BIZCOMMUNITY

Sophos discovers over a hundred fake cryptocurrency apps that steal money

IT security company Sophos has identified 167 fake Android and iOS apps that attackers are using to steal money from people who believe they have installed a financial trading, banking or cryptocurrency app from a well-known and trusted organisation.

Photo by Maulik Sutariya on Unsplash

A report on the findings show how the attackers used social engineering techniques, counterfeit websites, including a fake iOS App Store download page, and an iOS app-testing website to distribute the fake apps to unsuspecting users.

Sophos researchers investigated the fake apps and found that many were very similar. Some included an embedded customer support 'chat' option. When researchers tried to communicate with the support teams using the chat, the replies they received used near-identical language. The researchers also uncovered a single server loaded with 167 fake trading and cryptocurrency apps. Taken together, this suggests that the scams could all be operated by the same group, according to Sophos.

In one of the schemes investigated, the scammers befriended users via a dating app, setting up a profile and exchanging messages with individual targets before attempting to lure them into installing and adding money and cryptocurrency to a fake app. If targets later tried to withdraw funds or close the account, the attackers simply blocked their access.

Resembling trusted brands

In other cases, targets were caught through websites designed to resemble that of a trusted brand, such as a bank. The operators even set up a fake “iOS App Store” download page featuring fake customer reviews in order to convince targets they were installing an app from the genuine App Store.

If people clicked on the links to download the fake apps for either Android or iOS, they received something that looked like a mobile web app, but was in fact a short-cut icon that linked to a fake website.

The operators also distributed some of the fake iOS apps via third-party websites that help iOS developers test new applications with a limited number of Apple device users before they submit apps to the official App Store.

People trust the brands and people they know – or think they know – and the operators behind these fake trading and cryptocurrency scams ruthlessly take advantage of that. The fake applications we uncovered impersonate popular and trusted financial apps from all over the world, while the dating site sting begins with a friendly exchange of messages to build trust before the target is asked to install a fake app. Such tactics make the fraud seem very believable.