Lendf.Me 遭攻击引发的反洗钱与刑事防御思考

继北京时间 4 月 18 日上午 8:58Uniswap 平台遭受重入攻击后，Lendf.Me 于北京时间 4 月 19 日上午 8 点 45 分再次遭受攻击。据悉，两次攻击手法极为类似，推断为同一团体或个人所为。

黑客均利用 ERC-777 标准与其他平台的兼容性问题，在进行 ETH-imBTC 交易时连续利用智能合约提取资金，执行重入攻击，反复覆盖自己的资金余额，实现可提现资金的不断翻倍，进而循环套利。Uniswap 预计损失了 30 万美元至 110 万美元的资金，Lendf.me 借贷平台预计损失约 2500 万美元的资金。

Lendf.Me 于去年 9 月推出，是由 dForce 主导开发的去中心化借贷市场协议。

ERC-777 是以太坊区块链的基础技术之一，旨在支持智能合约（Lendf.me 和 imBTC 都在以太坊平台上作为智能合约运行）。

imBTC 在以太坊平台上运行的以 1:1 锚定比特币的 ERC-777 代币（兼容 ERC-20 ），采用 ERC-777 代币标准规范，由 Tokenlon 负责发行和监管。

此次 dForce 遭受黑客攻击事件，是自今年 2 月份 bZx 攻击事件后，又一起利用 DeFi 的系统安全性漏洞进行的攻击。

慢雾安全团队提醒交易所、钱包注意加强地址监控，避免相关恶意资金流入平台。去中心化交易平台 Tokenlon 已宣布暂停 imBTC 合约的转账功能。dForce 创始人杨民道写给公众的信中也表示“…（我们将）与主流交易所、OTC 交易商、公安机构积极配合展开相关调查，竭尽全力追索被盗款项，追踪黑客动态…”

Lendf.Me 黑客攻击事件引发的反洗钱思考

黑客通过非法手段获得的加密货币，俗称“黑钱”，难以“安全”地使用。为了避免公安机关的追踪，势必要对非法来源的资金进行掩饰，使其看起来“合法”、“清白”，而通常采取的掩饰手段便是借助交易所和 OTC 交易商的力量，通过复杂的交易使资金来源难以追溯。正如此次攻击中，黑客不断通过 1inch.exchange、ParaSwap、Tokenlon 等 DEX 平台将盗取的币兑换成 ETH 及其他代币，完成代币的转移。

洗钱过程并非难以察觉，如果交易所和 OTC 交易商能够做好客户信息搜集、尽职调查和信息保存工作，并能将动态及时上报，那么非法资金的流动是可以被

及时发现并引起警方注意的。并在最大程度上切断资金外流通道，追回赃款，挽回加密货币持有人的损失。监管机构或调查金融犯罪等机构也得以通过搜集到的各方面信息进行梳理、比对，逐步还原资金流向。

实践中，黑客洗钱的步骤会更加繁琐，将资金进行拆分并转入不同的地址，大额的资金会沿着前进方向进一步小额拆分，进而构建出更为复杂、繁密的资金网络，加大追踪、侦测的难度。如果交易所和 OTC 交易商在客户信息搜集、尽职调查、信息保存及上报方面的工作不到位，非法资金将难以被及时发现、上报并实现有效的追缴，损失将无法挽回。

北京时间 4 月 19 日晚 10 点左右，Lendf.Me 攻击者(0xa9bf70a420d364e923c74448d9d817d3f2a77822)刚向 Lendf.Me 平台 admin 账户(0xa6a6783828ab3e4a9db54302bc01c4ca73f17efb)归还 126,014 枚 PAX，并附言「Better future」。

看起来着实有些讽刺，但这次攻击也提醒加密货币交易平台应当更注重对交易参与者信息的收集工作，保证交易信息的透明度，从而构建真正的「Better future」。

Lendf.Me 黑客攻击事件引发的刑事思考

黑客入侵、加密货币被盗事件已不是第一次发生，黑客对加密货币的强烈渴望随着加密货币的价值攀升愈发强烈，他们通过利用合约漏洞、入侵技术支持网站、攻击加密钱包等多种方法非法盗窃加密货币，给加密货币持有者带来了不小的损失。

有少数观点认为，黑客的行为利用了合约漏洞，某种意义上是被合约所允许的。但是代码漏洞不等于同意，无论链上链下，盗窃行为的本质并没有发生改变，黑客理应为他们的行为承担刑事责任。

2019 年 3 月，日本一名 18 岁的黑客因盗窃加密货币被日本宇都宫的检察官起诉。他通过入侵智能手机上的数字钱包 Monappy，盗窃了价值 1500 万日元(约合 13. 42 万美元)的加密货币。

2019 年 4 月，美国 21 岁的乔尔·奥尔蒂斯（JoelOrtiz）因利用 SIM 卡对受害者的智能手机进行黑客入侵，共窃取了 40 余名用户约 750 万美元的加密货币，面临身份盗用和计算机犯罪等 41 项罪名的指控，最终被判入狱 10 年，这也是美

国有史以来第一个因“SIM 卡交换诈骗”而定罪的案子。其他参与人员也分别因窃取不同数量的加密货币而被批捕。

2019 年 5 月，20 岁的爱尔兰男子康纳·弗里曼（Conor Freeman）因涉嫌在网上盗取价值超 200 万美元的比特币等加密货币，面临网络诈骗、教唆诈骗等多重指控，或将在美面临超 100 年的监禁。

2020 年 2 月，前微软员工 Volodymyr Kvashuk 因从微软盗窃 1000 万美元的数字货币，被判犯有 18 项联邦重罪，将面临 20 年的监禁。

可以看到，包括盗窃行为在内，黑客针对加密货币所进行的的犯罪行为都会受到刑事法律的规制，从判决结果来看，黑客也将面临较为严厉的刑罚。本案中，黑客的攻击行为造成了 Lendf.Me 约 2500 万美元的资产损失，刑事制裁在所难免。

犯罪行为本身的应罚性毋庸置疑，但加密货币定性的不同可能指向不同的罪名，这点在我国表现的尤为突出。在加密货币的性质归属上，我国并没有形成一致的观点，加密货币被盗面临着盗窃罪和非法获取计算机信息系统数据罪两个不同的保护路径，前者肯定了加密货币的财产属性，后者则将加密货币视为信息。需要注意的是，两者在量刑上存在较大差距，盗窃罪量刑要远远高于非法获取计算机信息系统数据罪，这给司法实务留下了很大的不确定性。

不止我国，包括美国在内的一些国家在加密货币的定性上也未能达成一致：美国商品期货交易委员会（CFTC）将加密货币视为商品；美国证券交易委员会（SEC）将符合 HOWY 测试的加密货币视为证券；美国金融犯罪执法网络（FinCen）将加密货币视为在一种特定情况下扮演货币功能的交换媒介，可以适用货币规则；美国国税局将加密货币视为一种财产，具有合法的财产属性，需缴纳税收。

赋予加密货币明确的定性是各国都在努力的方向，对于更好的引导、管理加密货币活动具有重要的意义。

从执行角度看，区块链的不可篡改性的确为警方追踪资金去向提供了可能，但去中心化的特征也为黑客隐匿身份创造了空间，他们往往通过复杂的手段将加密货币分散，再进行洗钱、提币、洗币等操作，加大警察溯源的难度。

当然这并不意味着黑客的行为将毫无漏洞，黑客盗窃的目的最终是为了变现，而变现的途径无非是场外交易或交易所交易。黑客一旦向一个已知身份的用户进行转账，将很有可能暴露自己的身份，从而露出马脚。实务中，由于加密货币的走向往往跨越国界，追踪过程不是靠一己之力能够完成的，还需要借助国内外等多方力量的协助，执行起来要复杂得多。

然而，即便能够准确定位黑客的身份和位置所在，将丢失的加密货币全部追回的可能性也并不大。加密货币安全公司 CipherTrace CEO 大卫·埃文斯(David Jevans)曾表示，当交易平台或交易所遭到黑客攻击，由于加密货币可以轻易地跨越不同的国界，只有 20%的被盗加密货币能够找回。

接连两次的攻击都在警示我们，保障加密货币的安全不能仅依靠区块链技术本身的优势，可以看到黑客已经掌握了 DeFi 系统性风控漏洞的要害，无论是加密平台还是加密货币持有者，都应当提高风险防范意识。

对加密平台而言，尽可能的弥补技术短板，提升交易信息的透明度，并完善相应的反洗钱预警机制，在第一时间对加密货币风险作出反应。

对加密货币持有者而言，无论是反洗钱机制还是刑事法律制裁，都只能起到事后救济的作用，而目前制度框架还处在搭建和完善中，未必能提供强有力的保护。因此，提高警惕心理，妥善保管交易密钥，强化账户认证端口才能尽到最大程度的事前防范。

（来源：巴比特资讯。转引自：复旦大学中国反洗钱研究中心。网址：http://www.ccamls.org/newsdetail.php?did=37003。时间：2020 年 4 月 24 日。访问时间：2020 年 4 月 28 日 9:30。）