Sneaky motion-detection feature found on Android malware

By Jeff Stone

Published: 2019-01-18 · Archived: 2026-04-05 20:44:36 UTC

A strain of malicious software was activated on Android smartphones only when the infected phone was moved, according to research published by security vendor Trend Micro.

The malware came embedded in seemingly legitimate apps Currency Converter and BatterySaverMobi, which were available in the Google Play Store, Trend Micro said Thursday. Once downloaded, the malware sought to avoid detection by monitoring the motion sensor on victims' devices.

The logic seems to be that if a hacked phone was moving, the device probably wasn't a research tool being used by a security company trying to detect malware, researchers said.

"As a user moves, their device usually generates some amount of motion sensor data," the company explained in a blog post. "The malware developer is assuming that the sandbox for scanning malware is an emulator with no motion sensors, and as such will not create that type of data. … If it senses that the user and the device are not moving (if it lacks sensor data and thus, might be running in a sandbox environment), then the malicious code will not run."

The malicious code is "strikingly similar" to a banking trojan called Anubis, according to Trend Micro. Thieves used the hacking tool to record victims' keystrokes and take screenshots without their knowledge, according to the research.

BatterySaverMobi appeared to have roughly 5,000 downloads and a score of 4.5 stars from 73 reviews, though many of those may have been fake, Trend Micro noted. It was not immediately clear how many times Currency Converter had been downloaded.

Google removed both apps upon learning they were malicious.
