写作： Mortyn原文标题与链接： Shuming hao123 @ QQ.com [xy 002] [xy001] n昨天，Yam Finance成功阻止了对其储备资金库的管理攻击。
在这次攻击中，攻击者偷偷地通过内部交易提出了治理建议。 这一恶意治理提案包含未经验证的合同，目的是最终将Yam的协议资金储备转移到攻击者的钱包中。
如果成功，Yam Finance将损失310万美元。

攻击者采用了非常常见的攻击手段——治理攻击，治理在DeFi协议中的广泛应用，使得治理攻击也成为黑客在链上获利的主要手段之一。

区块链的理念是“Code is Law”，因此高度依赖于链上的治理。 最简单、直接的途径是通过令牌赋予持有者治理权重，令牌越多，治理权重往往越多。 货币持有者可以参与协议的提议和管理，建议内容可能很复杂和简单，但通过后会影响整个协议的运行和发展。

直观地看，这符合持有硬币的人的利益。
因为持有硬币的人越多，持有硬币的人就越不能提出违反自己利益的建议和投票。
但是，一些封锁价值高的DeFi合同，只要攻击成本低于利润，就有人想尝试。 当LUNA/UST崩溃时，Terra停止了区块链的封锁避免在LUNA大规模增发过程中可能带来的潜在低成本管理攻击。 [xy 002] [xy001]除了yam finance这次攻击没有结果的情况外，攻击成功的情况也不少。
例如，今年2月15日，Build Finance受到治理攻击，攻击者通过增发令牌获利。
攻击成功后，攻击者现在可以完全控制治理协议、铸造密钥和Treasury。
在这次攻击之后，Build Finance令牌失去了所有价值，等于零。

除了通过掌握大量令牌进行攻击外，黑客还会在某个时刻增加节点的提案数量，通过伪装成正常的治理提案来提高提案通过的可能性。

去年圣诞节，Terra公链上的合成资产协定Mirror也经历了非常严峻的考验。 攻击者准备充分，在以下四点上提高提案通过的可能性目标利润为3800万美元的MIR令牌。 n-攻击者准备了数百万美元的MIR令牌。n-攻击时间节点是圣诞节，大多数货币持有者都关心生活中的事情把n-提案而不是链条伪装成“与Solana的深度合作”的n-同时发起了多个提案，敷衍了事。 对此，MakerDAO的创始人Rune Christensen表示：“目前、达奥的“基本博弈论问题”是统治攻击等问题。 简而言之，像DeFi这样真正控制大部分有投票权的股票的人可以直接窃取合同中的所有资产。 “

这很令人担心另一个广泛的担忧是投资者对管理令牌本身价值的质疑。 对大多数DeFi协议来说，使用令牌数简单判定治理权重多寡的行为是一条捷径，更多的协议在治理方面创新较少，大多是Fork的先行者。 当然在治理方面也有创新的人。 例如

，Curve推出了veToken治理模式，AC基于veToken推出了veNFT，而第2层优化也通过本机令牌OP对治理进行了分层。

最令人担忧的是，进入熊市周期后，令牌价值下降可能会降低攻击成本，治理攻击的数量可能会成倍增加。 在风险激增的情况下，高概率激励开发者/项目团队在治理方面进行更多思考，挖掘令牌治理方面的潜力