



[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> [Top 10 Android banking trojans target apps with 1 billion downloads](#)

---

## Top 10 Android banking trojans target apps with 1 billion downloads

---

By

**Bill Toulas**

(<https://www.bleepingcomputer.com/author/bill-toulas/>)

June 2, 2022

05:09 PM

1



The ten most prolific Android mobile banking trojans target 639 financial applications that collectively have over one billion downloads on the Google Play Store.

Mobile banking trojans hide behind seemingly benign apps like productivity tools and games and commonly sneak into the Google Play Store, Android's official app store.





Once they infect a device, they overlay login pages on top of legitimate



According to a report by Zimperium (<https://get.zimperium.com/mobile-banking-heists/>) that gives an overview of the Android ecosystem in the first quarter of 2021, each of these trojans has assumed a unique spot in the market by how many organizations they target as well as functionality that differentiate them from the rest.

This finding is very worrying, as according to 2021 surveys, three out of four respondents in the U.S. use banking apps to perform their daily banking activities, providing a massive pool of targets for these trojans.

## The most targeted

United States tops the list of the most targeted countries having 121 targeted apps. The United Kingdom follows with 55 apps, Italy with 43, Turkey with 34, Australia counts 33, and France has 31.

The trojan that targets the most applications is Teabot, covering 410 out of 639 of those tracked, while Exobot also targets a sizable pool of 324 applications.

The targeted application with the most downloads is PhonePe, which is very popular in India, having 100 million downloads from the Play Store.

Binance, the popular cryptocurrency exchange app, counts 50M downloads. Cash App, a US and UK-covering mobile payment service, also has 50 million installations via the Play Store. Both of these are also targeted by several banking trojans, even if they don't offer conventional banking services.

The most widely targeted application is BBVA, a global online banking portal with tens of millions of downloads. This app is targeted by seven out of the ten most active banking trojans.

The most prolific banking trojans in the first quarter of this year, according to Zimperium, are the following.

- **BianLian** (<https://www.bleepingcomputer.com/news/security/bianlian-android-banking-trojan-upgraded-with-screen-recorder/>) – Targets Binance, BBVA, and a range of Turkish apps. A new version of the trojan discovered in April 2022 features photoTAN bypassing, which is considered a strong authentication method in online banking.
- **Cabassous** – Targets Barclays, CommBank, Halifax, Lloyds, and Santander . Uses domain generation algorithm (DGA) to evade detection and takedowns.
- **Coper** – Targets BBVA, Caixa Bank, CommBank, and Santander. It actively monitors device battery optimization "allowlist" and modifies it to exempt itself from restrictions.
- **EventBot** (<https://www.bleepingcomputer.com/news/security/new-android-malware-steals-financial-information-bypasses-2fa/>) – Targets Barclays, Intensa, BancoPosta, and various other Italian apps. It hides as Microsoft Word or Adobe Flash, and can download new malware modules from remote sources.
- **Exobot** (<https://www.bleepingcomputer.com/news/security/source-code-for-exobot-android-banking-trojan-leaked-online/>) – Targets PayPal, Binance, Cash App, Barclays, BBVA, and CaixaBank. It's very small and light because it uses shared system libraries and fetches overlays from the C2 only when needed.
- **FluBot** (<https://www.bleepingcomputer.com/news/security/flubot-android-malware-operation-shutdown-by-law-enforcement/>) – Targeted BBVA, Caixa, Santander, and various other Spanish apps. The botnet trojan was notorious for its rapid distribution using SMS and contact lists of compromised devices.
- **Medusa** (<https://www.bleepingcomputer.com/news/security/medusa-malware-ramps-up-android-sms-phishing-attacks/>) – Targets BBVA, CaixaBank, Ziraat, and a range of Turkish bank apps. It can perform on-device fraud by abusing the accessibility service to act as a normal user on the victim's behalf.

- **Sharkbot**  
(<https://www.bleepingcomputer.com/news/security/sharkbot-malware-hides-as-android-antivirus-in-google-play/>) – Targets Binance, BBVA, and Coinbase. It features a rich set of detection evasion and anti-deletion capabilities, as well as strong C2 communication encryption.
- **Teabot** (<https://www.bleepingcomputer.com/news/security/teabot-malware-slips-back-into-google-play-store-to-target-us-users/>) – Targets PhonePe, Binance, Barclays, Crypto.com, Postepay, Bank of America, Capital One, Citi Mobile, and Coinbase. It features a special keylogger for each app. and loads it when the user launches it.



dropper to fetch additional malware on the compromised device.



As it becomes clear from the above, each of the ten most prolific banking trojans maintains its own relatively narrow targeting scope, so the ecosystem is balanced and the operatives can pick the tool that matches their target audience.

豊丘		二和	
¥28,000		¥40,000	

To protect from all these threats, keep your device up to date, only install apps from the Google Play Store, check user reviews, visit the developer’s site, and keep the number of installed apps on your device at a minimum.

