BianLian - from rags to riches, the malware dropper that had a dream

Published: 2024-10-01 · Archived: 2026-04-02 10:39:05 UTC

Intro

Recently, while analyzing our daily portion of APK files, searching for the new banking related threats, we found a sample that was standing out among the others. While being seemingly benign, the sample was downloading and installing the infamous Anubis malware, which is responsible for financial losses of thousands of Android users around the globe, targeting more than 300 different apps.

The thorough investigation of this sample led us to uncover yet another malware dropper campaign on the Google Play store - the main source of the applications for the vast majority of the Android users. The actors have managed to bypass the Play store protections on a regular basis, the first sample that we were able to attribute to this campaign was built and uploaded to the store in the July 2018 and most recent one – on October 16th, so the campaign is active for at least 3 months now:

As visible in the following chart, several different droppers were built through time, on quite a regular basis:
