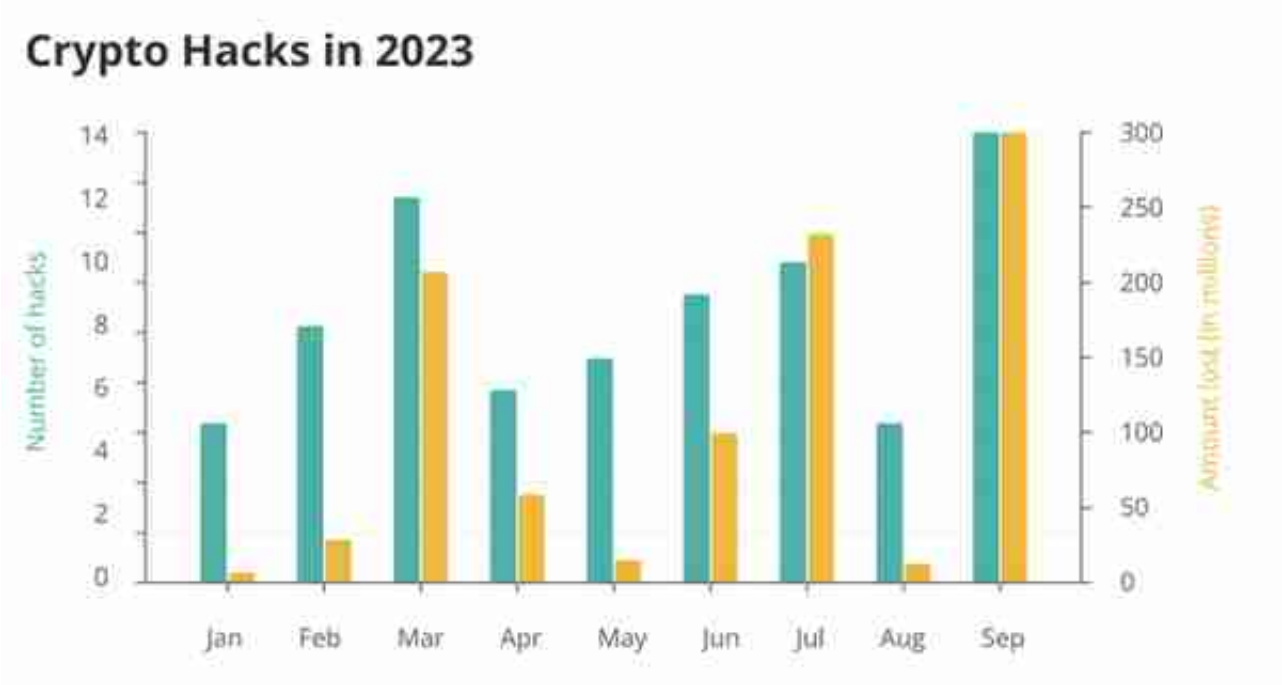
加密货币领域的黑客攻击金额超过 9 亿美元。区块链分析如何帮助找回被盗资产？

在去中心化金融 (DeFi) 和更广泛的 Web3 领域的快速发展中，安全性至关重要。新的威胁不断出现，因此了解攻击模式以进行风险评估和可靠性评估至关重要。根据 Cointelegraph 的 Crypto Hacks 数据库，仅 2023 年一年，就有超过 9.9 亿美元丢失或被盗。

这种不断增长的安全需求导致了 Web3 安全专业知识多元化生态系统的出现，从去中心化身份解决方案到智能合约审计员，确保了这个动态数字空间的安全。

Lazarus是一个来自朝鲜的国家级黑客组织，仍然是一个持续的威胁。Lazarus 在 2023 年造成了至少 2.91 亿美元的确认损失。即使进入第三季度，Lazarus 仍然活跃，并对 CoinEx 进行了攻击，导致损失超过 5500 万美元，这给网络安全留下了令人不寒而栗的提醒。



通过区块链分析加强加密安全

此外，即使是公司有时也难以应对潜在的黑客攻击和漏洞利用。因此，单独的加密货币爱好者需要技能来进行分析和研究以保护资金。区块链分析是检查区块链交易以追踪非法活动并追回被盗资产的调查过程。它的工作原理如下：

1.交易追踪：区块链分析师仔细追踪涉及被盗加密货币的区块链交易。

2.地址聚类：分析人员对相关地址进行分组，以识别被盗资金的流向。这种聚类有助于了解资金如何在钱包之间移动。

3.行为分析：分析师可以通过研究交易模式来识别可能表明黑客攻击或盗窃的异常或可疑行为。

4.模式识别：分析师使用历史数据和已知的攻击模式来识别新出现的威胁，以便及早检测和缓解。

5.监管警惕：世界各国政府正在推动在加密货币领域引入更严格的反洗钱（AML）和了解你的客户（KYC）法规。

6.协作：区块链分析通常涉及与执法机构、交易所和其他利益相关者的协作，以冻结或追回被盗资产。

在调查加密货币黑客事件时，区块链分析是调查人员可以使用的工具之一。开源情报（OSINT）是另一个关键组成部分。调查人员使用 OSINT 收集有关参与黑客攻击的个人或实体的信息。这可能包括使用 Etherscan、Nansen、Tenderly、Ethective 或 Breadcrumbs 等工具来更好地了解情况。

通过将区块链分析与开源情报相结合，调查人员可以构建黑客的全面视图，从而有可能识别肇事者并更有效地追回被盗资产。

在一个值得注意的案例中，Curve Finance 漏洞利用的肇事者于 7 月 30 日导致了超过 6100 万美元的加密货币损失，现已向 Alchemix Finance 和 Curve Finance 返还了约 890 万美元的加密货币。令人惊讶的是，攻击者的动机不是逃避捕获，而是为了保护被利用协议的完整性。这次攻击利用了重入漏洞，影响了多个矿池，包括 Alchemix Finance 的 alETH-ETH、JPEG'd pETH-ETH 和 Metronome sETH-ETH 矿池。虽然返还的资金约占总流失资金的 15%，但这一事件凸显了安全漏洞后加密货币领域错综复杂的道德和动机动态。

链上数据仍然是一种宝贵的调查工具，是区块链和加密资产世界所独有的。得益于底层的分布式账本技术，它为所有 Web3 爱好者提供了一个了解资产流动、交易跟踪和强大分析功能的特殊窗口。