ZachXBT：先潜伏再攻击 起底朝鲜加密黑客不为人知的幕后

作者：ZachXBT，加密侦探；翻译：本站xiaozou

最近有一个团队寻求我的帮助，事情的起因是有人通过恶意代码从他们的金库中盗走130万美元。

这个团队不知道的是，他们雇佣了多名虚假身份的朝鲜IT人员作为开发者。

然后，我发现了自2024年6月以来与这些开发人员有关的一直保持活跃的加密项目就有至少25个。





## 该事件的洗钱途径如下：

1)将130万美元转移到偷盗地址

2)通过deBridge将130万美元从Solana桥接到以太坊

3)向Tornado存入50.2 ETH

4)向两个交易所转账16.5 ETH

偷盗地址为：

6USfQ9BX33LNvuR44TXr8XKzyEgervPcF4QtZZfWMnet



借助21个开发者的多个支付地址，我能够绘制出过去的一个月里最近一批约37.5万美元的支付集群。

0 xb721adfc3d9fe01e9b3332183665a503447b1d35

在过去的一周里，你可能也看到了，我请这些项目直接联系我。



此前，有550万美元流入了一个外汇存款地址，其中包括朝鲜IT人员从2023年7月至2024年期间收到的款项，该地址与OFAC制裁人员Sim Hyon Sop有关。

0x8f0212b1a77af1573c6ccdd8775ac3fd09acf014







## 调查过程中发现了一些有趣的事：

- 俄罗斯电信IP被美国和马来西亚的开发者使用。

- 在开发记录中他们不小心泄露了他们在记事本上的其他身份。

- 开发付款地址涉及到OFAC制裁名单上的Sang Man Kim和Sim Hyon Sop的。

- 一些开发者是由招聘公司安排的。

- 多个项目具有3名以上互推荐IT人员。





许多经验丰富的团队都雇佣了这些开发者，所以把他们当成是罪魁祸首是不公平的。

## 各团队未来可以关注的一些指标包括：

1) 他们互推荐的角色

2) 漂亮的简历/ GitHub活动，尽管有时会谎报工作经历。

3) 通常表面上乐意接受KYC，但却提交假身份证，希望团队不会进一步调查。

4) 关于他们所声称的来源地，问些具体问题。

5) 一个开发人员被解雇了，但立即出现了好几个找工作的新账户。

6) 可能一眼看起来是很优秀的开发者，但往往工作起来就表现不佳。

7) 查看日志

8) 喜欢使用流行NFT pfps

9) 亚洲口音

以防你是那种把一切归咎于朝鲜的事都称为巨大阴谋的人。

## 无论如何，这项研究证明：

在亚洲，一个实体通过使用假身份可以同时从事25个以上的项目，每月可以获得30万至50万美元的收入。

## 后续：

在本文发布不久后，另一个项目发现他们雇佣了我名单里列出的一个朝鲜IT人员（Naoki Murano），项目管理人员在他们的聊天中分享了我的文章。

结果是，就在两分钟之内，Naoki退出了聊天，并删除了他的Github。



