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

gbhackers.com/teabot-banking-trojan/

March 3, 2022

BANK
TeaBot banking trojan posted as QR code app in Google Play Store targeting US users

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”.

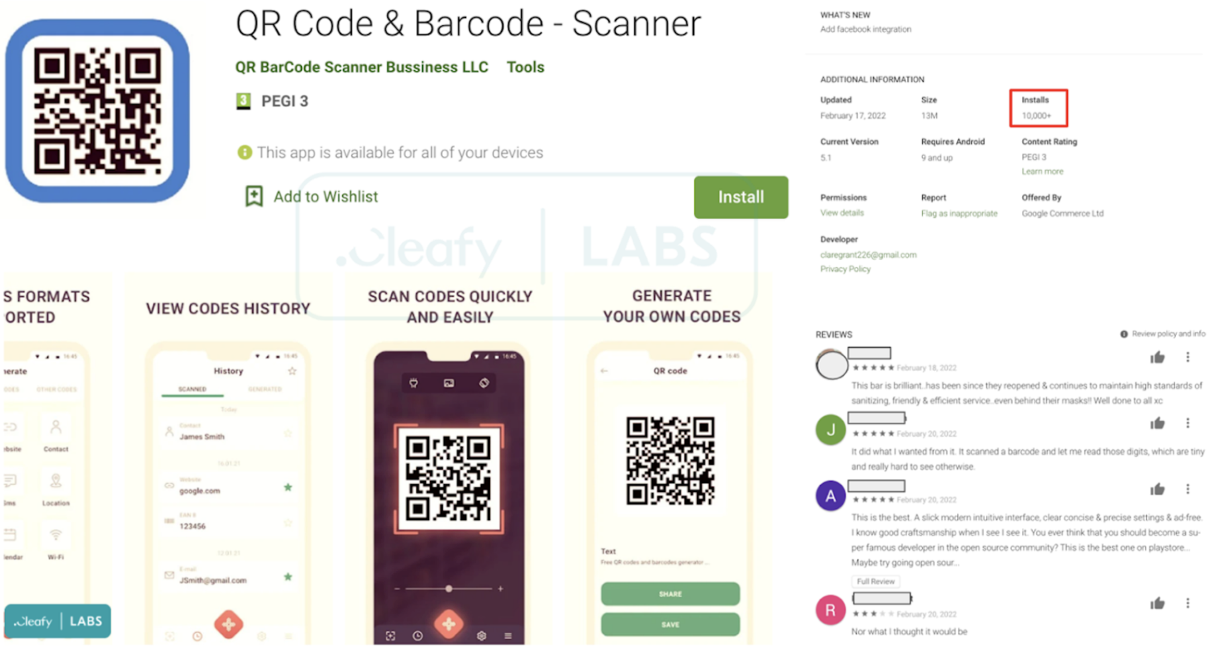
Teabot trojan was distributed through smashing campaigns where attackers used a lure list such as VLC media player, TeaTV, DHL and UPS, etc. Recent researches show that hackers have used the Google Play store to distribute the “dropper applications”.

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.



QR Code & Barcode - Scanner

QR BarCode Scanner Bussiness LLC Tools

PEGI 3

This app is available for all of your devices

Add to Wishlist

Install

WHAT'S NEW

Add facebook integration

ADDITIONAL INFORMATION

Updated	Size	Installs
February 17, 2022	13M	10,000+
Current Version	**Requires Android**	**Content Rating**
5.1	9 and up	PEGI 3 Learn more
Permissions	**Report**	**Offered By**
View details	Flag as inappropriate	Google Commerce Ltd

Developer

claregrant226@gmail.com

Privacy Policy

REVIEWS

Review policy and info

[redacted]
★★★★★ February 18, 2022
This bar is brilliant..has been since they reopened & continues to maintain high standards of sanitizing, friendly & efficient service..even behind their masks!! Well done to all xc

[redacted]
★★★★★ February 20, 2022
It did what I wanted from it. It scanned a barcode and let me read those digits, which are tiny and really hard to see otherwise.

[redacted]
★★★★★ February 20, 2022
This is the best. A slick modern intuitive interface, clear concise & precise settings & ad-free. I know good craftsmanship when I see I see it. You ever think that you should become a super famous developer in the open source community? This is the best one on playstore... Maybe try going open sour...

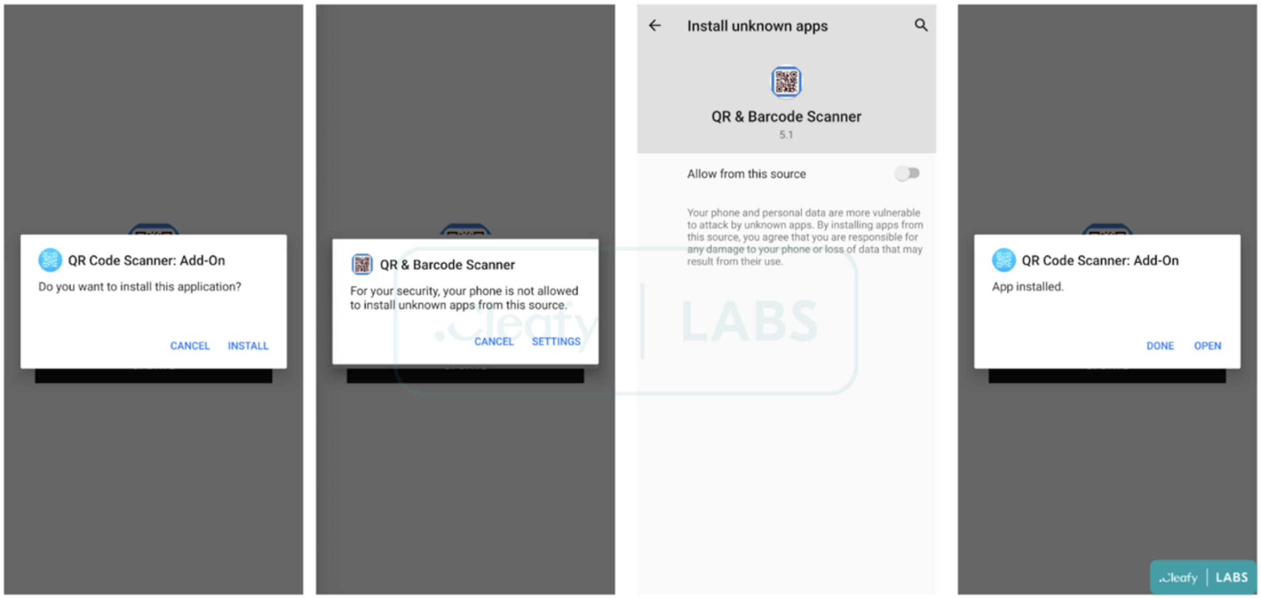
Full Review

[redacted]
★★★☆☆ February 20, 2022
Nor what I thought it would be

The application was a QR code and Barcode Scanner Application published under the name “**QR BarCode Scanner Bussiness 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.



QR Code Scanner: Add-On

Do you want to install this application?

QR & Barcode Scanner

For your security, your phone is not allowed to install unknown apps from this source.

Install unknown apps

QR & Barcode Scanner

5.1

Allow from this source

Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

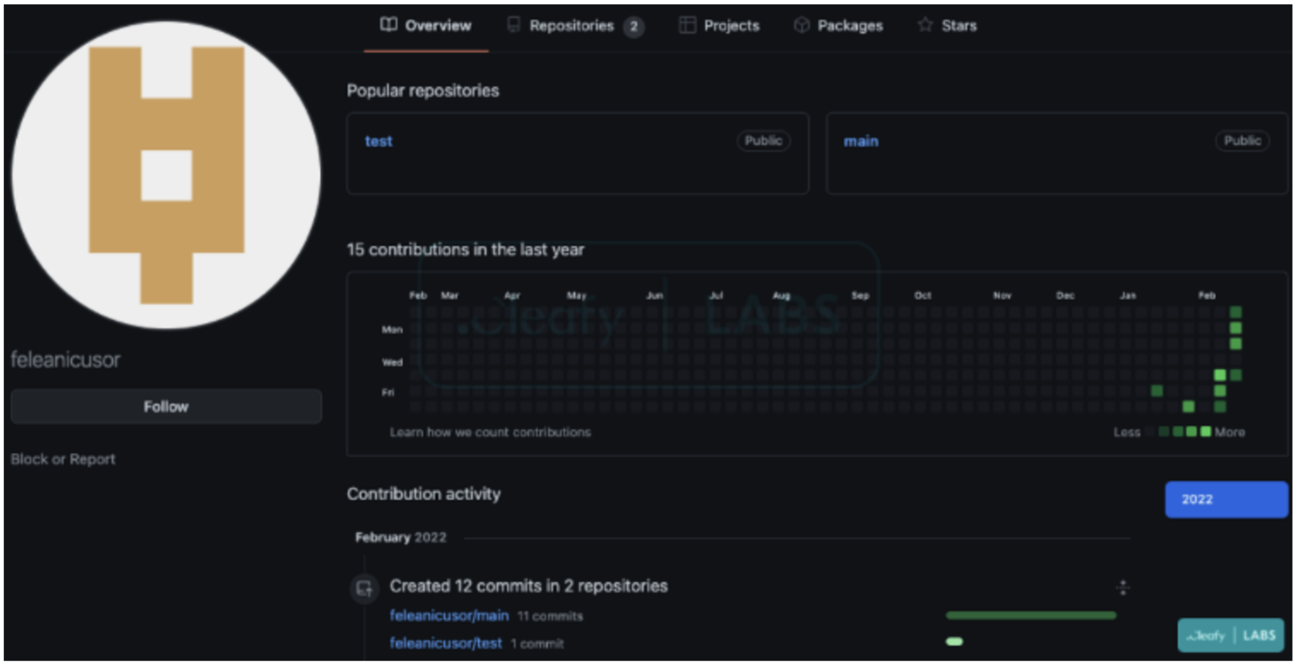
QR Code Scanner: Add-On

App installed.

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 *feleanicusor.*

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



feleanicusor

Popular repositories

test Public

main Public

15 contributions in the last year

Learn how we count contributions

Contribution activity

February 2022

Created 12 commits in 2 repositories

feleanicusor/main 11 commits

feleanicusor/test 1 commit

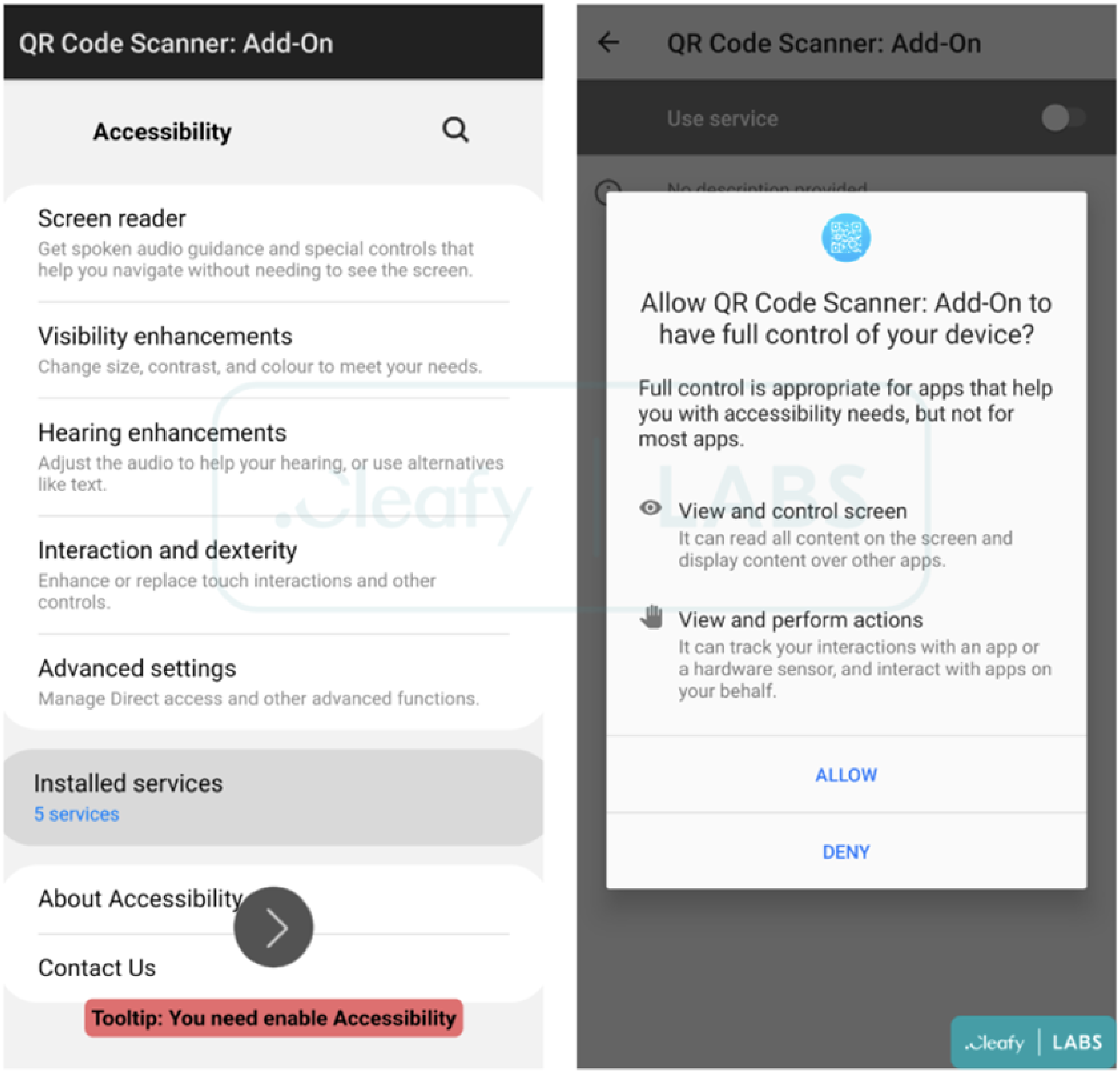
Source : Cleafy

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.



QR Code Scanner: Add-On

Accessibility

Screen reader
Get spoken audio guidance and special controls that help you navigate without needing to see the screen.

Visibility enhancements
Change size, contrast, and colour to meet your needs.

Hearing enhancements
Adjust the audio to help your hearing, or use alternatives like text.

Interaction and dexterity
Enhance or replace touch interactions and other controls.

Advanced settings
Manage Direct access and other advanced functions.

Installed services
5 services

About Accessibility

Contact Us

Tooltip: You need enable Accessibility

QR Code Scanner: Add-On

Use service

No description provided

Allow QR Code Scanner: Add-On to have full control of your device?

Full control is appropriate for apps that help you with accessibility needs, but not for most apps.

View and control screen
It can read all content on the screen and display content over other apps.

View and perform actions
It can track your interactions with an app or a hardware sensor, and interact with apps on your behalf.

ALLOW

DENY

Source : Cleafy

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

Leave a Reply