an early conclusion that this newly discovered Malw either an update to Lokibot, either another banking trojan developed by the same actor.
Information	<https://www.threatfabric.com/blogs/mysterybot__a_new_android_banking_trojan_ready_for_android_7_and_8.l
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.mysterybot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:MysteryBot>

Last change to this tool card: 21 May 2020

Download this tool card in JSON format

All groups using tool MysteryBot

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

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