EOS回滚攻击手法之重放篇

by yudan@慢雾安全团队

事件背景：

据慢雾区情报，今日凌晨，攻击 BetDice、ToBet 等游戏的黑客团伙再次对 LuckyMe、GameBet 发动攻击，造成数千 EOS 的损失。

经过慢雾安全团队的分析，此次黑客采用的手法有别于上一次的攻击。本次的攻击为针对项目方的重放攻击。

攻击回顾：

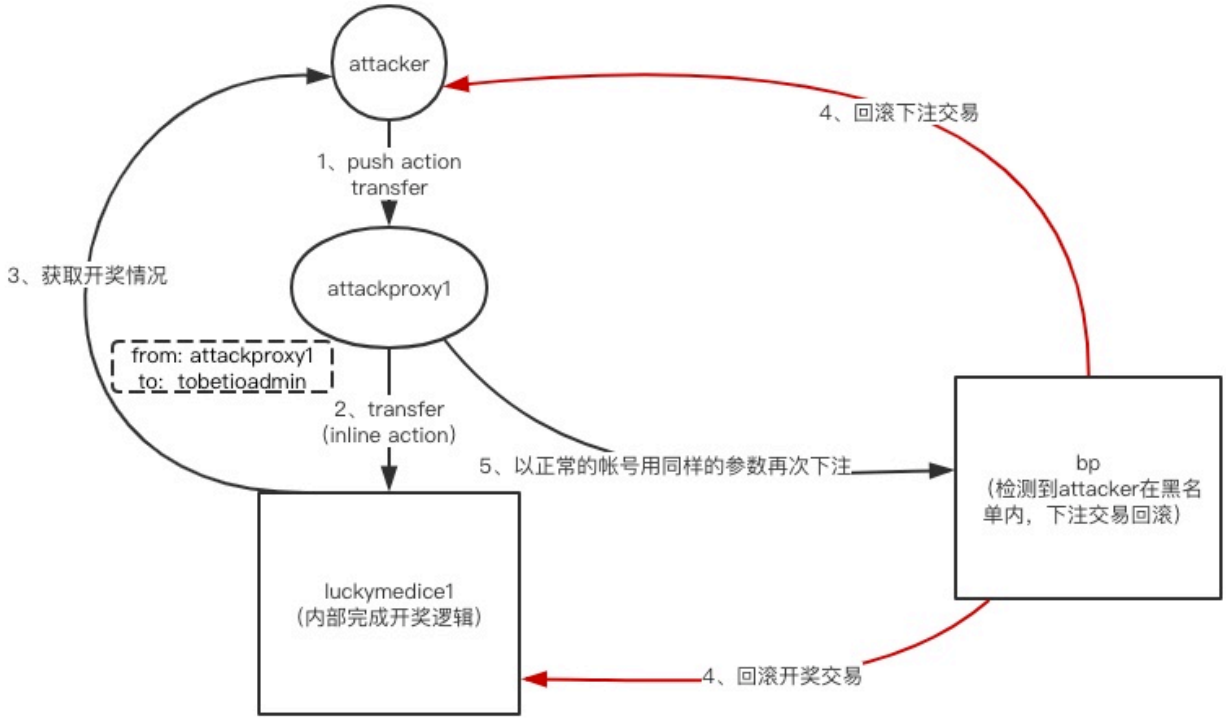
据慢雾安全团队威胁情报分析，截止北京时间上午8时，攻击者ultnavrzhium此次攻击共投入金额3773.95 EOS，收入6906.6 EOS，共获利3132.65 EOS。

攻击手法：

本次攻击手法与上一篇文章（地址链接：https://mp.weixin.qq.com/s/WyZ4j3O68qfN5IOvjx3MOg）有所不同。但依然利用到了黑名单的手法。以下是攻击详细过程。

(1)第一步，攻击者调用非黑名单合约的 transfer 函数，函数内部有一个 inline action 进行下注，from 填写的是攻击者控制的非黑名单合约帐号，to 填写的是游戏合约帐号。这时，攻击者发送交易是发向游戏合约自己的全节点服务器。使用的是黑名单帐号进行。
(2)第二步，游戏节点读取到了这笔交易，立刻进行开奖，如果中奖，将对攻击者控制的非黑名单帐号发送 EOS。到这里和上一篇黑名单篇的第一步和第二步都是一样的。
(3)第三步，因为项目方开奖和交易id绑定，所以按照上一篇文章的说法,下注交易和开奖交易都会被回滚。即使项目方给攻击者开奖了，到了bp节点的时候，由于查询不到开奖id，开奖交易也会失败。所以为什么还是能攻击成功呢？答案在第四步
(4)上一篇文章说到，在攻击者攻击的时候，所有的逻辑都是在项目方的节点完成的，根据这一点，攻击者就可以在项目方节点广播交易时监听到开奖结果，如果这笔下注是中的，立马以同样的参数（如种子）使用攻击者控制的同一合约帐号发起相同的交易，actor为合约帐号本身，即可成功中奖。

本次攻击可以参考下面的图：



防御建议：

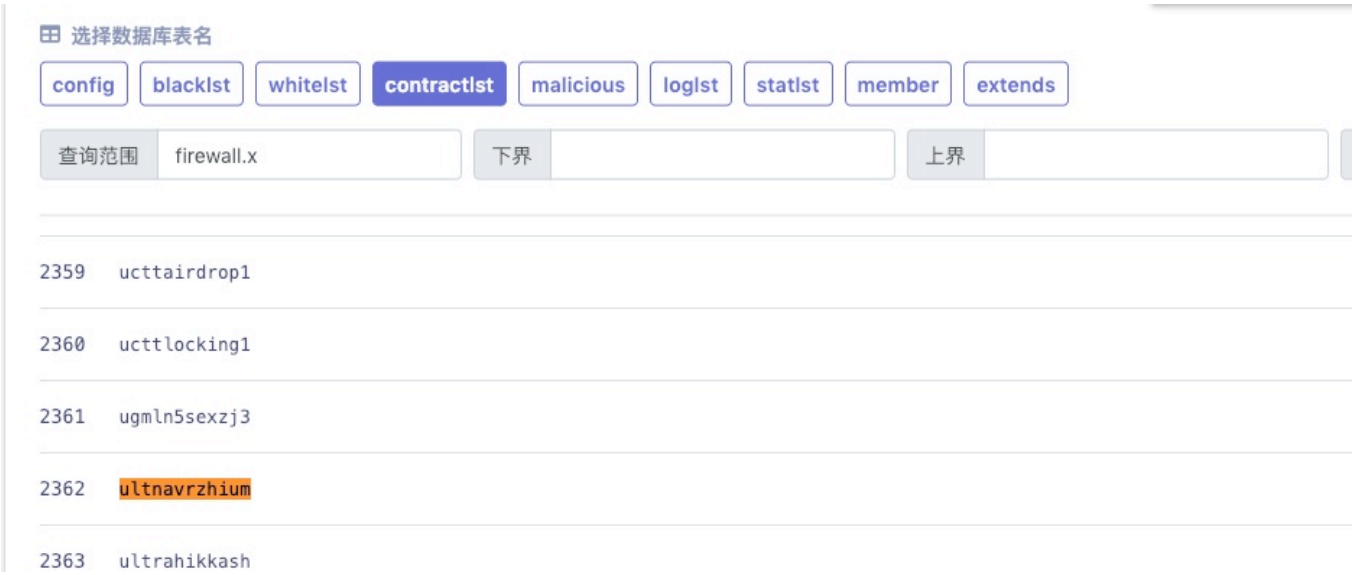
1、节点开启 read only 模式，防止节点服务器上出现未确认的块

2、建立开奖依赖，如订单依赖，开奖的时候判断订单是否存在，就算在节点服务器上开奖成功，由于在 bp 上下注订单被回滚，所以相应的开奖记录也会被回滚。

3、项目方在玩家下注的时候校验交易中的`actor`和`from`是否是同一帐号。

4、接入慢雾安全团队孵化的DApp防火墙--FireWallX(体验地址：https://firewallx.io/console/index.html)，本次LuckyMe攻击者帐号（ultnavrzhium）在LuckyMe被攻击前已在防火墙合约监控名单中。

查询地址：https://www.eosx.io/account/firewall.x?mode=contract&sub=tables&table=contractlst&lowerBound=&upperBound=&limit=10000



参考链接：

慢雾安全团队分析文章：https://mp.weixin.qq.com/s/WyZ4j3O68qfN5IOvjx3MOg