“21%的操作存在截屏、录屏记录；26%未检测到系统运行环境；9%存在钱包APP伪造漏洞；6%交易密码未检测弱口令；38%核心代码未加固。”这些数字来自360集团信息安全部近日发布的一份《数字货币钱包安全白皮书》（以下简称“《白皮书》”）。

随着区块链的火热，数字货币也逐渐为投资者所熟知，但安全问题也随之而来。早在2014年，当时世界上最大的比特币交易所运营商Mt.Gox就被黑客窃取了85万个比特币，占当时全球比特币总数的7%；2017年11月份，以太坊钱包Parity被曝漏洞，导致价值2.8亿美元的93万个以太币被冻结；2018年1月份，日本数字货币交易所CoinCheck钱包被黑，价值5.3亿美元的新经币被窃。

所谓数字货币钱包，其实是管理诸如比特币等基于区块链技术的数字货币的应用。它一般提供钱包地址的创建、转账、交易查询等功能。数字货币钱包的“百花齐放”，对应的正是区块链技术在数字虚拟货币上的广泛应用。在我国，2017年区块链相关项目融资总额超过12.7亿元，融资事件54起，而仅在2018年第一个月，区块链行业融资额就达到6.8亿元，融资事件19起。

数字货币钱包的安全性从何而来？来自市场研究机构猎豹全球智库的一份研究报告显示：每个钱包地址都对应一个密钥对——私钥和公钥。公钥是根据私钥进行一定的数学运算生成，与私钥一一对应。公钥主要是对外交易使用，私钥则是数字货币钱包中唯一能够证明对数字资产有控制权的凭证，因此它的生成和存储方式决定了资产安全与否。助记词是明文私钥的另一种表现形式，因此能否安全地管理助记词也是区别钱包是否安全的重要条件。

正因如此，针对私钥和助记词的攻击也成为数字货币钱包最重要的安全隐患之一。《白皮书》介绍，根据使用时的联网状态不同，数字货币钱包分为“热钱包”和“冷钱包”。由于业务场景的快速迭代以及推广需求，两种钱包都存在不少安全隐患，但总体上来说，“热钱包”漏洞多于“冷钱包”，可被攻击的环节更多。360集团信息安全部负责人高雪峰表示：“拿‘热钱包’来说，如果新用户在创建助记词时，钱包没有进行截屏、录屏等操作的监测，就有可能造成助记词泄露，如果私钥生成过程的相关算法被逆向分析，那黑客就能得到私钥。”此外，数字货币钱包也同样面临着包括植入恶意代码、输入监听、转账地址篡改等常见网络攻击。

数字货币钱包为何会有如此多的安全隐患，对它的攻击又为何能频频得手？高雪峰认为，区块链兴起后，数字货币钱包的安全标准严重滞后，大部分钱包开发团队以业务优先为原则，对安全性未做足够的防护。黑客一旦瞄准钱包，找到漏洞，就会将账户货币洗劫一空，而且由于数字货币匿名、不可追踪等特性，被盗后难以追回。

目前，数字货币钱包的安全主要靠平台方加强安全审核。《白皮书》建议，数字货币钱包服务商要进行包括域名系统安全检测、主机实例安全检测、服务端应用安全检测等一系列审核，同时还要监控私钥、助记词、交易过程、数据存储的安全。而对于普通用户来说，能进行的安全防范则相当有限。

猎豹全球智库高级分析师刘鹏表示，对于普通用户来说，如果正在使用的加密数字货币钱包存在安全漏洞，应在开发商完成漏洞修补升级版本之前换用其他安全的加密数字货币钱包，并重新创建一个全新的钱包地址，通过转账的方式将旧地址的资产转移到新地址，最后将旧地址作废。

本文源自经济日报