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

Published: 2024-10-01 · Archived: 2026-05-05 02:19:37 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:

Overlay targets

The injects are stored in the encrypted ZIP file in the assets folder and cannot be dynamically changed. Below is the list of package names related to the Apps targeted by BianLian:

Package name	**App name**
com.binance.dev	Binance - Cryptocurrency Exchange
com.akbank.android.apps.akbank_direkt	Akbank Direkt
com.akbank.android.apps.akbank_direkt_tablet_20	Akbank Direkt
com.akbank.android.apps.akbank_direkt	Akbank Direkt
com.btcturk	BtcTurk Bitcoin Borsası
com.finansbank.mobile.cepsube	QNB Finansbank Cep Şubesi
com.garanti.cepsubesi	Garanti Mobile Banking
com.garanti.cepsubesi_20	Garanti Mobile Banking
com.garanti.cepsubesi	Garanti Mobile Banking

Package name	App name
com.htsu.hsbcpersonalbanking	HSBC Mobile Banking
com.ingbanktr.ingmobil	ING Mobil
com.kuveytturk.mobil	Mobil Şube
com.magiclick.odeabank	Odeabank
com.pozitron.albarakaturk	Albaraka Mobil Şube
com.pozitron.vakifbank	VakıfBank Cep Şifre
com.pozitron.iscep	İşCep
com.teb	CEPTETEB
com.tmob.denizbank	MobilDeniz
com.tmob.tabletd>	MobilDeniz Tablet
com.tmob.denizbank	MobilDeniz
com.vakifbank.mobile	VakıfBank Mobil Bankacılık
com.ykb.android	Yapı Kredi Mobile
com.ykb.androidtablet	Yapı Kredi Mobil Şube
com.ykb.android	Yapı Kredi Mobile
finansbank.enpara	Enpara.com Cepubesi
tr.com.sekerbilisim.mbank	ŞEKER MOBİL ŞUBE
com.ziraat.ziraatmobil	Ziraat Mobil
com.tmobtech.halkbank	Halkbank Mobil

Conclusion

This particular story of the new malware evolution shows that malware authors are always eager to explore new ways to maximize their profits. After establishing a way to regularly upload the droppers to the Play Store, it was a reasonable move for the malware author to work on adding new features to the Trojan, while still providing dropper service to the Anubis actors. We have seen only one version of the dropper with the new modules enabled, and there is a newer variant with the disabled modules, so we assume that the actor behind it is still testing his setup.

We can imagine two possible ways for this story to develop: 1) The dropper authors still see an important source of revenue in dropping the Anubis malware and will have both malware running side by side on the infected devices 2) There is no honor among thieves and the dropper author decide to pursue his own career in banking malware and therefore stop dropping the Anubis malware, which we believe to be the most realistic option. 3) It is also possible that the actor was just renting the Anubis Trojan while he was building his own malware, and when this will be done, he will stop using the rented Anubis

Only time will tell us what path the actors will go.

Mobile Threat Intelligence

Our threat intelligence solution – MTI, provides the context and in-depth knowledge of the past and present malware-powered threats in order to understand the future of the threat landscape. Such intelligence, includes both the strategic overview on trends and the operational indicators to discern early signals of upcoming threats and build a future-proof security strategy.

Client Side Detection

Our online fraud detection solution – CSD, presents financial institutions with the real-time overview on the risk status of their online channels and related devices. This overview provides all the relevant information and context to act upon threats before they turn into fraud. The connectivity with existing risk or fraud engines allows for automated and orchestrated, round the clock fraud mitigation.

IOC

```
Canlı Döviz Takip & Çevir(com.ganatolii.android.apps) b2398fea148fbcab0beb8072abf47114f7dbbccd589f88ace6e33e293
```

Special thanks

A special thanks to the AVAST team and their APKLAB platform, which allowed us to search for additional samples.
