2019年1月，黑客攻击了新西兰的虚拟货币交易所 Cryptopia，盗取了以 ETH 为主的数字资产（当时价值1,600万美元左右）之后销声匿迹。近日，随着币价的攀升，该黑客在沉寂了数月后，开始密集的洗钱行动。据 PeckShield 数字资产护航系统（AML）数据显示，近两天来，该黑客已经将4,787个 ETH 转入了火币交易所，而且仍有26,003个 ETH 等待被洗时机。

PeckShield 安全人员梳理黑客洗钱路径发现：

1、黑客在攻击成功后，一般会将资产分散到多个地址或直接转移到新地址后沉寂一段时间以避开风头；

2、在洗钱过程中，黑客会先转移出少部分资产进行尝试，寻找最佳洗钱方式；

3、在少部分资产尝试清洗成功后，才会处理剩余资产，否则会继续沉寂等待时机。

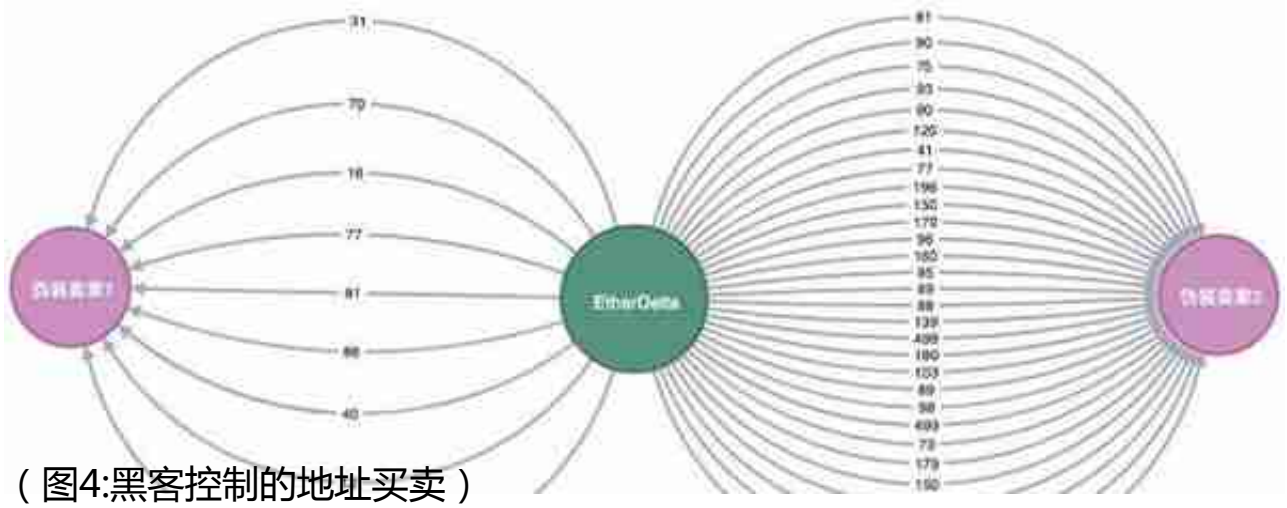
从本次洗钱路径看，黑客是有通过去中心化交易所 EtherDelta，以BAT、ELF 等代币配对交易，进行伪装买卖，逃离追踪的想法。不过，纯链上交易信息清晰可查，黑客虽魔高一尺，但白帽安全人员布下了天罗地网，能层层剖析，抽丝剥茧清晰还原黑客洗钱的全过程。

一图概览黑客洗钱全过程：

（图2:黑客将部分资产转移到一个新地址）

第二步：伪装买卖

黑客为了逃避资产追踪，一般会将大额资产，以小额多笔的形式分散到大量的地址中，再在各个地址上进行频繁的分散汇聚。而此次黑客采用了一种新方式，通过伪装成去中心化交易所的买家和卖家，试图以正常的挂单配对交易来逃避追踪。



（图4:黑客控制的地址买卖）

黑客将每次收到的1,000 ETH，再散成以约500个 ETH 一笔进入去中心化交易所，开始买卖。从图3和图4中发现，黑客以普通用户的方式，不是仅用一两笔，而是通过大量多笔的交易，完成从买家到卖家的资产转移。

伪装买家卖家，买卖 BAT、ELF 代币

下图中可以看到黑客控制多个帐号伪装成买家和卖家将资产倒手，图中是黑客成交的多笔 ELF 和BAT 代币的订单。

（图5:黑客伪装成买家交易 ELF、BAT 代币）

具体来看买家在去中心化交易所 EtherDelta 合约上的一条交易（trade）记录

（图7:卖家在 EtherDelta 上的提现记录）

第三步：再次汇聚，进入交易所

通过去中心化交易所的倒手交易后，黑客已认为能够避免资产被追踪，又将获得的ETH汇总到一个地址，并分批次进入火币交易所。