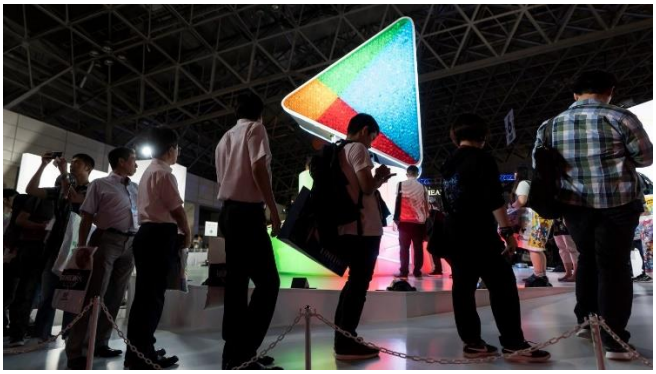
4 dangerous Android malware apps discovered on Google Play

By Jacob Siegal
November 6th, 2022 at 1:42 PM



No matter how legitimate an app looks, there's always a chance that it's actually malicious. We see this time and time again on the Google Play store, and this week, yet another batch of malicious apps has been uncovered. Even worse, these apps are still active on Google's app store at the time of writing, so be sure to avoid them at all costs.

On Tuesday, the analysts from Malwarebytes Labs highlighted a family of malicious Android apps that are infected with a hidden ads trojan. All four apps are from the developer Mobile apps Group, and they have garnered over 1 million downloads combined.

Malwarebytes Labs analyst Nathan Collier notes that this developer has spread malware on Google Play before. He states that it's unclear if Google actually caught Mobile apps Group, but notes that some versions of the popular Bluetooth Auto Connect app have been clean in the past. That suggests the developer has been caught and uploaded a clean version of the app before eventually loading it up with more malware.

Android malware apps on the Google Play store. Image source: Google Play

Delete these Android malware apps ASAP

Here are the four apps, all of which you should delete if they're on your device:

- **Bluetooth Auto Connect**
- **Bluetooth App Sender**
- **Driver: Bluetooth, Wi-Fi, USB**
- **Mobile transfer: smart switch**

According to Malwarebytes, the apps don't exhibit any malicious behavior within the first 72 hours of being downloaded. After the self-imposed delay, these apps start opening phishing sites in Chrome. Some of the sites are relatively harmless, generating revenue by having the user click on ads. Other sites are more dangerous, attempting to trick users by telling them that they've been infected or need to update their device.

Collier shared even more details about how the malware works in his blog post:

The Chrome tabs are opened in the background even while the mobile device is locked. When the user unlocks their device, Chrome opens with the latest site. A new tab opens with a new site frequently, and as a result, unlocking your phone after several hours means closing multiple tabs. The user's browser history will also be a long list of nasty phishing sites.

This is especially concerning because Mobile apps Group has uploaded clean versions of these apps in the past. In other words, they aren't always malicious, and that's apparently enough to keep them on Google Play. Again, all four of these

apps are freely available on the Play store at the time of writing, so clearly, the system isn’t working.