美国公司Foley＆Lardner进行的一项研究表明，71％的大型加密货币交易商和投资者认为，加密货币盗窃主要原因是来自恶意软件和黑客的袭击。另外，31％的受访者认为黑客对全球加密货币行业形成了巨大威胁。

然而，Poloniex团队并没有为Android开发应用程序，其网站也没有任何移动应用程序的链接。根据ESET的恶意软件分析师Lukas Stefanko的说法，在从Google Play中删除该恶意软件之前，已有5500名交易者受到了影响。

另一方面，iOS设备的用户会经常下载到隐匿矿工的App Store应用程序。为此，苹果公司甚至被迫收紧了对其商店的应用程序的准入规则，以便暂停此类软件的发布。不过，用户下载应用后，隐匿的矿工只会减慢移动设备的操作速度，这相比安卓手机黑客对钱包的侵犯与破坏，有着明显的不同。

Slack平台上的机器人

小贴士：

① 举报屏蔽Slack机器人。

② 无视机器人的活动。

③ 使用Metacert或Webroot安全机器人、Avira防病毒软件甚至内置的Google安全浏览功能来确保Slack通道的安全。

自2017年年中以来，Slack聊天应用迅猛发展，与此同时，旨在窃取加密货币的Slack机器人也为该公司埋下了祸害。通常情况下，黑客会创建一个机器人，通知用户其加密货币存在一些问题，然而，这么做的目的实则是强制用户单击相关链接并输入私钥。

加密货币交易附加组件

小贴士：

① 使用单独的浏览器进行加密货币操作。

② 选择隐身模式。

③ 不要下载任何加密附加组件。

④ 使用单独的PC或智能手机，仅用于加密交易。

⑤ 下载防病毒软件并安装网络保护程序。

为了让用户更轻松地使用钱包和进行交易，互联网浏览器提供了自定义用户界面的扩展服务。即便问题不在于附加组件会读取用户在使用互联网时输入的所有内容，但这些扩展是在JavaScript上开发，这就使得它们极易受到黑客攻击。

原因在于，近年来，随着Web 2.0，Ajax和富Internet应用程序的普及，JavaScript及其随之而来的漏洞已经变得非常普遍。此外，鉴于用户的计算资源，许多扩展应用可用于隐藏挖掘。

通过短信认证

小贴士：

① 关闭呼叫转移，使攻击者无法访问自己的数据;

② 在文本中发送密码时，不要使用通过短信提供的双因素认证识别，而是使用双因

素认证识别软件解决方案。

由于智能手机的便捷性，许多用户会习惯性地选择使用移动身份验证。 Positive Technologies是一家专门从事网络安全的公司，它曾经做过的一次演示表明，通过信令系统7（SS7）协议，对在全球范围内传输的密码确认短信进行拦截，这很容易就可以实现。

借助自己的研究工具，专家们能够轻易地劫持短信，而这其实是利用了蜂窝网络的弱点，以对传输中的文本信息进行拦截。此外，一次Coinbase帐户的演示也让交易所的用户感到震惊。

表面上看，这是Coinbase存在的漏洞，但真正的问题在于蜂窝系统本身。这就说明，即使是使用2FA，也可以通过SMS直接对任何系统进行访问。

公共Wi-Fi

小贴士：

① 即便是使用VPN，也不要通过公共Wi-Fi进行加密货币交易活动。

② 随着硬件制造商不断发布旨在防止密钥被替换的更新内容，记得定期升级更新自己的路由器固件。

去年10月，在使用路由器的Wi-Fi保护访问（WPA）协议中，就发现了一个不可恢复的漏洞。在执行基本KRACK攻击（重新安装密钥的攻击）之后，用户的设备重新连接到了黑客的相同Wi-Fi网络。

因此，用户通过网络下载或发送的所有信息，包括来自加密钱包的私钥信息，都可供攻击者使用。对于火车站、机场、酒店和人流量大的地方的公共Wi-Fi网络来说，这个问题显得尤为迫切。

站点克隆和网络钓鱼

小贴士：

① 在没有HTPPS协议的情况下，禁止与加密货币相关的站点进行交互。

② 使用Chrome浏览器时，对显示子菜单的地址的扩展名进行自定义设置。

③ 在从任何与加密货币相关的资源接收消息时，将链接复制到浏览器地址字段，并将其与原始站点的地址进行比较。

④ 一旦出现可疑，关闭窗口并删除收件箱中的信件。

自“互联网革命”以来，人们就已经知道这些古老的黑客攻击手段，但它们似乎仍旧在兴风作浪。

第一种可能的情况是，攻击者在仅仅一个字母之差的域名上创建原始站点的完整副本。这一把戏的目的（包括替换浏览器地址字段中的地址）是为了引诱用户访问经克隆的网站，并强制他们输入帐户密码或密钥。

在第二种情况下，他们会蓄意发送一封电子邮件，其风格设计完全复制官方项目的信件，但实际上，它旨在强迫用户点击链接并输入个人数据。

根据Chainalysis的消息，诈骗者通过使用这种方法，已经窃取了价值2.25亿美元的加密货币。

隐匿挖矿和常识

好消息是，由于加密货币服务越来越多的抵制，以及用户自身水平的提高，黑客逐渐失去了对钱包进行野蛮攻击的兴趣。当前，黑客的焦点是隐匿挖矿。

根据McAfee Labs的数据，在2018年第一季度，全球共有290万个用于隐藏挖矿的病毒软件样本。相比2017年最后一个季度，增加了625%。这种方法被称为“加密货币劫持”，由于其实施操作简单，黑客们对其甚是喜爱，以至于他们开始大量采用这一伎俩，并且逐渐放弃了传统的勒索窃取计划。

坏消息是，黑客攻击的活动并没有减少。从事网络安全业务的Carbon Black公司的专家透露，截至2018年7月，暗网上大约有1.2万个交易平台为黑客供应信息。在这样的平台上，销售恶意攻击软件的平均价格约为224美元。