因解冻财务被盗损失1200万美元的大家族Hoi昨晚终于松了一口气。将近12o&#039；昨晚，他写道&quot黎明&quot在推特上。一个多小时前，解冻金融宣布黑客已经归还了钱。，将很快返还给用户。

虽然最后是大团圆结局，但还是被打上了&quot自导自演&quot由用户。

解冻金融接连被黑，大户受损1200万美元

。

回到圣诞节，12月25日，雪崩生态初级稳定货币项目解冻财务协议被曝光，再次出现问题。协议中加入了假抵押令牌，当前用户被恶意价格预测机清算。损失估计超过1200万美元。除霜金融官员说，它已经注意到V1的紧急情况，该小组目前正在调查。请等待更新，不要&#039；暂时不要用V1或V2。就在两天前，12月23日。DefrostFinanceV2遭到黑客攻击，获利17.3万美元，但由于V1不提供闪电贷款服务，因此未受影响。

随后，一个叫Hoi的用户在社区里发推文求助。，声称解冻金融的大部分存款都是由其提供的，其个人损失为1200万美元。审计公司CertiK尚未回应，并要求提供线索。

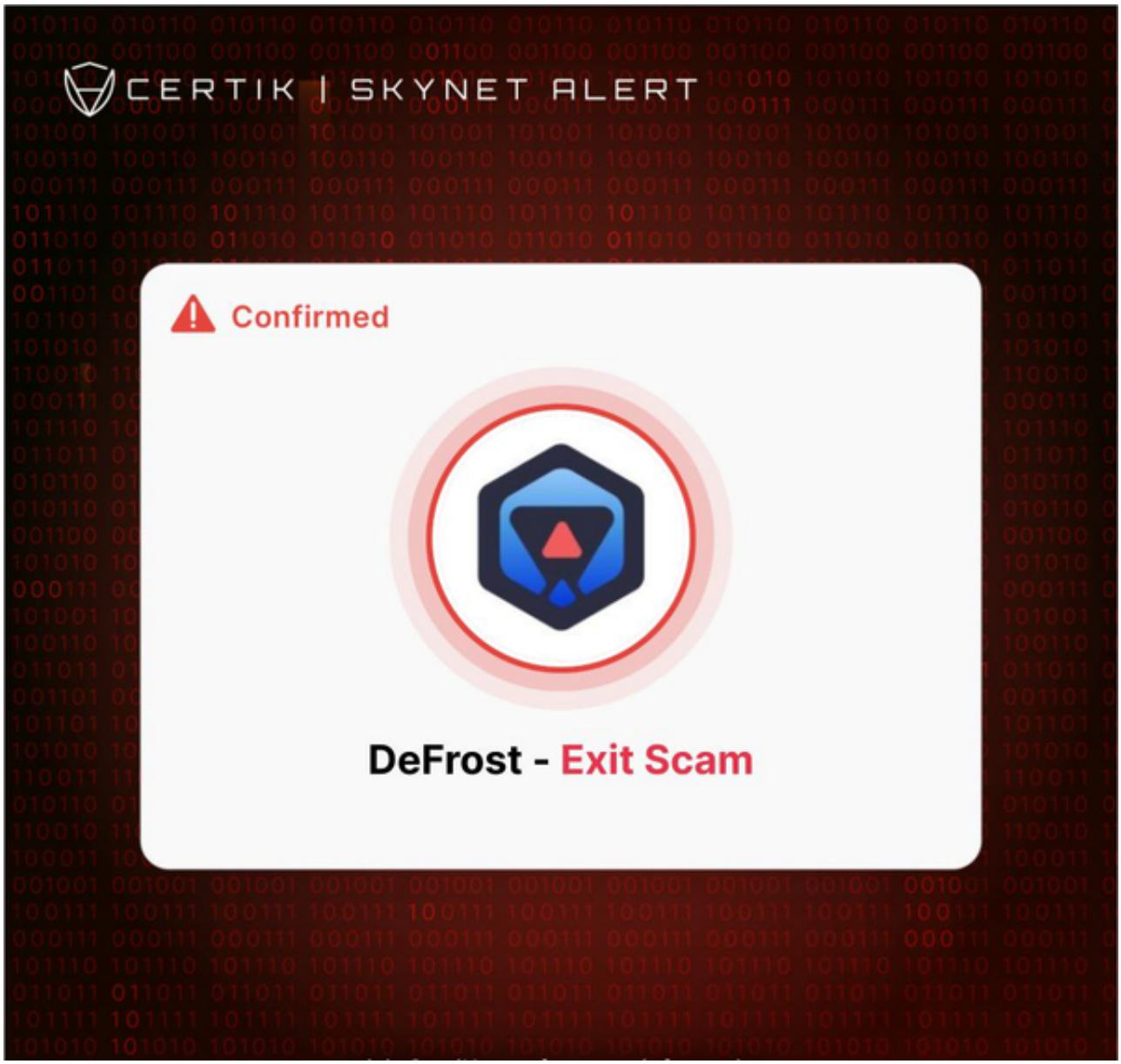
不久后Hoi再次发微博称自己掌握了项目方的一些实名线索，认为项目方是一个内部窃贼。因为在V1被偷的前一天，V2所有的钱都被偷了。V1的所有接口都有防写入，而V2的接口没有写入。他猜想球队总想成为V2。这样就可以推卸说是第三方攻击，因为V2被攻击时可以通过闪电贷被第三方触发。但是V2的钱太少了，不足以满足球队的胃口。于是第二天，我铤而走险，直接用了开发者权限。。强行改变神谕的价格，为自己铸造硬币，获得新的抵押贷款池。这些操作不能由第三方触发。如果开发团队能够&#039；不要在熊市中赚钱，它&#039；估计他们会失去他们的心。不管怎样，我&#039；现在我是唯一一个投资这个项目的人，而且它&#039；s估计没人会维权去偷。

根据区块链安全审计公司Beosin的分析，攻击者通过setoracleAddress函数修改了Oracle的地址。然后利用joinAndMint函数将100，000，000个H20代币铸造到0x6f31地址，最后通过虚假价格预测机调用清算函数获得大量USDT。。后续攻击者通过跨链将盗取的资金转移到以太坊的0x4e22。这与Hoi分析的操作是一致的。

黑客退回资金，公链官和审计公司难辞其咎

12月25日晚8点。Defrost发推文称，该团队愿意与黑客谈判，分享20%的被盗资金，以换取大部分被盗资产。具体金额可以协商，呼吁黑客尽快联系我们。"12月26日下午

。DefrostFinance的审计公司CertiK在推特上称，监控显示DefrostFinance项目是一个退出骗局，CertiK试图联系该团队的几名成员，但没有得到回应。此外CertiK还说&quot该小组没有对KYC进行调查，但我们正在利用我们掌握的所有信息来协助当局&quot。这似乎是除霜的最终结论&#039；从内部偷窃的行为。



也许是&quot黑客&quot被掌握了，所以他选择了快速归还资金。DefrostFinance在26日晚上10点发推文说：&quot被盗资金已被归还给解冻融资。。受影响的用户将很快能够恢复他们的资产。"

到目前为止，这个黑客事件只有两天就有了一个圆满的结局。但也给安全公司和生态敲响了警钟。

Hoi在推特上回顾自己选择这个矿的原因时列举了几个理由。1我自己和我的员工都看了合同，没问题。第三方黑客可以&#039；不要黑它。2Certik和其他审计。这个项目得到了很多Avax平台的推广，甚至还有官方号的推荐。。4后来想出来的时候发现其他德菲矿收入一般，然后社区都是好说话的兄弟。

审计公司对被审计项目的团队没有基本的了解，仅凭合同的安全性无法防止主观恶意。因此，掌握团队的KYC至关重要。所以也有用户质疑CertiK。既然调查组拒绝了KYC，就应该拒绝提供审计。此外，雪崩公链中国官方也确实多次推进该项目，因此生态方需要谨慎推进该项目。

另外，有用户表示DefrostFinance的项目方也是之前被盗的Finnexus和PhoenixFinance的同一个团队。这些信息的真实性还有待考证，但也提醒用户尽量选择实名制项目。