ZachXBT：起底朝鲜加密货币开发者不为人知的幕后

作者：Stephen Katte，CoinTelegraph；编译：白水，本站

区块链调查员 ZachXBT 表示，他发现了一个复杂的朝鲜开发者网络的证据，这些开发者每月为“成熟的”加密项目工作，收入高达 50 万美元。”

ZachXBT 在 8 月 15 日的 X 帖子中告诉他的 618,000 名粉丝，他认为一个“亚洲的单一实体”，可能在朝鲜运营，每月收入 30 万至 50 万美元，雇用至少 21 名员工参与超过 25 个加密项目。



区块链研究员 ZachXBT 声称发现 21 名朝鲜人使用假身份正在开展数十个加密项目。来源：ZachXBT

“最近，一个团队向我寻求帮助，因为恶意代码被推送后，国库中的 130 万美元被盗，”ZachXBT 说道。

“团队不知道，他们雇佣了多名使用假身份的朝鲜 IT 工作人员作为开发人员。”

ZachXBT 声称，朝鲜工人最近窃取的 130 万美元通过一系列交易进行了洗钱，包括转移到盗窃地址，最后将 16.5 个以太坊转移到两个不同的交易所。

在对这些开发者进行进一步调查后，ZachXBT 认为他们是一个更广泛网络的一部分。

通过跟踪多个付款地址，他发现一群开发者“上个月收到了 37.5 万美元”，之前的交易总额为 550 万美元，这些资金从 2023 年 7 月到 2024 年的某个时间流入了一个交易所存款地址。

这些付款随后与朝鲜的 IT 工作者和个人 Sim Hyon Sop 联系在一起，后者因涉嫌协调资金转移而受到外国资产控制办公室 (OFAC) 的制裁，这些资金转移最终用于支持朝鲜的武器计划。



ZachXBT 认为一群使用假身份的朝鲜开发者在过去一个月内获得了 375,000 美元。来源：ZachXBT

ZachXBT 表示，他的调查发现，其他付款地址与另一名 OFAC 制裁的个人 Sang Man Kim 密切相关，后者过去曾与朝鲜相关的网络犯罪有关。

美国执法部门认为，Kim“参与向 Chinyong 海外朝鲜工人代表团的家庭成员支付工资”，并因向中国和俄罗斯的朝鲜附属团队出售 IT 设备而获得 200 万美元的加密货币。

ZachXBT 还发现，自称在美国和马来西亚工作的开发人员之间存在俄罗斯电信 IP 重叠的情况。至少有一名工人“在记事本上意外泄露了他们的其他身份”。

他发现的一些开发人员甚至是由招聘公司安排的，在某些情况下，他们互相推荐工作。

“许多经验丰富的团队都雇用了这些开发人员，所以把他们单独归咎于他们是不公平的，”ZachXBT 说。

“在发布另一个项目后不久，我发现他们雇佣了我表中列出的一名朝鲜 IT 工作者（Naoki Murano），并在他们的聊天中分享了我的帖子。两分钟内，Naoki 就离开了聊天室并清除了他的 GitHub。”

据信，多年来，与朝鲜有关的组织是多起网络攻击和其他诈骗的幕后黑手。其网络犯罪手法通常涉及网络钓鱼、利用软件漏洞、网络入侵、私钥漏洞和面对面渗透。据了解，有些人还从事这些工作来赚取薪水，然后将薪水寄回该国。

2022 年，美国司法部、国务院和财政部发布联合咨询警告，警告朝鲜工人涌入各种自由职业技术工作，尤其是加密货币。

据称，与这个隐士王国有关的最臭名昭著的组织拉撒路集团 (Lazarus Group) 在截至 2023 年的六年间窃取了超过 30 亿美元的加密资产。