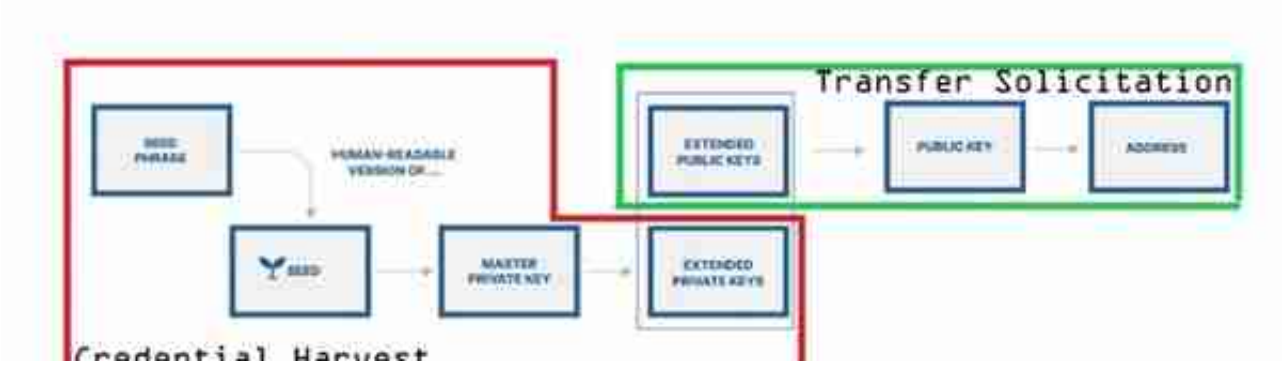
网络犯罪分子正在冒充 Binance、 Celo 和 Trust Wallet 等流行的加密平台，伪造电子邮件和虚假登录页面，试图窃取登录细节，并欺骗性地转移虚拟资金。

Proofpoint 在一份新报告中表示: “随着加密货币和不可替换令牌(NFT)变得更加主流，并因其赖以成名的波动性，个人成为数字货币欺诈行为受害者的可能性正在大大增加。”

“加密货币的兴起和扩散，也为攻击者提供了一种新的金融榨取方法。”

微软365防御研究小组(Microsoft 365 Defender Research Team)最近呼应了威胁行为者将敏感的加密货币数据作为攻击目标的做法，该小组警告称，私人密钥、种子短语和钱包地址正在受到一种被称为“冰箱软件（cryware）”的威胁，其目的是通过欺诈性转账窃取虚拟货币。



这些有针对性的活动的一个关键推动因素是，使用网络钓鱼工具可以相对容易地制作假冒登录页面，从而使技术不熟练的威胁行为者能够大规模分发和管理这些活动。

进一步刺激网络犯罪计划的是像 BulletProofLink 这样的“网络钓鱼即服务”(PHaaS)运营商，它们提供网络钓鱼模板、垃圾邮件服务、防弹托管服务和证书收集服务等。

这些工具包不断更新和扩展，旨在模仿不同的品牌，如blockchain[.]com以及其他 NFT 和其他加密货币钱包服务提供商。

同样引人注目的是商业电子邮件妥协(BEC)试图通过以供应商付款和捐赠请求为幌子的加密货币信息来促进数字硬币的欺诈性转移，以支持乌克兰战争的努力。

2021年，加密相关犯罪造成的损失同比增长了79% 。美国联邦贸易委员会(FTC)指

出，有超过4.6万人报告称因诈骗而损失了超过10亿美元的数字货币。