First clipper malware discovered on Google Play

welivesecurity.com/2019/02/08/first-clipper-malware-google-play/

February 8, 2019

Cryptocurrency stealers that replace a wallet address in the clipboard are no longer limited to Windows or shady Android app stores

Lukas Stefanko
8 Feb 2019 - 11:58AM

Cryptocurrency stealers that replace a wallet address in the clipboard are no longer limited to Windows or shady Android app stores

For security reasons, addresses of online cryptocurrency wallets are composed of long strings of characters. Instead of typing them, users tend to copy and paste the addresses using the clipboard. A type of malware, known as a “clipper”, takes advantage of this. It intercepts the content of the clipboard and replaces it surreptitiously with what the attacker wants to subvert. In the case of a cryptocurrency transaction, the affected user might end up with the copied wallet address quietly switched to one belonging to the attacker.

This dangerous form of malware first made its rounds in 2017 on the Windows platform and was spotted in shady Android app stores in the summer of 2018. In February 2019, we discovered a malicious clipper on Google Play, the official Android app store.

Although relatively new, cryptocurrency stealers that rely on altering the clipboard’s content can be considered established malware. ESET researchers even discovered one hosted on download.cnet.com, one of the most popular software-hosting sites in the world. In August 2018, the first Android clipper was discovered being sold on underground hacking forums and since then, this malware has been detected in several shady app stores.

Copy&Steal

The clipper we found lurking in the Google Play store, detected by ESET security solutions as *Android/Clipper.C*, impersonates a legitimate service called MetaMask. The malware’s primary purpose is to steal the victim’s credentials and private keys to gain control over the victim’s Ethereum funds. However, it can also replace a Bitcoin or Ethereum wallet address copied to the clipboard with one belonging to the attacker.

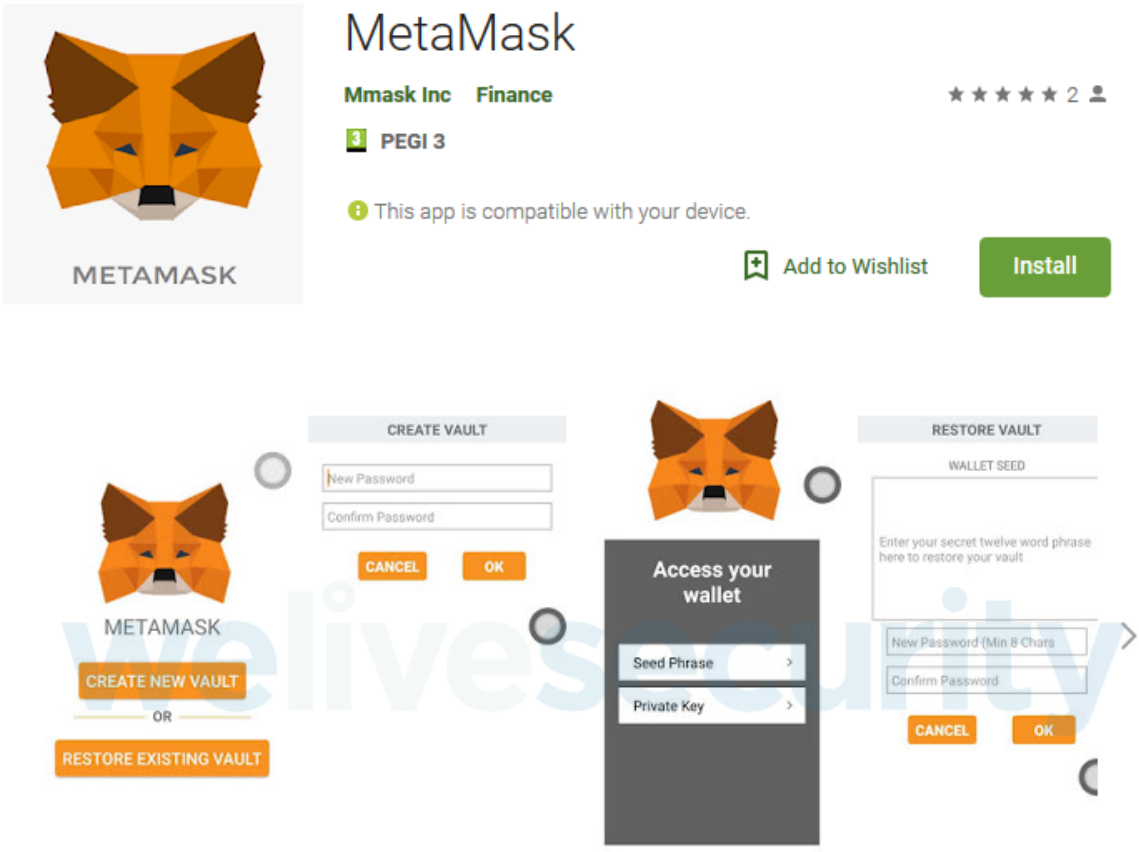

Figure 1. Android/Clipper.C impersonating MetaMask on Google Play

We spotted *Android/Clipper.C* shortly after it had been introduced at the official Android store, which was on February 1, 2019. We reported the discovery to the Google Play security team, who removed the app from the Store.

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.

Security tips

This first appearance of clipper malware on Google Play serves as another imperative for Android users to stick with the best practices for mobile security.

To stay safe from clippers and other Android malware, we advise you to:

- Keep your Android device updated and use a reliable mobile security solution
- Stick to the official Google Play store when downloading apps…
- …however, always check the official website of the app developer or service provider for the link to the official app. If there is not one, consider it a red flag and be extremely cautious to any result of your Google Play search
- Double-check every step in all transactions that involve anything valuable, from sensitive information to money. When using the clipboard, always check if what you pasted is what you intended to enter.

Indicators of Compromise (IoCs)

Package Name	Hash
com.lemon.metamask	24D7783AAF34884677A601D487473F88

BTC address: 17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA

ETH address: 0xfbbb2EF692B5101f16d3632f836461904C761965

8 Feb 2019 - 11:58AM