Google Play caught hosting an app that steals users' cryptocurrency

Yu Chun Christopher Wong/S3studio/Getty Images

reader comments

100 with 71 posters participating

Share this story

Google Play has been caught hosting yet another malicious app, this time one that was designed to steal cryptocurrency from unwitting end users, researchers said Friday.

The malware, which masqueraded as a legitimate cryptocurrency app, worked by replacing wallet addresses copied into the Android clipboard with one belonging to attackers, a researcher with Eset said in a blog post. As a result, people who intended to use the app to transfer digital coins into a wallet of their choosing would instead deposit the funds into a wallet belonging to the attackers.

So-called clipper malware has targeted Windows users since at least 2017. Last year, a botnet known as Satori was updated to infect coin-mining computers with malware that similarly changed wallet addresses. Last August came word of Android-based clipper malware that was distributed in third-party marketplaces.

The clipper malware available in Google Play impersonated a service called MetaMask, which is designed to allow browsers to run apps that work with the digital coin Ethereum. The

primary purpose of Android/Clipper.C, as Eset has dubbed the malware, was to steal credentials needed to gain control of Ethereum funds. It also replaced both bitcoin and Ethereum wallet addresses copied to the clipboard with ones belonging to the attackers.

Eset malware researcher Lukas Stefanko wrote:

> *This attack targets users who want to use the mobile version of the MetaMask service, which is designed to run Ethereum decentralized apps in a browser, without having to run a full Ethereum node. However, the service currently does not offer a mobile app—only add-ons for desktop browsers such as Chrome and Firefox.*

> *Several malicious apps have been caught previously on Google Play impersonating MetaMask. However, they merely phished for sensitive information with the goal of accessing the victims' cryptocurrency funds.*

Eset spotted the app shortly after its introduction to Google Play on February 1. Google has since removed it. Stefanko said it's the first time clipper malware has been hosted in the Android app bazaar.

The discovery is yet more evidence that Google can't be trusted to proactively keep malware out of Play. That leaves the onus on end users. People should limit the number of apps they install and then only after doing a fair amount of research. One way to check the legitimacy of an app is to independently visit the site of the outfit that purportedly developed the app. The official MetaMask website makes no mention of an Android app. That should have been a red flag that the Google Play offering was an imposter.

It's not a bad idea to read user comments and stick with apps with at least 100,000 downloads, although this practice, at least on its own, is no guarantee against downloading malicious titleshttps://arstechnica.com/?p=1454053