本想着通过买虚拟币投资，

没想到遭到恶意程序捣鬼，

浙江宁波徐先生一下损失了3800余万元！

7月19日，宁波江北公安分局通报

一起新型黑客案件：

抓获黑客盗币团伙成员苏某等6人。

今年3月7日，徐先生向江北网安部门报案称：其手机虚拟币钱包被盗，160多万个泰达币被人转走，同时怀疑自己的电脑被远程操控，发送给好友的聊天内容被人替换，导致又有398万个泰达币、100个以太币被骗走。经专业部门鉴定，损失达3800余万元。

因为虚拟币常会被黑灰产团伙用于“洗钱”，因此民警介入调查，并对被害人电脑开展分析取证，然后就发现了名为svchsot.exe的可疑恶意程序。进一步侦查后，警方锁定了嫌疑人的身份。

6月9日，专案组在前期谋划、周密部署后，奔赴广东廉江，一举抓获黑客盗币团伙成员苏某等6人，现场扣押涉案电脑9台、手机10部、远程服务器26台。

经查，嫌疑人苏某（男，28岁）等人，利用钓鱼网站或是发送伪装成社工文档的木马文件等方式，诱导用户下载木马程序，实现远程控制被害人电脑，非法获取他人电脑内的敏感文件，盗窃、诈骗虚拟币进行套现获利百余万元。

目前，该6人因涉嫌非法获取计算机信息系统数据、非法控制计算机信息系统罪被采取刑事强制措施。另外，就报案人持有大额虚拟币的情况，公安部门已通报相关主管部门予以关注。目前，相关侦查工作还在进一步推进中。

“请大家注意，在我国，虚拟币不具有与法定货币等同的法律地位，不具有法偿性。但个别人依旧盲目认为虚拟币具有升值空间并高价囤积。实际上，很多人其实并不真正了解虚拟币。一旦发生私钥或助记词泄露，就会被不法分子轻而易举盗窃，且无法追回。”办案民警说，2021年9月15日，人民银行、最高法、最高检、公安部等10部门就联合发布《关于进一步防范和处置虚拟币交易操作风险的通知》，明确虚拟货币和相关业务活动的本质属性，严禁虚拟币作为货币在市场上流通使用，虚拟币相关业务活动属于非法金融活动。

除了关于“持币风险”提醒外，民警还建议大家赶紧自查一下自己的电脑：

1.检查电脑启动项里（C:Users用户AppDataRoamingMicrosoftWindowsStart MenuProgramsStartup）有无“显卟稳定.lnk”“AudiorHDriversvs.lnk”等可疑文件；

2.检查电脑公用下载里（C:UsersPublicDownloads），有无“AudiorHDriversvs.lnk”“Program Files”（svchsot.exe）等可疑文件。

（江北公安）