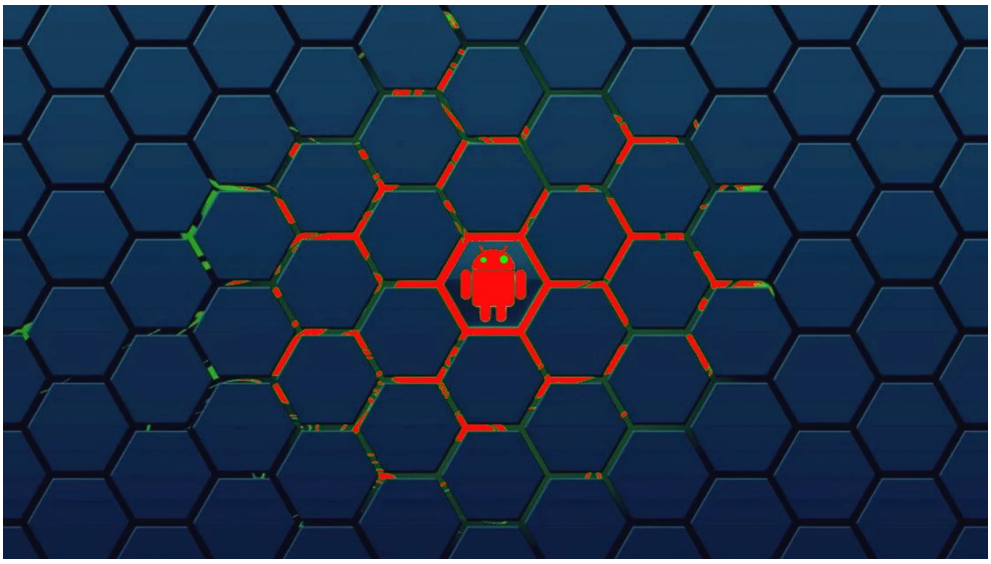
New FluBot and TeaBot campaigns target Android devices worldwide

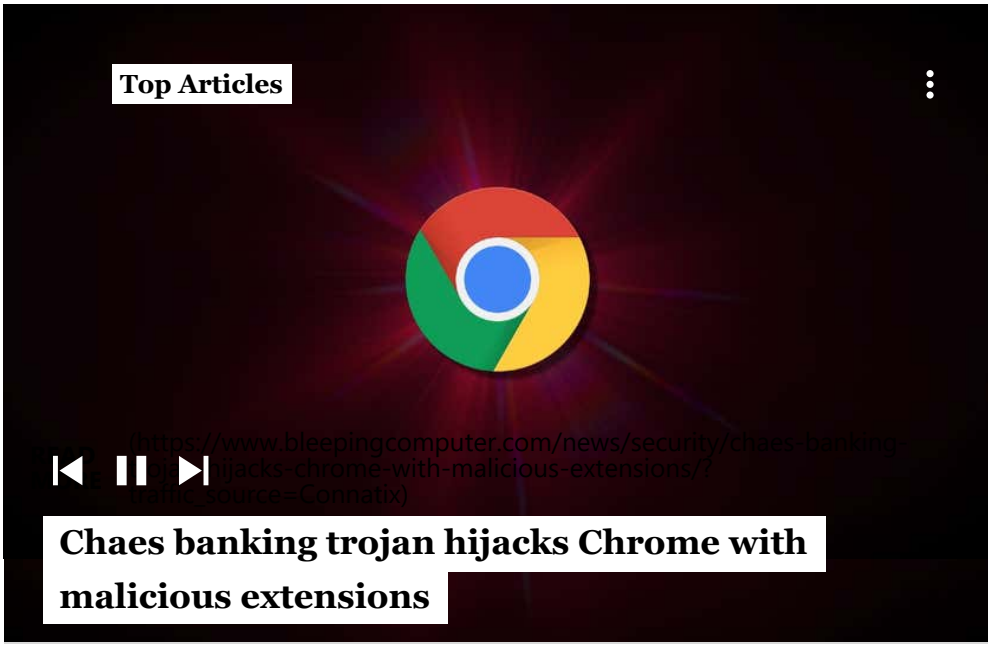
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 26, 2022 09:19 AM **0**



New FluBot and TeaBot malware distribution campaigns have been spotted, using typical smishing lures or laced apps against Android users in Australia, Germany, Poland, Spain, and Romania.

The SMS topics used for spreading the FluBot malware include fake courier messages, "Is this you in this video?" coaxes, phony browser updates, and fake voicemail notifications.

The most recent FluBot campaign was tracked by researchers at Bitdefender Labs, who intercepted over 100,000 malicious SMS since December 2021, illustrating the threat actor's massive volume of distribution.



According to the report, the FluBot operators conduct attacks in short-term waves using different lures for each country.

Upon infecting one device, the malware uses the victim's contact list to distribute other SMS lures (https://www.bleepingcomputer.com/news/security/flubot-malware-now-targets-europe-posing-as-flash-player-app/), achieving better infection rates due to recipients' trust in known contacts (https://www.bleepingcomputer.com/news/security/flubot-android-malware-now-spreads-via-fake-security-updates/) and continuous growth.

FluBot distribution has remained active throughout 2021, and the reports about high-volume 2022 activity prove that its operators aren't ready to call it a day yet.

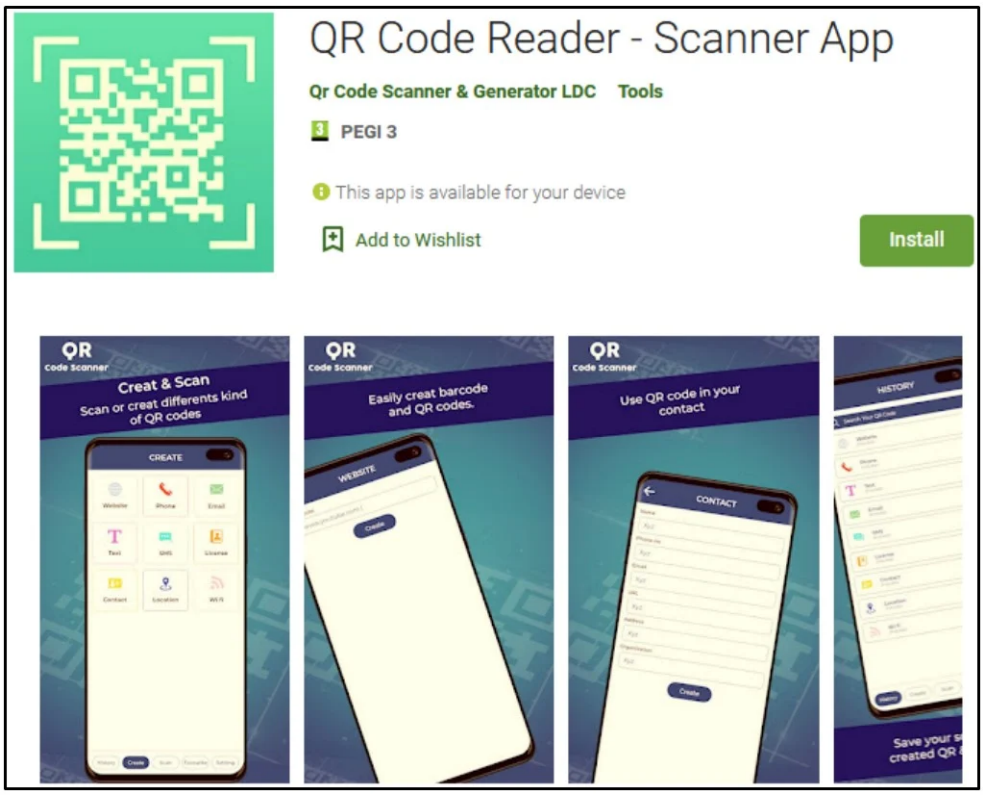
TeaBot on the rise in the Google Play Store

TeaBot is a different Android banking trojan discovered in January 2021 and has a global reach.

As reported by Bitdefender, TeaBot has made multiple appearances on the Play Store since December 2021.

According to the researchers, TeaBot is distributed to unsuspecting victims via trojanized apps on the Google Play Store, including:

- QR Code Reader – Scanner App – 100,000 downloads
- QR Scanner APK – 10,000 downloads
- QR Code Scan – 10,000 downloads
- Smart Cleaner – 1,000 downloads
- Weather Cast – 10,000 downloads
- Weather Daily – 10,000 downloads



QR code app that silently fetches TeaBot

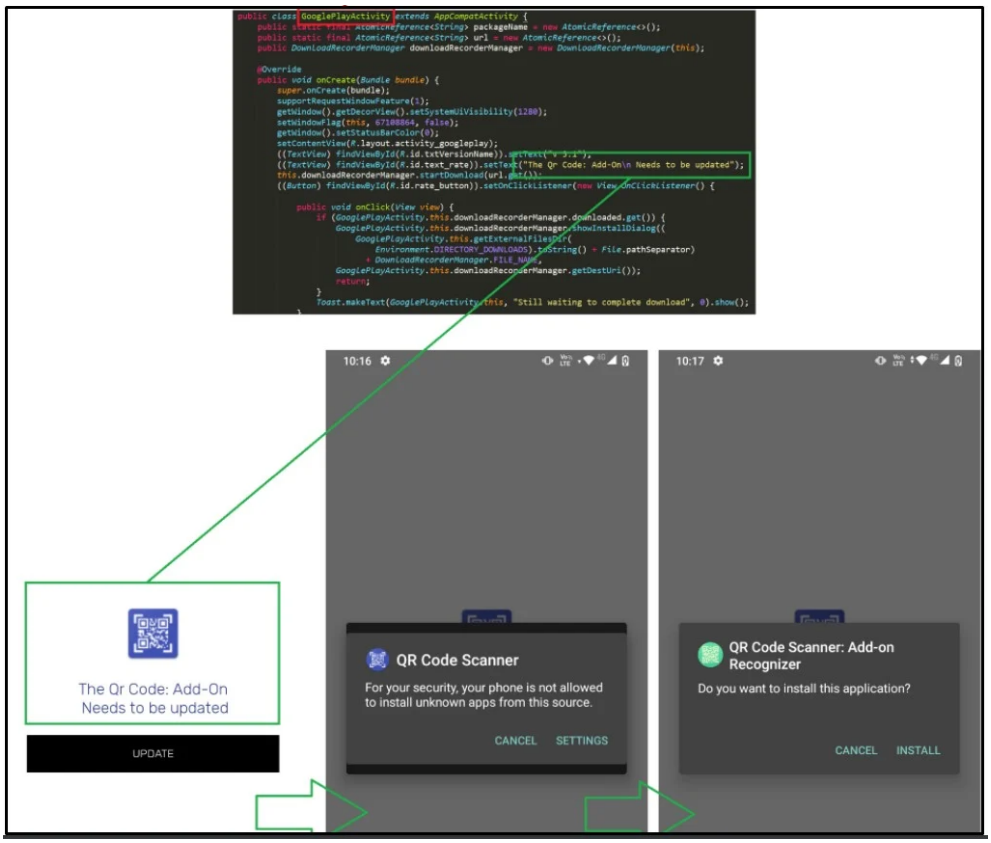
Source: Bitdefender

None of these applications featured malicious functionality, and all offered the promised features, which allowed them to pass the Google Play Store's review process and reach a wider infection pool.

Moreover, the actors actively promoted these apps by paying to appear in Google Ads served within other applications and games.

However, once installed and executed on the victim's device, the apps started a background service that checked the country code and stopped if the result was Ukraine, Uzbekistan, Uruguay, or the United States.

The app retrieved its configuration for all other victims and fetched an APK from a GitHub repository, which contained a TeaBot variant. At the same time, the apps prompted the user to allow third-party sources to install packages.



Alert to allow the installation via 3rd party sources

ource: Bitdefender

Between December 6, 2021, and January 17, 2022, Bitdefender analysts have counted 17 different versions of TeaBot infecting devices through the listed apps.

The TeaBot campaign illustrates that even when installing software from the Google Play Store, it does not mean that you will always be safe.

Therefore, it is advisable to remain vigilant with new installations, check user reviews, monitor the app's network and battery usage, and only grant non-risky permissions.

Remember, this is not the first time (https://www.bitdefender.com/blog/labs/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/) that TeaBot has managed to infiltrate the Play Store through laced apps, and it's unlikely it'll be the last one.