CULMEN
INTERNATIONAL

网络战争中的朝鲜

黑客攻击加密货币和洗钱

风险增加

在过去的五年里，几起对加密货币交易所的直接攻击和盗窃已经被确定是由朝鲜直接精心策划的。尤其是臭名昭著的“Lazarus Group”，又名“APT38”，是朝鲜发起的专门从事金融网络行动的威胁组织，归属于其侦察总局。自 Lazarus Group 首次因索尼影业和WannaCry网络攻击而得名以来，该组织一直专注于加密货币犯罪，事实证明该犯罪行动利润丰厚。 从2018年至今，估计与朝鲜有关的黑客窃取了超过 30 亿美元的资金，这些资金正被用于资助该国的核导弹计划。

朝鲜的网络实力位居世界第一，并展现出不断演变的网络犯罪策略。[1] 加密货币具有去中心化和匿名性，已成为朝鲜用于洗钱的最强大工具。美国联邦调查局 (FBI) 和国家安全局跟踪了与朝鲜有关的加密货币黑客攻击，并发现 DeFi（去中心化金融）协议通常是黑客攻击的目标，因为 DeFi 平台不保管用户资金，并且因容易收集“了解你的客户（KYC）”信息而闻名。现已侦测到与朝鲜有关的黑客具有多样化以及使用不同加密货币混合器的趋势。

资金被盗后被转移到多个加密货币混合器（软件工具）进行洗钱，这些混合器把来自数千个地址的加密货币进行汇集和混合扰乱以进行洗钱。利用 Mixter 进行加密货币黑客洗钱已成为与朝鲜有关的网络犯罪的趋势。在洗钱的最后阶段，为了能够兑现，比特币被发送到将加密货币转变成法定货币的存款地址，这些存款地大多数位于亚洲，但最近发现越来越多地使用俄罗斯交易所对加密资产来进行非法洗钱。[2]

风险增加

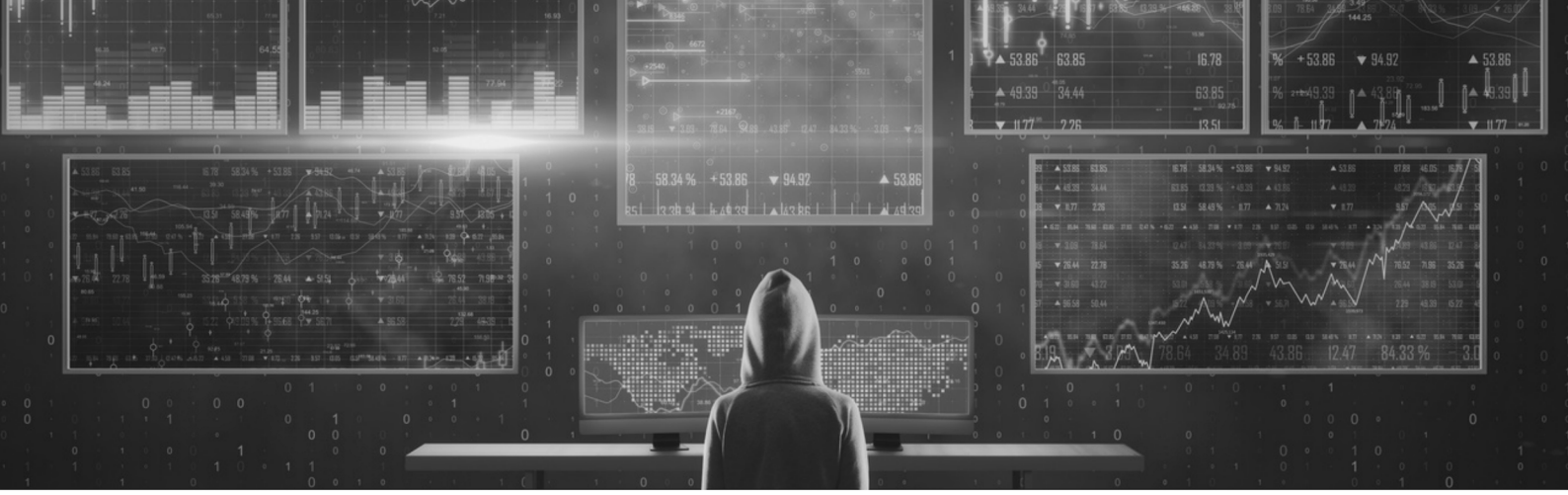
在2020至2022期间，Tornado Cash 、 Blender 和 Sinbad 等混合器被用来对黑客窃取的加密货币进行洗钱。以下是与朝鲜有关的加密货币黑客攻击和洗钱事件：

KuCoin 案：朝鲜 Lazarus 集团与对新加坡加密货币交易所 KuCoin 的黑客攻击有关，该集团从该交易所窃取了价值 2.8 亿美元的加密资产。其中一些资金是通过 DEX 洗钱的，这表明朝鲜有能力利用 DeFi 技术。

辛巴达Sinbad案：从辛巴达案的行动策略来看，黑客将被盗资金从以太坊区块链桥接至比特币，然后将比特币发送给辛巴达。[3]

Tornado Cash 是一家提供虚拟货币混合服务的实体，在2022 年 3 月，它故意混淆了 OFAC 指定的、朝鲜控制的 Lazarus Group 窃取的超过 4.55 亿美元的资金移动，这是迄今为止已知的最大规模的虚拟货币盗窃案。 Tornado Cash 于 8 月受到制裁，并于2022 年 11 月根据 EO 13722 和 EO 13694 摘牌并在黑名单上被登记。[4]

Harmony 案：2023 年 8 月 22 日，美国联邦调查局 (FBI) 确认，朝鲜恶意网络组织 Lazarus对 2022 年 6 月 24 日 报道的从Harmony Horizon Bridge[5] 盗窃 1 亿美元虚拟货币负有责任。 从 Harmony Protocol 窃取的价值2190 万美元的加密货币被转移到一家以处理非法交易而闻名的俄罗斯交易所。



加密货币洗钱

最近朝鲜和俄罗斯领导层之间紧密的合作关系和具有历史意义的武器会谈非常令人不安。同样，最近的黑客攻击表明，与朝鲜有关的黑客组织正在更多地使用俄罗斯的交易场所，这些交易场所以对非法加密资产洗钱而闻名。

加密货币的跨境性质可能是流氓国家犯罪团伙转移非法资金的最可行的工具，幸运的是，最近的发展表明美国执法和国家安全机构利用区块链技术和交易数据，更有能力追踪和追回来自加密货币黑客的资金。在 2022 年，追回了有史以来与朝鲜黑客有关的第一笔3000 万美元的资金，这笔资金是在 Axie Infinity Ronin Bridge黑客事件中被窃取的。

1. 哈佛大学肯尼迪学院贝尔弗中心发布的《2022年国家网络力量指数》显示，朝鲜网络力量实施金融犯罪排名全球第一。
2. Chainaanalysis 追踪到朝鲜黑客从加州加密货币公司 Harmony 窃取的 1 亿美元资金，这些黑客从银行和加密货币公司窃取了数十亿美元，为其非法导弹计划提供资金。 2023 年 4 月，追回了 100 万美元的被盗资 金 。 （ https://www.chainathesis.com/blog/ofac-dprk-north-korea-sanctions-april-2023/ ）(https://www.chainathesis.com /博客/朝鲜俄罗斯加密货币洗钱/)
3. https://www.chainaanalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/
4. https://home.treasury.gov/news/press-releases/jy1087
5. https://www.fbi.gov/news/press-releases/fbi-identizes-cryptocurrency-funds-stolen-by-dprk

顶峰国际提供帮助

如果你对朝鲜规避制裁有任何问题，顶峰国际可以提供帮助。可以联系我们，咨询有关如何改进尽职调查以及合规性规程的事宜。

Prepared by Culmen International