Android Clipper found on Google Play | video demo

web.archive.org/web/20201107225915/https://lukasstefanko.com/2019/02/android-clipper-found-on-google-play.html

Lukas Stefanko

February 10, 2019

The first Android Trojan Clipper – that exchanges cryptocurrency address in copied clipboard – was discovered on Google Play. Android Clipper targeted Bitcoin and Ethereum cryptocurrency addresses when being copied in to clipboard and replaced them with the attacker's wallet address. Once this transaction is sent, it can not be canceled.

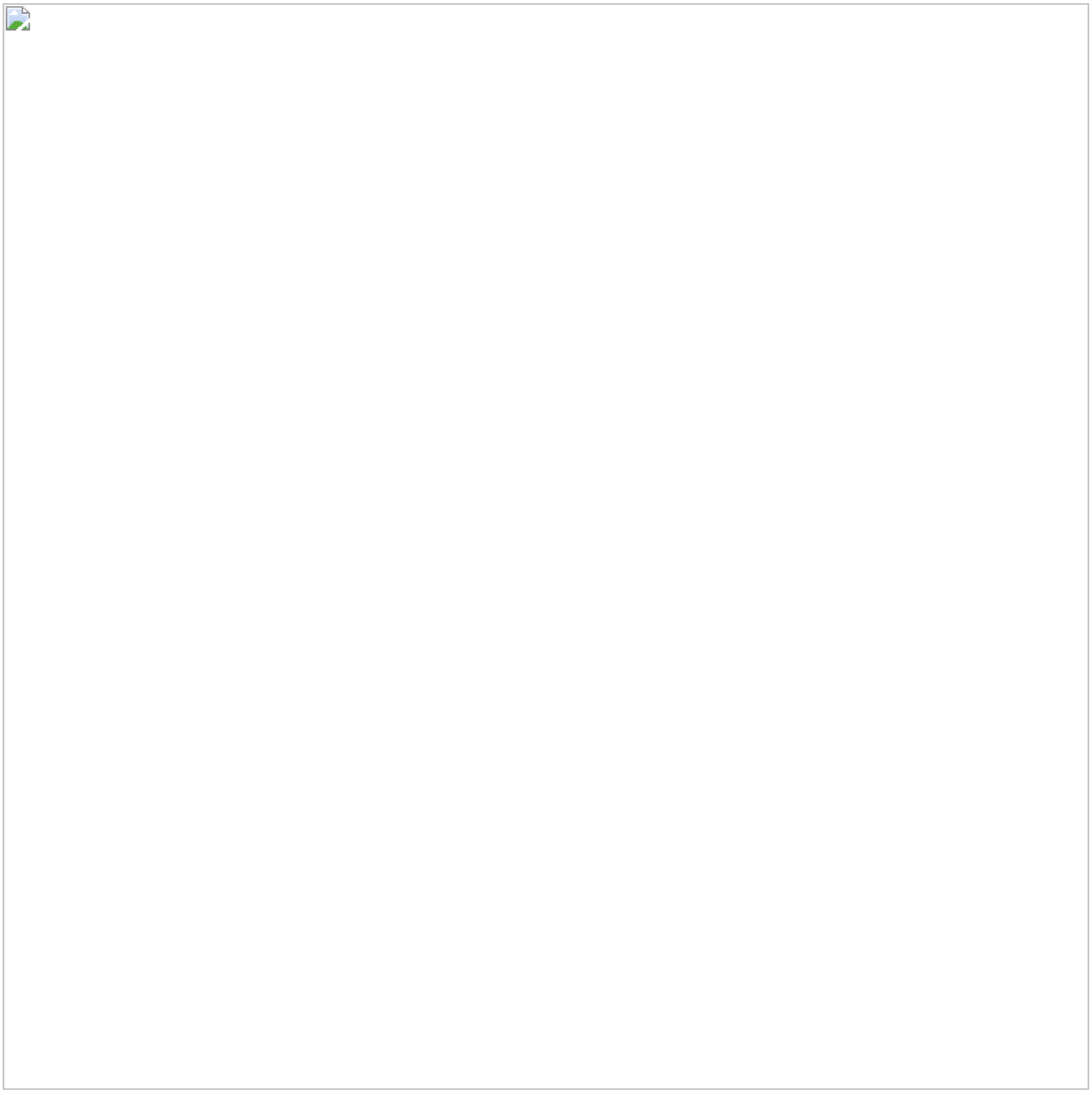

Figure 1. Replacing wallets in clipboard

Functionality

In the video I explained what is Clipper and demonstrated its functionality including possible attack scenario.

Attack Scenario

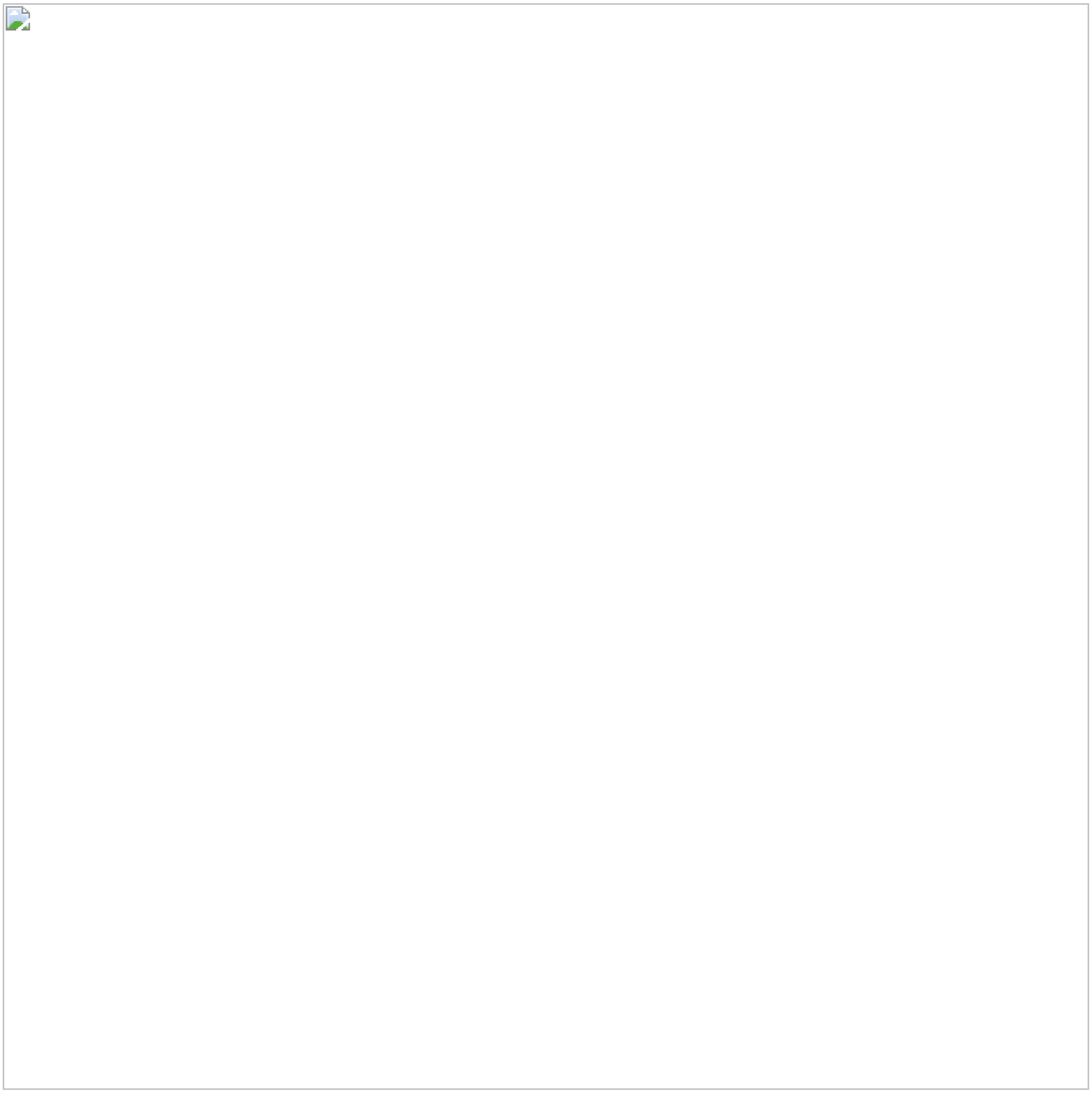

Figure 2. How Android Clipper works

History of Android Clipper malware

August 7, 2018 – Discovered first Android Clipper outside of Google Play by Dr. Web

February 8, 2019 – Discovered first Android Clipper in Google Play by ESET

Sample

Package Name	Hash
com.lemon.metamask	24D7783AAF34884677A601D487473F88

I test Android malware, so you don’t have to. Be Aware, Be Secure!