What is Media File Jacking?

Recently, an attack named Media File Jacking has been revealed on Android devices running WhatsApp and Telegram. If you use these applications, there are steps you need to take to protect yourself and your device.

People use secure messaging services with end-to-end encryption like WhatsApp or Telegram, believing they will keep their messages and devices more secure. Although this is generally true, there are security issues with these applications that users need to know.

Recently, an exploit attack called Media File Jacking has been revealed on Android devices running WhatsApp and Telegram. If you use one of these apps, there are steps you need to take to protect yourself and your device.

How do media files become security risks?

Security company Symantec has announced security vulnerabilities, which can be used to spread fake news or trick users into sending payment information to the wrong address. It works through a system that allows messaging applications to receive media files, such as when a friend sends you a photo or video through the application.

Media files can become a security risk
To receive files, your Android device needs to have write access to the external memory. This means the app can take a file sent to you and save it to the SD card on the device.

Ideally, apps like Telegram or WhatsApp will only have permission to write to the internal memory. That means that the files can be viewed in the application, but other programs cannot access them. This means that if someone sends you a photo, you can't automatically see it in your camera collection.

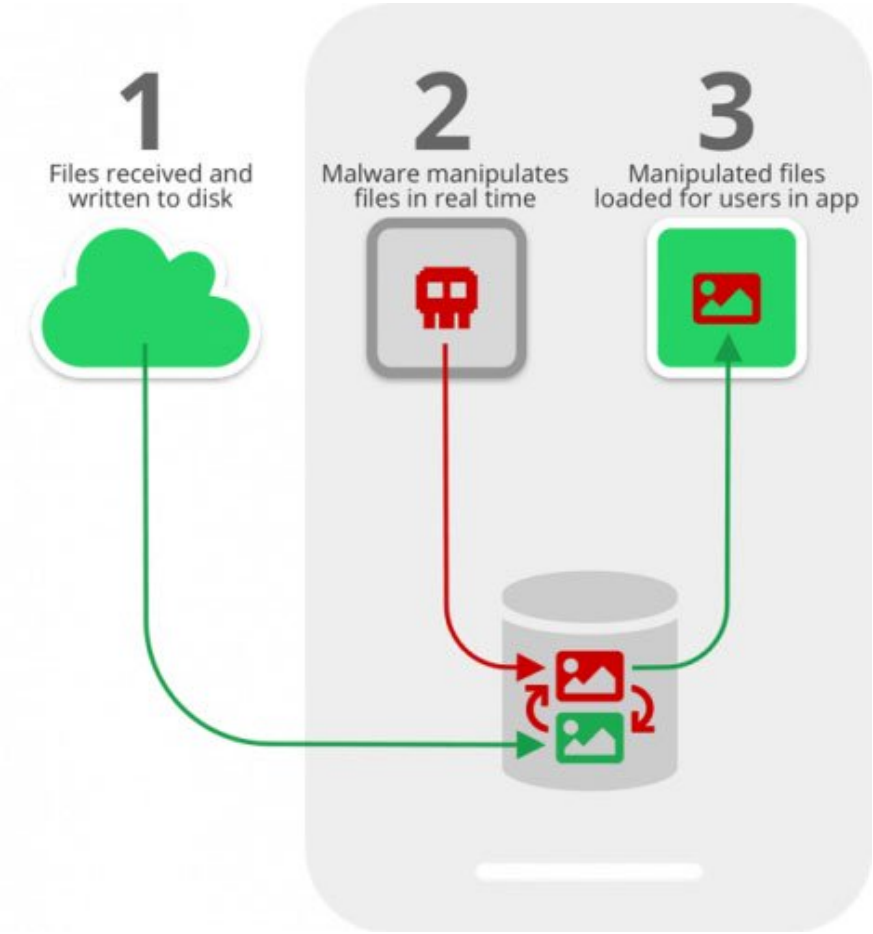
WhatsApp saves files to external storage by default. Telegram saves files to SD card if the **Save to gallery** option is turned **on** .

What is Media File Jacking?

This attack works by blocking the messaging application from saving media files.

First, a user downloads an app that looks harmless, such as a free game, but actually has malware inside, and the app runs in the background of their device.

Now, the user goes to the messaging application. If the application saves media files to external storage, the malicious application may target the files at a time between when they are saved on the hard drive and when they are displayed in the application.



This attack works by blocking the messaging application from saving media files
This is similar to a Man-in-the-middle attack. The malicious application monitors the device for any changes to external memory and the steps at which the device detects changes. When a real file is saved to the device from a messaging application, the malicious application will jump in and overwrite the file with its own file. Then the fake file will be displayed in the messaging application.

This attack applies to images and audio files. It even swaps thumbnails in the messaging app, so users don't know the file they're opening is not the file the contact sent them.

How does Media File Jacking spread fake news?

This attack may cause a problem. That is spreading fake news. Many people use a Telegram feature called **Channel** . Channel is a forum through which an administrator can send a message to a large group of subscribers. Some people use this feature as a news feed, viewing daily news stories from a trusted channel in their Telegram app.

The concern is that Media File Jacking could be used to interfere with news channels. A trusted channel administrator will post a notable news image. The image was then blocked by a malicious application on the recipient's phone. Real images are swapped with a fake news image. Administrators will not know this has happened and the recipient will think that image is a true news story.

How to protect the device from Media File Jacking

A real fix for this vulnerability would require developers to rethink the way they access files stored in Android. However, there is a quick fix for users during this time. You just need to disable the feature to save files to external memory.

Protect your device from Media File Jacking
To do this on Telegram, open the menu by swiping from the left of the app and going to **Settings.** Then go to **Chat Settings.** Make sure the **Save to Gallery** switch is set to **Off.**

To turn off file storage to external storage on WhatsApp, go to **Settings** , then **Chats. Make sure the Make sure the Media Visibility** switch is set to **Off.**

Once you have changed this setting, the messaging application will be protected from Media File Jacking attacks.

Media File Jacking is an example of clever ways that an attacker can use to interfere with the device through a messaging application. It is best to change the settings to ensure your device is not vulnerable.

If you're concerned about the security of messaging apps, check out the article: 5 ways WhatsApp messages can be hacked.