The Coper—a new Android banking trojan targeting Colombian users

news.drweb.com/show/

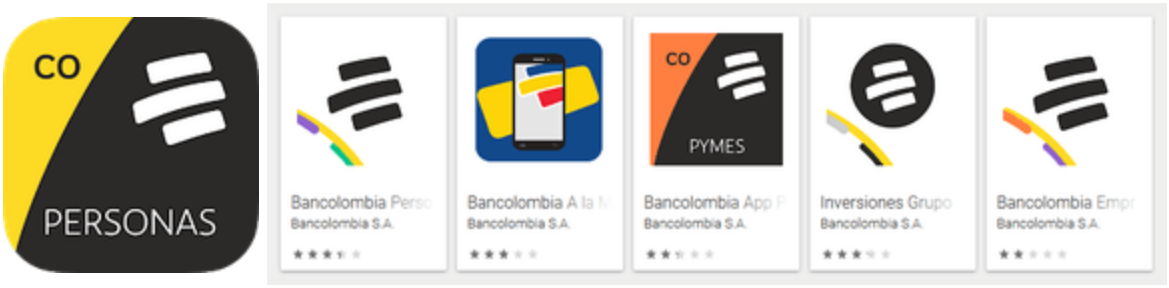
Doctor Web

Back to news

July 21, 2021

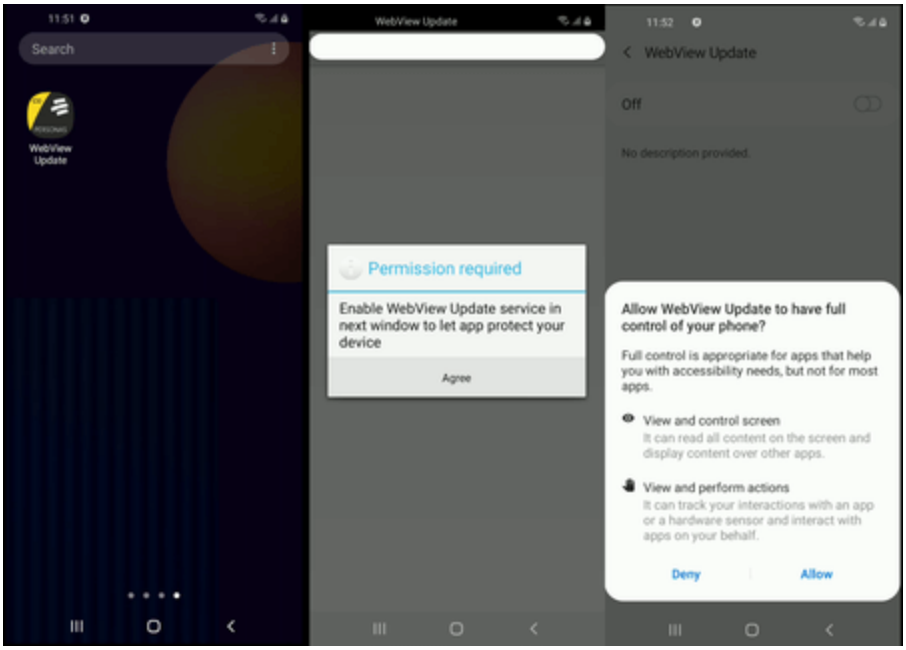
Doctor Web warns of a newly discovered family of Android banking trojans dubbed Android.BankBot.Coper. The malicious apps have a modular architecture and a multi-stage infection mechanism. They also have several protective techniques helping them withstand removal attempts. That allows the trojans to stay active longer and perform more successful attacks. All known Coper banker trojan modifications target Colombian users to date. However, new versions targeting users from other countries are likely to emerge over time.

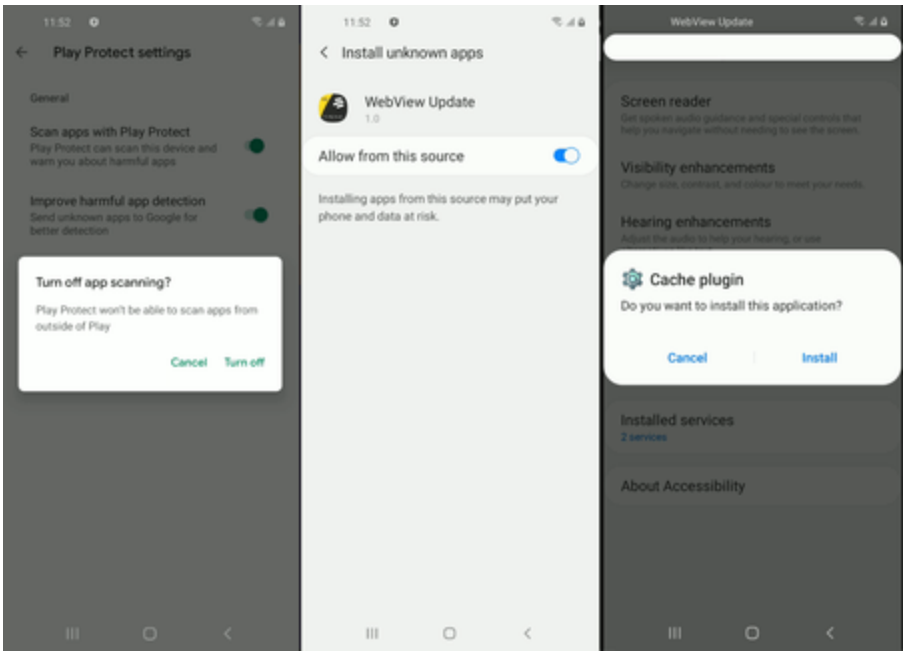
All **Android.BankBot.Coper** samples discovered and investigated by our malware analysts were spread as the official Bancolombia financial institution app called Bancolombia Personas. To make them appear more legitimate, the icon of these fake apps was designed to follow the looks of genuine software from the targeted bank. For comparison, below is an example of the fake app's icon (left image) and the genuine Bancolombia app icons (right image) available on Google Play:



The infection process itself is divided into several stages. The first step is installing the decoy fake app that cybercriminals pass off as banking software. This application is none other than a dropper whose primary task is to spread and install the main malicious module hidden inside it onto the targeted Android device. Since the operating logic of the analyzed trojan modifications is practically the same as **Android.BankBot.Coper.1**, this trojan will be used as an example to describe the functioning mechanism.

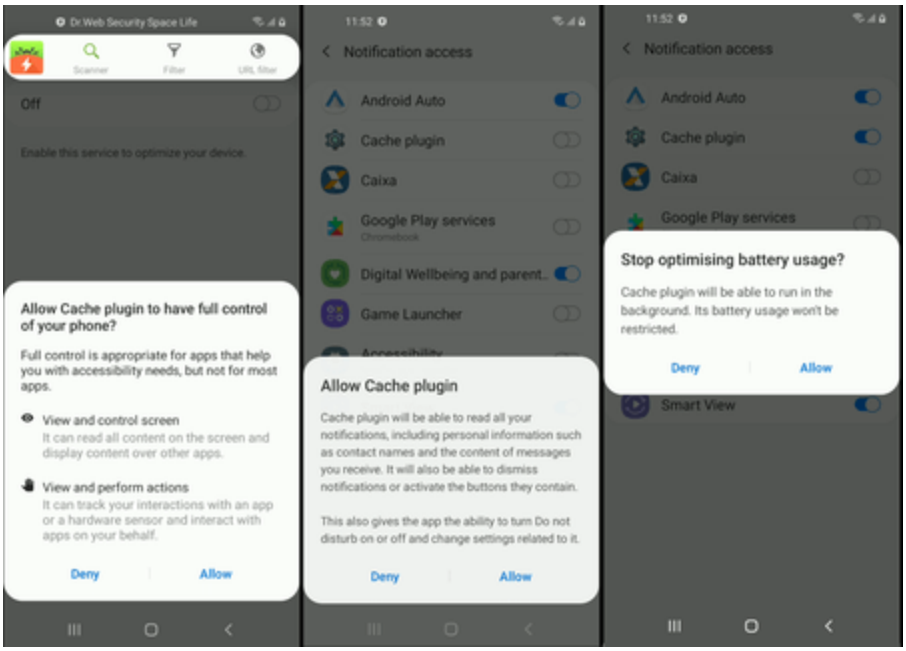
Upon launch, the dropper decrypts and runs an executable dex file (**Android.BankBot.Coper.2.origin**) located in its resources and disguised as a web document named o.htm. This trojan component plays a role in the second stage of the infection process. One of its tasks is to obtain access to the Accessibility Services functions. Using these functions, the trojan will have full control over the infected device and imitate user actions like pressing the menu button and closing windows. To do so, it requests corresponding permissions from the victim. If successful, the trojan will perform all further malicious actions on its own. It tries to disable Google Play Protect, built-in malware protection in the operating system; it also tries to allow installing apps from unknown sources and to install and run the main malicious module, providing it with access to the Accessibility Services.

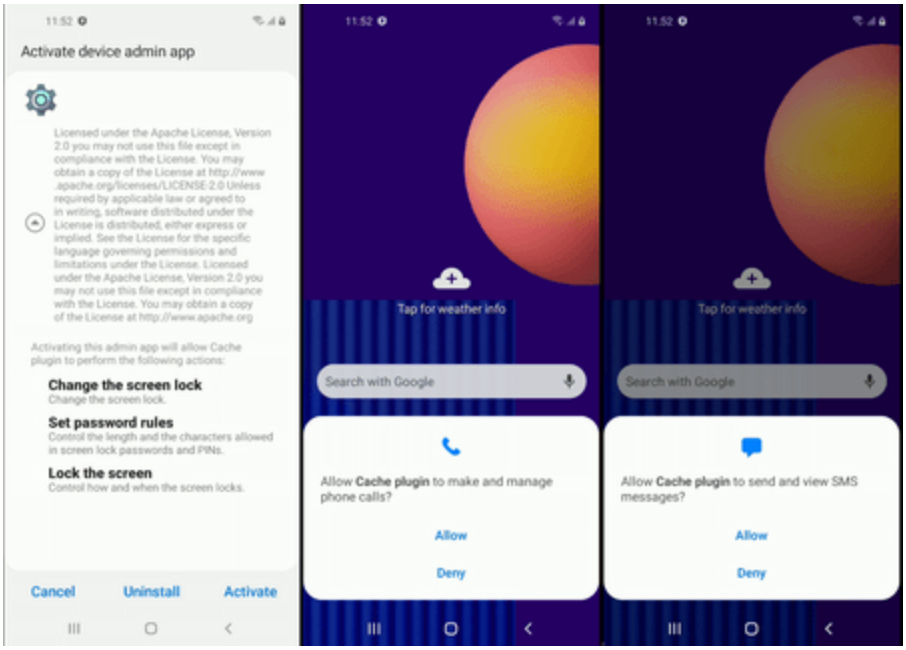




The trojan decrypts and, using obtained privileges, installs the malicious apk package (**Android.BankBot.Coper.2**) that's hidden in the second decrypted file, disguised as an audio file PViwFtl2r3.mp3. This file contains the trojan module **Android.BankBot.Coper.1.origin** that performs the main malicious tasks the attackers need. The trojan module is installed under the guise of a system application called Cache plugin that uses a default gearwheel icon normally used by some Android system apps. Such app name and the icon increase the chances that users won't suspect that this software is a threat.

When launched, this main module gains access to many important functions. For example, the trojan requests permission from the victim to read and manage notifications and join the device's battery optimization white-list. The latter will allow the trojan to operate continuously without the risk of being terminated by the system. Moreover, the trojan automatically becomes the device administrator and gains access to manage phone calls and SMS.





Next, this malicious module conceals its icon from the list of installed apps located on the home screen, hiding from the user. Then, it notifies the C&C server about the successful infection and waits for further commands. The trojan maintains a constant connection to the C&C server by sending out requests every minute. If needed, this time interval can be changed with corresponding command. In addition, depending on the answer received from the C&C server, the trojan can also change other settings, including:

- a list of C&C servers
- a list of targeted applications determining which windows will be overlaid by a phishing window upon launch
- a list of applications to delete

- a list of applications that the trojan will prevent from launching, returning the user to the home screen
- a list of apps that will have their notifications blocked
- other parameters

Upon receiving the direct commands, the **Android.BankBot.Coper.1.origin** can perform the following malicious actions:

- send USSD requests
- send SMS
- lock the device screen
- unlock the device screen
- start intercepting SMS
- stop intercepting SMS
- display a push notification
- re-display phishing window on top of the specified app
- run a keylogger
- stop a keylogger
- uninstall applications specified in the command
- uninstall itself with the dropper app

Moreover, the trojan intercepts and sends the contents of the incoming push notifications to the C&C server.

To display a phishing window, the **Android.BankBot.Coper.1.origin** uses a well-known technique that has become a standard for Android banking trojans. The contents of such a window are downloaded from the remote server and placed into WebView, making it imitate the appearance of the targeted application to trick the victim.

Android.BankBot.Coper trojans are endowed with several defensive mechanisms. One of them is to control the integrity of the primary malicious component. In case it's deleted, the Copper bankers will try to reinstall it.

The second protective method is to monitor potentially dangerous actions to the trojan, including:

- opening the Google Play Protect page in the Play Store app
- user attempts to change the device administrators' list
- user access to the trojan's information page from the system's list of installed apps
- user attempts to change the trojan's access rights for the Accessibility Services functions

If the trojans detect any of these events, they use Accessibility Services to simulate pressing the Home button, returning the victim to the home screen. And if they detect that the user is trying to uninstall them, they simulate pressing the Back button. So, the trojans not only

prevent their removal but also prevent the owners from normally using their own devices.

In addition, the **Android.BankBot.Coper** droppers are equipped with additional protective mechanisms. For example, they check if they're running in a virtual environment, verify if there's an active SIM card and also check user's country of residence. If one of these checks fails, the droppers will immediately stop running. The purpose of such verifications might be to prevent the installation of the main malicious module in conditions unfavorable for the trojans, effectively avoiding early detection. Unfavorable conditions might include installing under the control of security specialists or onto user devices from countries of no interest to the attackers. It's worth noting that in the analyzed samples, these verifications are not used, but they might be used in future modifications.

Doctor Web recommends Android users to install banking software only from official app catalogs and official financial institutions' websites. That's if, for some reason, using the official app store isn't possible.

Dr.Web anti-virus products for Android successfully detect and delete all known modifications of the **Android.BankBot.Coper** banking trojans, so they pose no threat to our users.

Indicators of compromise

- More details on **Android.BankBot.Coper.1**
- More details on **Android.BankBot.Coper.2.origin**
- More details on **Android.BankBot.Coper.2**
- More details on **Android.BankBot.Coper.1.origin**

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments