

TeaBot Banking Trojan Posted as QR Code app in Google Play Store Targeting US Users

By Gurubaran

Published: 2022-03-03 · Archived: 2026-04-05 17:30:36 UTC

At the beginning of 2021, a new type of trojan called “Teabot” was found attacking users. The trojan was specifically designed to steal the victim’s bank credentials and SMS messages.

Other features of the trojan included Remote access capabilities and screen capturing via request-on-demand services. Threat actors have the ability to do account takeovers directly from compromised mobile devices. This technique is called “On-device fraud”.

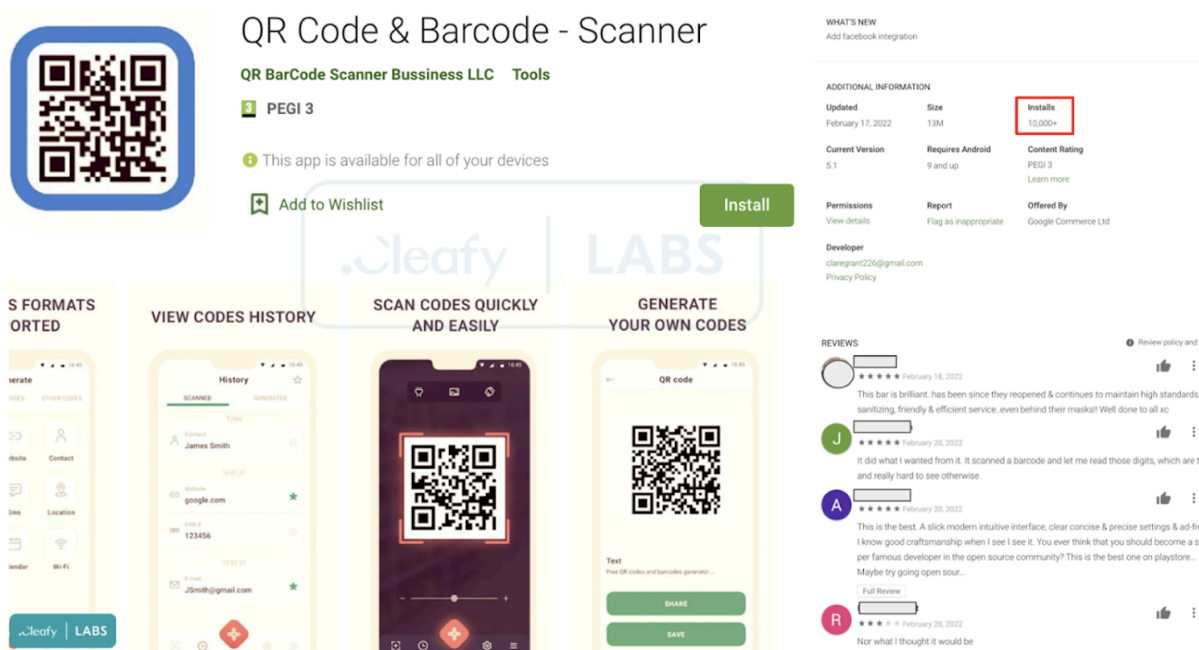
Teabot trojan was distributed through smashing campaigns where attackers used a lure list such as VLC media player, TeaTV, DHL and UPS, etc. Recent researches show that hackers have used the Google Play store to distribute the “dropper applications”.

Reports suggest that the target list has expanded further including 400 applications that involve various banks, crypto exchanges or wallets, and digital insurances in countries like the US, Russia, and Hong Kong.

Evolution and Distribution of TeaBot

In its initial stages in 2021, TeaBot was not fully developed. Nevertheless, hackers were distributing it through smashing campaigns as mentioned before. Later, the trace was lost and the malware was found to be non-existent until February 21, 2022.

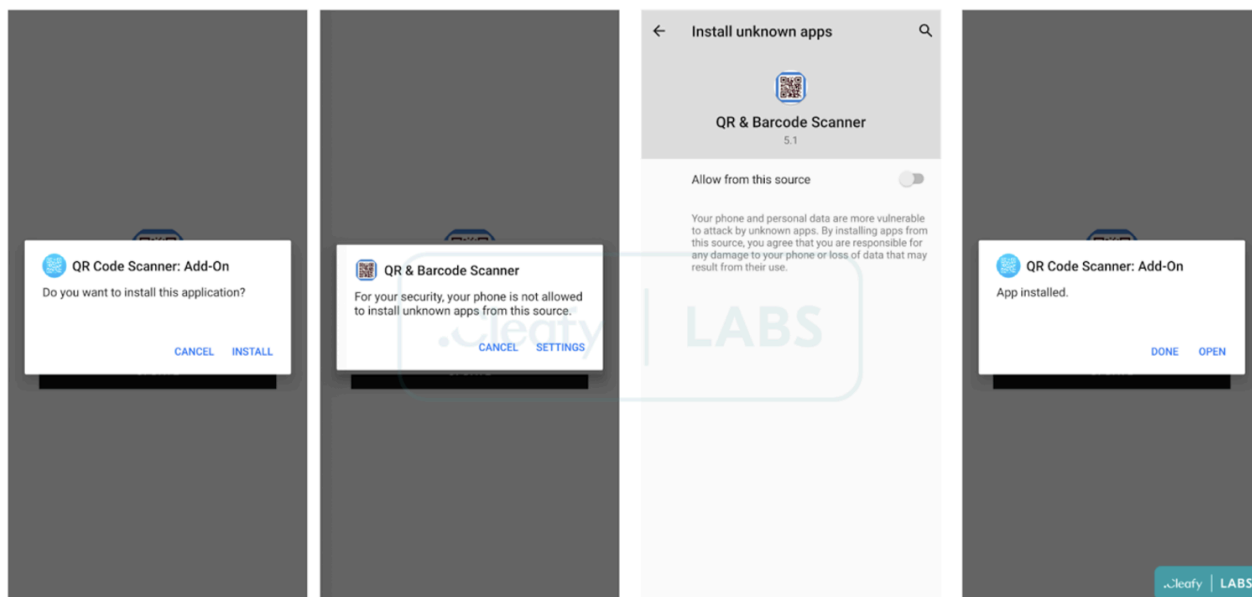
Researchers at Cleafy were able to take a glimpse of a particular application that was published on the Google Play store. Reviews seemed very legitimate with almost 10,000+ downloads. However, this application was found to be a TeaBot dropper application. The dropper was delivering TeaBot through fake update procedures.



The application was a QR code and Barcode Scanner Application published under the name “QR BarCode Scanner Business LLC”. Users were giving feedback that the app was good and well-functioning. The dropper was hiding behind the QR code scanner.

Once the victims install and open the app through the Google Play store, the app gives a pop-up message that an update must be installed. When victims click on install, the application downloads the dropper and installs another application on the victim’s device.

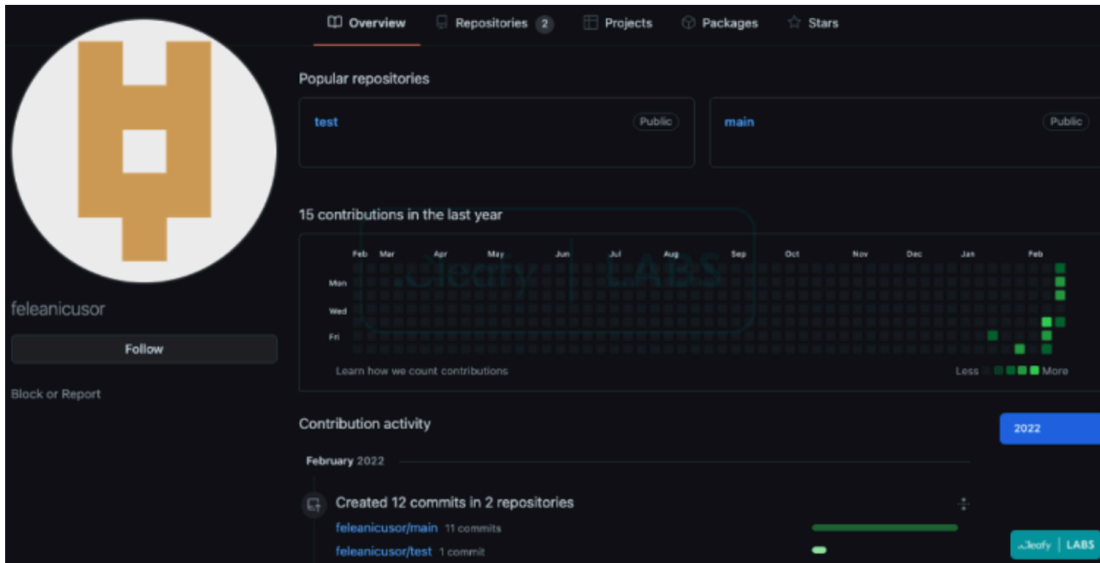
Legitimate Play store apps will redirect to Google play store for any updates. The installed application was found to be TeaBot trojan.



Source : Cleafy

Cleafy labs reported that the second application which was named **QR Code Scanner: Add-on** is downloaded from two particular Github repositories owned by the user *feleanicursor*.

On exploring further, the repositories had so many samples of TeaBot dated from Feb 17, 2022.



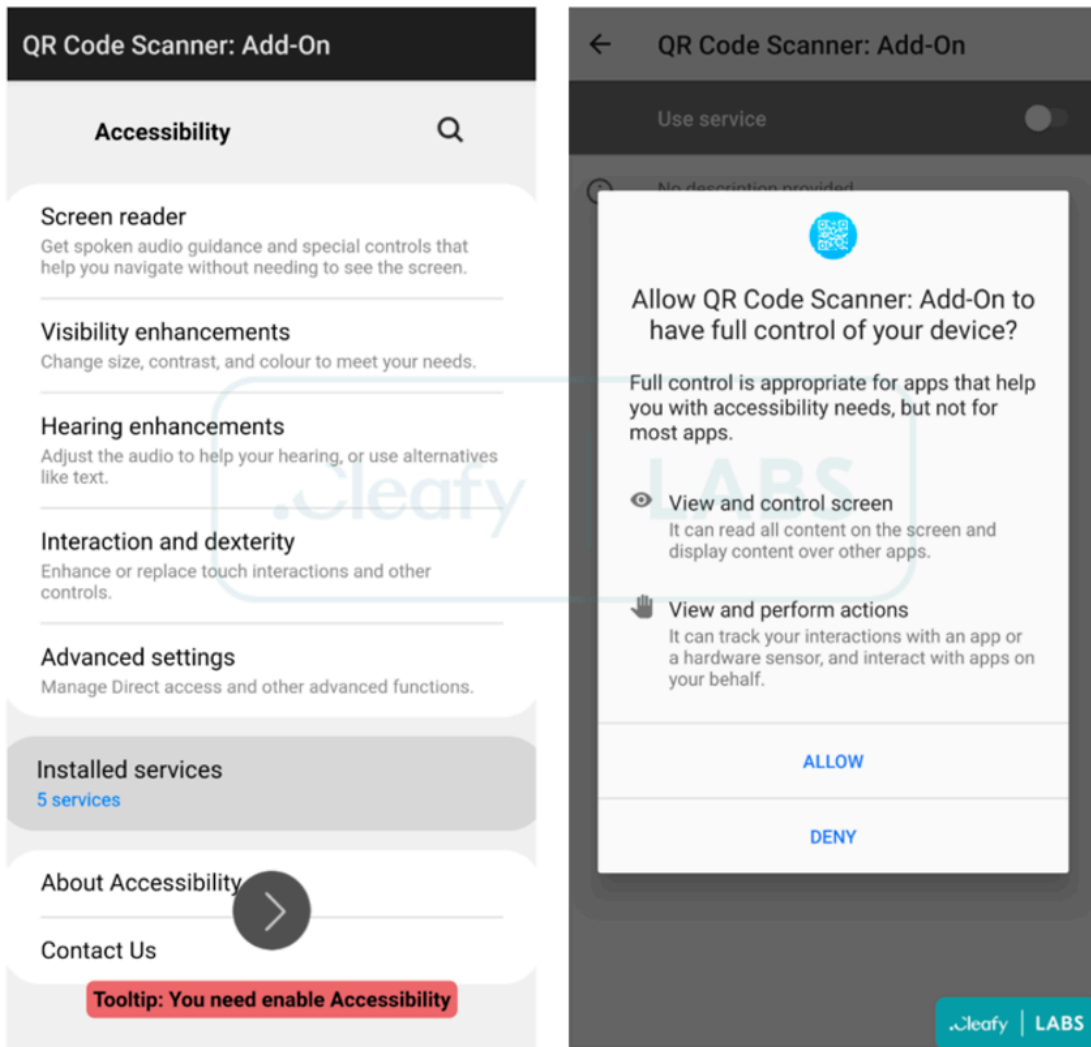
Source : Cleafy

Attack Chain of TeaBot

Teabot's attack chain clearly states that attackers have been working on the sideloading and evasive techniques which start from the initial dropper application to the hosting of the malicious payload.

When the victims accept the download of the fake update, TeaBot installation procedures take place. During the installation, it also asks for Accessibility services permission to get necessary privileges. The application specifically asks for 2 permissions.

- **View and control Screen** – This permission is acquired to view and control the screen on the victim's device which is used for obtaining login credentials, 2FA codes, and to read SMS.
- **View and Perform actions** – This permission is described as interaction with an app. But actually, it is required to perform malicious actions with the infected device.



Source : Cleafy

A full detailed [report](#) on how threat Actors used strong obfuscation techniques to evade antivirus software was published by Cleafy.

You can follow us on [Linkedin](#), [Twitter](#), [Facebook](#) for daily Cybersecurity and hacking news updates.



[Gurubaran](#)

Gurubaran is a co-founder of Cyber Security News and GBHackers On Security. He has 10+ years of experience as a Security Consultant, Editor, and Analyst in cybersecurity, technology, and communications.

Source: <https://gbhackers.com/teabot-banking-trojan/>