

本文由KEX News独家编译！

11月13日，恶意软件研究员Lukas Stefanko表示，其在Google Play商店中发现4款虚拟货币假钱包软件，这4款软件均存在盗取用户个人信息的风险。这些软件是NEO和USDT的钱包，是具有管理ETH功能的MetaMask，同时它们能够盗取用户移动银行认证信息和信用卡信息。

Stefanko将这几款假钱包软件分为两类，其中1款是钓鱼钱包，另外3款是假钱包。如果安装启动钓鱼钱包，需要用户和钱包的密码。他还指出，被称为“NEO钱包”的软件自从10月份在Google Play商店上架以来，安装量已经超过1000次。

虚拟货币假钱包不仅能够生成安全交易所需的公开地址和新钱包，还可以通过仅显示攻击者的公开地址获取用户信息。即便用户认为软件能够生成公开地址而存入虚拟货币，由于网络犯罪者掌握相关信息，用户也无法提取虚拟货币。

Stefanko指出，这些软件开发难度较低，即便不具备Coding知识也能够进行开发。换言之，当比特币价格上涨时，任何人均可简单地开发出恶意软件，盗取重要的个人信息。该研究员已经向Google安全团队反应虚拟货币假钱包问题，该问题已得到解决。

(文章来源于Cointelegraph)