MysteryBot; a new Android banking Trojan ready for Android 7 and 8

Published: 2024-10-01 · Archived: 2026-04-05 17:31:25 UTC

Intro

While processing our daily set of suspicious samples, our detection rule for the Android banking trojan LokiBot matched a sample that seemed quite different than LokiBot itself, urging us to take a closer look at it. Looking at the bot commands, we first thought that LokiBot had been improved. However, we quickly realized that there is 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 Malware is either an update to Lokibot, either another banking trojan developed by the same actor.

To consolidate evidence, we searched some other sources and found more matches between samples of both malware using the same C&C, as visible in following screenshot from Koodous:
