# When your phone gets sick: FluBot abuses Accessibility features to steal data

By SRLabs

Published: 2021-12-21 · Archived: 2026-04-05 15:32:43 UTC

### Key take-aways

- Accessibility features enable malware to bypass Android's permission system that is supposed to prevent malware from stealing credentials. Therefore, the majority of the active banking Trojans exploit this weak spot
- Awareness for this issue seems to be limited: Only few apps implement safeguards
- Right now, there are no known Android-level countermeasures that would preserve the usability of Accessibility features while at the same time preventing their abuse

## We face a pandemic of Android malware abusing Accessibility

2021 was a truly pandemic year, not only in terms of COVID-19 but also for Android banking malware. The rise in Android banking Trojans is driven by several catalysts: a general professionalization of malware distribution services, and the leaked source codes of Anubis and Cerberus. Many banking Trojans have in common their (ab)use of Accessibility service to control the infected device.

This article explains how Accessibility features are abused by Android malware to steal sensitive data and spread to other phones. The post focuses on FluBot, a banking Trojan active since December 2020. The analysis is based on FluBot as observed "in the wild" in Germany in July 2021.

## Android Accessibility features: A blessing and a curse

Accessibility features are tools included with Android that ease access to mobile phone services for people with disabilities. For example, Android can read text aloud and prescribe voice into text, lowering the barrier of mobile phone usage for visually impaired users. Android Accessibility featurescan be grouped in four categories: screen readers, display configurations like magnification and Select to Speak, interaction controls like the Accessibility Menu, and audio & on-screen text transcription. These services require broad access to the system itself, the stored data (including e.g., contacts, photos, and passwords), the ability to read the screen, create overlays, and to perform actions on behalf of the user. These all happen to also be features that Android malware can abuse to steal data.

Each "helper app" must be given specific permission to use Accessibility service. This permission is given only once per app, usually right after the installation of the helper app (or malware app).

Accessibility features can help malware to circumvent Android's security framework that makes use of a kernel-level application sandbox to isolate application resources. This isolation intends to prevent apps from interacting

with other apps unless they have exposed services such as intents and content providers. Even if a malicious app is installed, Android prevents third-party access to protected app resources. In theory.

When a user enables Accessibility for a malicious app, **the security framework can be bypassed in two ways to steal data from other apps**:

### Overlay

The first method is that the malicious Accessibility service puts an HTML overlay resembling the actual login screen on the targeted app when it is launched. When the user tries to log in, their login credentials are sent to the hacker's server.

### Keylogger

In the second method, the malicious Accessibility service takes the role of a keylogger by tracking the changes on the EditText fields where the user can input their login credentials. Every time the user inputs or deletes a character, the result is sent to the hacker's server, enabling them to capture the user credentials.

Google partly mitigated these issues in 2017 by attempting to ban all apps from the Play Store that misused Accessibility services and by limiting the use of this Android API for developers. Yet, since Google can only control the apps in their app store, this did not fix the general problem as fraudsters now lure victims into installing apps from other sources. Therefore, Accessibility features can be considered the current Achilles' heel of Android.

Given that only a minority of Android users actually use Accessibility features, the authors believe that the barrier of initially activating the far-reaching access should be significantly higher than simply giving an app permission to use them. Users should be asked to authenticate twice to acknowledge a clear warning message highlighting the potential dangers of giving Accessibility privileges to a newly installed app. Google Play services should by default scan all Accessibility-requesting apps independent of whether they were installed through Google Play.

## FluBot in action: Lure users through Smishing

The FluBot malware demonstrates how Accessibility features are commonly abused. First "in-the-wild" samples of FluBot were detected by CSIS in December 2020. The first piece of analysis was released in January 2021 by ThreatFabric. An initial in-depth analysis was published by PRODAFT in March 2021, and another one in April 2021 by Proofpoint. Our analysis has been conducted on a more recent sample that we obtained "in-the-wild" in July 2021 through a malicious SMS message distributed to German mobile numbers. The package name is "com.UCMobile.intl".

The fraud typically starts with an SMS that informs users that they are expecting a parcel (Figure 1) or received a voicemail (Figure 2). The messages are usually sent in the national language of the network where it is received. To circumvent simple carrier SMS spam filters, the included links change often, words are misspelled or capitalized, or, as seen in Figure 2, random letters are added.


Figure 1: Example for a phishing SMS by FluBot received in April 2021 in a German mobile network. The message says: “Your parcel will be sent returned to the sender. Last possibility to get it <link>”.

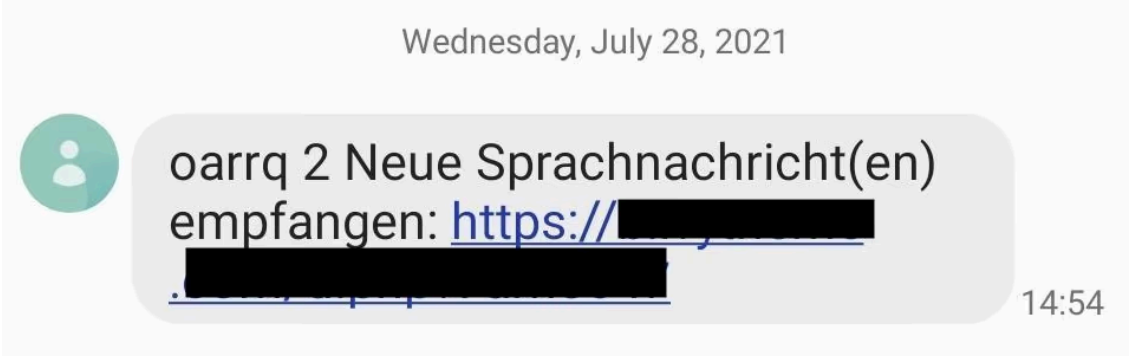


Figure 2: The phishing SMS we received in July 2021 in a German mobile network. The message says: “oarrq 2 New voicemail(s) received <link>”.

The analyzed version of FluBot notifies the user of a missed voicemail (Figure 2). The link redirects victims to a website where they are asked to download an app (Figure 3). This website often imitates well-known brands like T-Mobile (Figure 3), DHL, and FedEx. In a twist to irony, one version of FluBot directs users to a website which informs them that their mobile is infected with FluBot and suggests that they download an app to get rid of it.

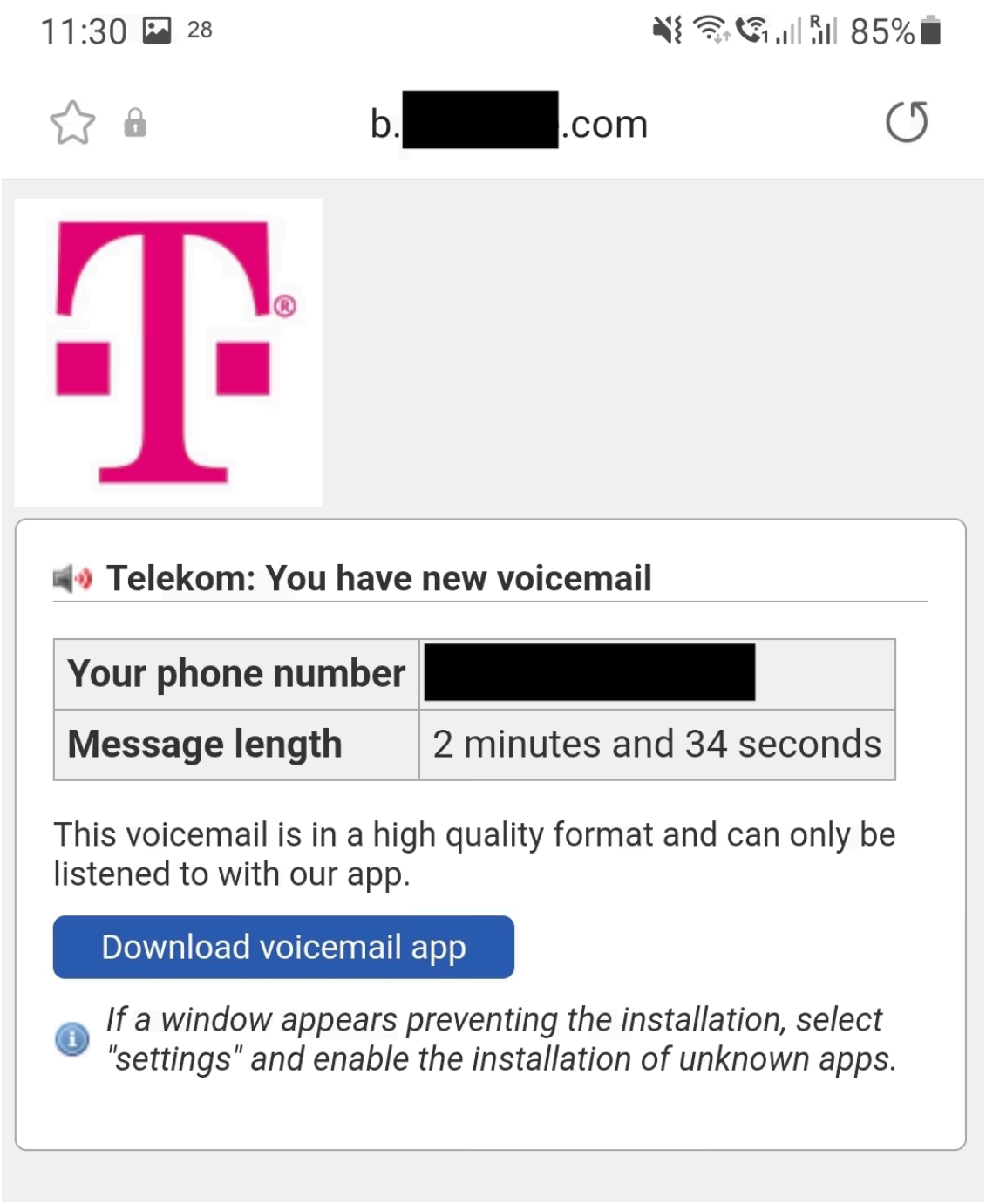


Figure 3: Website that lures people to download the FluBot app

As soon as users download and install the app – despite several warning messages – the malware app will ask for permission to use Accessibility features and notification access to gain control over the phone (Figure 4).

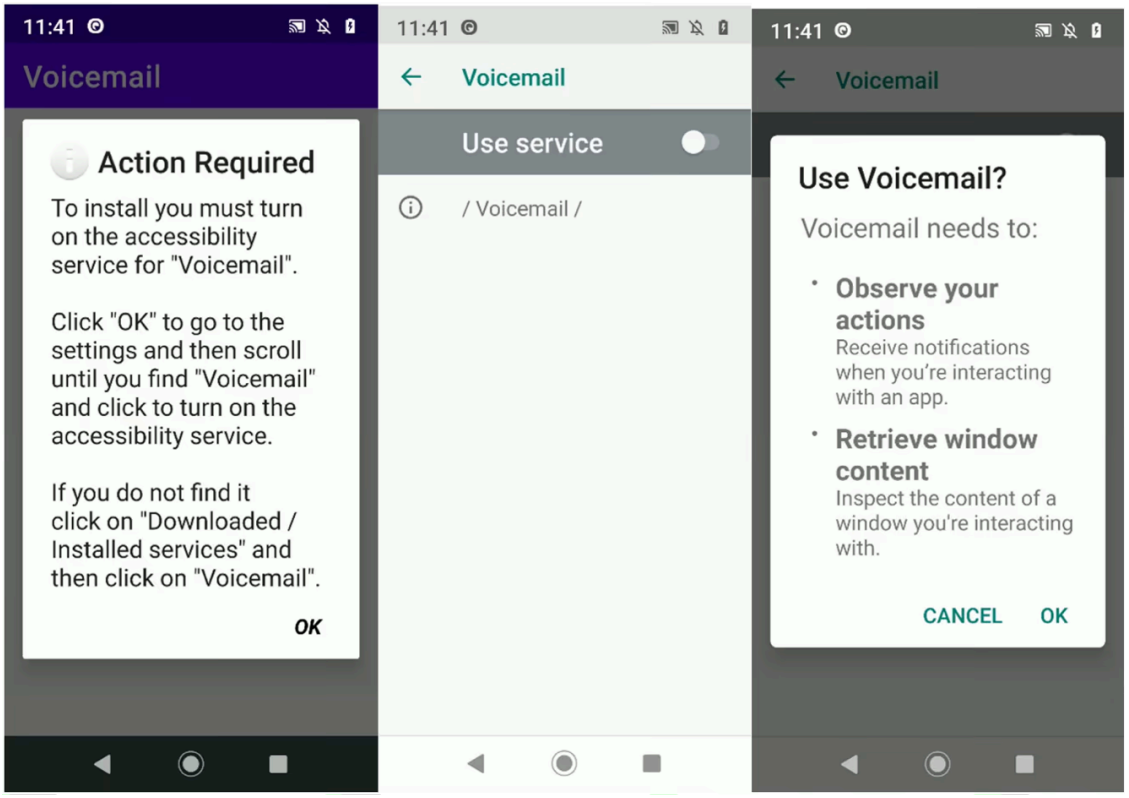


Figure 4: FluBot asking for permission to use Accessibility features

One key feature of FluBot is making use of the mobile's contact list and Messages app to spread further. For this spreading mechanism, the infected device uploads the contact list of the victim to the Command&Control (C&C) server. Then, it receives a list of text messages and phone numbers to send the SMS message which includes the APK file to download – this is hosted on a hacked website (Figure 5).


Figure 5: A GET_SMS command sent from the C&C server

Next, FluBot prepares to its core objective: Stealing credentials of banking and cryptocurrency apps, it needs to be in the target scope of the C&C server. FluBot sends a list of apps installed on the victim's phone to the C&C server. The server responds with a subset of apps that are targeted and sends the HTML files for overlay attacks (Figure 6). A wide range of cryptocurrency trading and online banking apps are being targeted by FluBot.

Figure 6: A GET_INJECT command sent from the C&C server for one of the banking apps installed

## FluBot in action: Abuse Accessibility features in three ways

Accessibility permissions allow FluBot to steal the app credentials, evade detection and removal, and send SMS to spread to further victims.

First, to steal the login credentials from the user, FluBot leverages two approaches. The first one is using an overlay: An HTML page resembling the login dashboard of the targeted app is shown to the user with an overlay by making use of the Accessibility services (Figure 7). When the user inputs their password and clicks ‘Log In’, their credentials are sent to the C&C server.

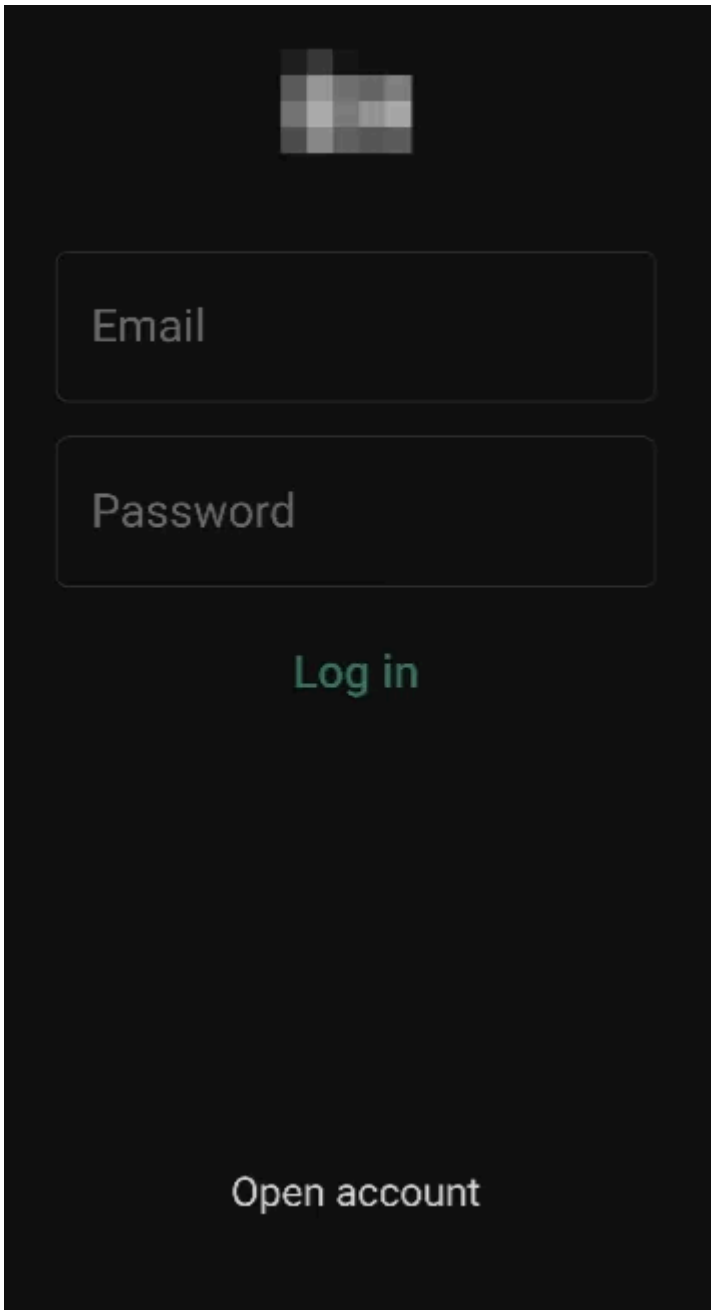


Figure 7: Overlay attack on a banking app

The second approach is to observe the EditText events using Accessibility services, sending the value of the EditText every time a change is made (Figure 8). This approach can be more dangerous as there is no modification of the UI and the credentials are being stolen from the actual UI of the targeted app. We have observed that this approach serves as a fallback option when the overlay attack does not work.

```
LOG,INJECT:          .android,{"email":"      @gmail.com","password":"kajsnxhskshsj","exit":true}
```

Figure 8: Logging of captured credentials from the overlay attack

FluBot also abuses Accessibility services to lie quiet and block its uninstallation. When Accessibility permissions are granted, FluBot obtains the permission to run in background through the permission “ignore battery optimizations”. As a final self-defense, FluBot prevents its uninstallation via the Android UI by immediately sending a “go-back" command using the Accessibility services when the user is viewing the App Info window of FluBot. Additionally, with the use of Accessibility services, FluBot can go into Google Play settings and disable Google Play Protect when it receives the “DISABLE_PLAY_PROTECT” command.

Thirdly, through Accessibility features, FluBot sets itself as the default SMS app so that it can handle the spreading mechanism. To prevent users from seeing the malicious messages FluBot sent on their behalf, the malware puts an overlay on the Google Messages app, preventing the user from seeing the malicious messages that were sent.

## App developers can make Accessibility-based abuse harder

Developers of finance-related and other high-value apps should take precautions against malware abusing Accessibility services. Apps should check if the Accessibility services are turned on and warn their users. One notable example that does this correctly is Coinbase. When the Coinbase Android app detects the type of hooking that enables a keylogger, it warns the user: “An Accessibility service is trying to interact with Coinbase. Shake your device to authorize it.” Since malware can simulate touches and gestures, a warning that can be ignored by shaking the device is the right approach as the malware will not be able to skip the warning.

However, while developers can take precautions for the keylogging approach, there is not much they can do against overlay attacks using the Android SDK. We have not encountered any financial apps which take precautions against overlay attacks.

## Android users should follow a few best practices to stay safe

For now, users should assume that neither the OS nor their apps prevent Accessibility-based abuse. Users should instead follow basic security precautions to limit their exposure to FluBot and other malware:

### Prevention

- Do not click on links in messages, suspicious emails, and fishy websites. Instead, use the company website or app to access your information
- Ideally, only install apps from a trusted app store, most notably the Google Play Store, and even from there, only install apps that have a considerable number of downloads

- If you do not rely on Accessibility features to use your phone, never give the Accessibility permission to any app. You can also check it in Settings > Accessibility
- Backup your data frequently to keep it safe in case you need to reset your device, which sometimes is the only simple way to remove malware

## If you installed malware

- Put your mobile in flight mode immediately
- Reset your device to default settings
- Change your passwords of all the accounts you accessed after installing the malware
- Contact your bank in case you are using their banking app from your phone
  This research was done by the mobile security team at Security Research Labs. If you are interested in researching similar topics, please get in touch or consider joining our team.

---