因Defrost Finance被盗而损失1200万美元的大户Hoi昨晚松了一口，昨晚近12点，他在推特上写到“天亮了”。一个多小时前，Defrost Finance公告称黑客已退还资金，将很快退还给用户。

虽然最终是大欢喜的结局，但依旧被用户扣上了“自导自演”的帽子。

时间拉回圣诞节当天，12月25日，Avalanche生态原生稳定币项目Defrost Finance协议被爆出再次出现问题，协议被添加了假的抵押代币，并使用恶意价格预言机清算当前用户，损失估计超过1200万美元。Defrost Finance官方表示，已注意到V1 出现的紧急情况，团队目前正在调查，恳请社区等待更新，暂时不要使用V1或V2。

而就在两天前，12月23日，Defrost FinanceV2曾遭到黑客的闪电贷攻击，黑客获利173,000美元，但因为V1并没有提供闪电贷服务，因此未受到影响。

随后，名为Hoi的用户发推特并在社区内求助，称Defrost Finance中的大部分存款都由其提供，其个人损失了1200万美元，审计公司CertiK尚未回应，并请求大家提供线索。

不久后，Hoi再次发推称已经掌握了一些项目方的实名线索，并认为项目方是监守自盗。因为在在V1被盗前一天，V2的所有钱都被盗了；V1的所有接口都有写防重入，V2的竟然没有写；他猜测团队一直想做大V2，这样攻击时可以推脱是第三方攻击，因为V2被攻击时可以由第三方通过闪电贷触发。但是V2里面的钱实在太少了，不够团队的胃口。所以第二天铤而走险直接用开发者权限。强行更改了预言机价格、铸币给自己、弄了一个新的抵押池，这些操作不可能由第三方触发。开发团队熊市赚不到钱估计就把心一横了，反正现在项目只有我一个傻大户放钱在这，估计也没啥人维权，就偷了。

据区块链安全审计公司Beosin分析，攻击者通过setOracleAddress函数修改了预言机的地址，随后使用joinAndMint函数铸造了100,000,000个H20代币给0x6f31地址，最后调用liquidate函数通过虚假的价格预言机获取了大量的USDT。后续攻击者通过跨链的方式将被盗资金转移到了以太坊的0x4e22上。这与Hoi分析的操作情况相吻合。

12月25日下午8点，Defrost发推称，团队愿意与黑客谈判，愿意分享20%的被盗资金以换回大部分被盗资产，具体金额可以协商，并呼吁黑客尽快和我们联系。”

12月26日下午，Defrost Finance的审计公司CertiK发推称，监测显示，Defrost

Finance项目为退出骗局（exit scam），CertiK曾试图联系该团队的多名成员，但没有得到回应。此外，CertiK还表示“该团队未进行KYC，但是我们正在利用我们掌握的所有信息协助当局”。这似乎把Defrost监守自盗的行为，盖棺定论。

或许是“黑客”的个人信息被掌握，因此选择迅速归还资金。Defrost Finance在26日晚10点发推表示：“被黑客入侵的资金已退还给DefrostFinance。受影响的用户将很快能够收回他们的资产。”

至此，这起黑客事件，仅用了2天就有了个愉快的大结局。但这对于安全公司和生态也敲醒了警钟。

Hoi在推特上回顾自己为何会选择这个矿时列了几点原因，1
合约我自己和员工都看过没问题的，第三方黑客黑不到。2 Certik等审计。3
这个项目上过很多Avax各种平台的推广，甚至官方号推荐。4
后来想出来时发现其他Defi矿的收益都一般，然后社区里面都是好说话的兄弟。

审计公司竟然没有对被审计项目的团队有基本的了解，仅合约的安全并不能防止主观的恶意，因此掌握团队的KYC必不可少。因此也有用户质疑CertiK，既然团队拒绝KYC，你们就应该拒绝提供审计。此外，Avalanche公链中文官方的确多次为该项目推广，因此生态方需要谨慎推广项目。

此外也有用户称，DefrostFinance的项目方也是之前被盗的Finnexus和PhoenixFinance的同一个团队。这一信息真实性还有待考证，但也对用户提了个醒，尽量要选择实名的项目，匿名创始人背后，很有可能另有企图。