盘点历史上十大中心化交易所遭黑客攻击事件

参考来源：Top Centralized Exchange Hacks: Lessons Learned from History

近年来，像 Mt. Gox 和 WazirX 这样的中心化交易所 (CEX) 因外部黑客攻击而遭受重大损失，而 FTX 等其他交易所则因内部资金滥用而崩溃。即使是行业巨头币安和 Coinbase 也面临着来自世界上最强大的金融监管机构的生存威胁。

去中心化交易所 (DEX) 可以有效防御这三大威胁——黑客攻击、欺诈和监管过度——这些威胁一直困扰着 CEX。当然，除了“黑客攻击”之外，还有其他威胁。例如，FTX 的垮台涉及其高管管理不善和滥用客户资金，而这种情况在 DEX 上不太可行，因为 DEX 的固有结构提倡透明度和用户控制。

本文探讨了顶级中心化交易所黑客攻击历史上最大的漏洞，从臭名昭著的入侵事件到系统性漏洞，加密货币世界经历了动荡。在这里，我们回顾了 10 大最严重的中心化交易所黑客事件。

### 10. Bithumb 黑客攻击：屡屡受击

Bithumb 成立于 2014 年，迅速成为韩国加密货币市场的基石，拥有超过 800 万注册用户，交易量超过 1 万亿美元。尽管 Bithumb 声名显赫，但它却屡屡受到攻击。

从 2017 年开始，Bithumb 遭受了多次入侵：

2017 年 2 月：黑客窃取了 700 万美元。

2018 年 6 月：员工个人数据被利用窃取近 3200 万美元的加密货币。

2019 年 3 月：Bithumb 宣布再次遭到入侵，在损失约 2000 万美元的 EOS 和 XRP 后暂停存款和取款。

2019 年 6 月：Bithumb 再次遭受攻击，黑客盗取了价值 3000 万美元的数字代币。

针对屡次发生的违规行为，韩国科学技术部 (MIC) 展开了彻底调查，主要发现包括：

### 9. WazirX加密货币黑客攻击事件

2024 年发生的 108 起事件中，因黑客攻击和欺诈而损失了价值超过 4.73 亿美元的加密货币。仅WazirX一家就占了 7 月份因黑客攻击而损失的加密货币总量的 86.4%。

印度 CEX WazirX 宣布计划在 2024 年 7 月 18 日冻结提款后撤销所有交易。当日，WazirX 遭遇重大钱包漏洞攻击，导致超过 2.3 亿美元的加密资产被未经授权转移。此次攻击针对的是 WazirX 在以太坊上的多重签名钱包。

超过 1 亿美元的柴犬 (SHIB)、2000 万个 MATIC 代币（1100 万美元）、6400 亿个 PEPE 代币（750 万美元）、570 万个 USDT 和 1.35 亿个 GALA 代币（350 万美元）被盗。

尽管采用了硬件钱包和地址白名单等先进安全措施，WazirX 还是遭受了一次复杂的攻击。这要求进行全面的安全审计并不断改进数字资产的保护措施。私钥集中控制的风险显而易见。

### 8. 币安黑客事件：加密货币漏洞的严峻提醒

2019 年，全球领先的加密货币交易所币安 (Binance) 遭遇了一起大型中心化交易所黑客攻击。5 月 7 日，恶意攻击者利用网络钓鱼和病毒攻击币安的安全系统，窃取用户的双因素身份验证代码和 API 密钥。

这次入侵使他们能够在一次交易中从交易所的热钱包中窃取 7,074 个比特币，当时价值超过 4000 万美元。

此次事件发生后，币安首席执行官赵长鹏宣布成立用户安全资产基金 (SAFU)，以在极端情况下保护用户的资金。尽管采取了这些措施，但币安在 2022 年 10 月仍面临另一项重大安全挑战。黑客利用跨链桥 BSC Token Hub 非法生成并窃取了 200 万个 BNB 代币，约合 5.7 亿美元。

### 7. KuCoin：遭遇了好莱坞式的盗窃

2020 年 9 月，KuCoin 遭遇了好莱坞式的盗窃，这起盗窃案在中心化交易所黑客攻击中名列前茅。黑客先发起了一次狡猾的攻击，将比特币和以太币盗取到一个神秘的钱包中。随着数字窃贼通过窃取库币热钱包的私钥进入金库，阴谋变得更加复杂。

第二天，当 KuCoin 首席执行官 Johnny Lyu 在直播中向全世界发表讲话时，加密社区已经紧张不安。KuCoin 团队反应迅速，将剩余资金转移到新的热钱包，关闭了被盗的钱包，并暂时冻结了所有客户交易，以减轻进一步的风险。

进一步调查发现，被盗资金涉及 BTC、ETH、LTC、XRP 等多种加密货币，总额约为 2.81 亿美元。尽管损失惨重，但KuCoin 采取的主动措施在数周内追回了约 2.04 亿美元的被盗资金。

更令人感兴趣的是，KuCoin 与国际执法部门合作，将这一网络攻击行为归咎于疑似朝鲜黑客组织。

### 6. BitGrail：内部工作

意大利加密货币交易所 BitGrail 因平台被盗 1.2 亿欧元（1.4655 亿美元）而陷入争议。意大利警方指控 Firano（又名“FF”）可能参与了黑客攻击，或者在最初发现漏洞后疏忽未能加强安全措施。

这一系列事件导致约23万用户的资金损失，Firano面临的指控包括计算机欺诈、欺诈性破产和洗钱，这是意大利历史上最大的金融违规事件之一。

事后，意大利破产法院采取果断行动，宣布 Firano 和 BitGrail 破产。法院还要求 Firano 尽可能多地向客户返还被盗资产。

此外，法院还批准扣押 Firano 的资产，包括超过 100 万美元的个人物品和 BitGrail 账户中的数百万加密货币。法院发现 BitGrail 平台的软件缺陷导致多次不正当地请求提款。

在像 BitGrail 这样的 CEX 中，所有资产和安全措施的控制都是集中的，这使得它们成为黑客的诱人目标。

### 5. Poloniex：两次黑客攻击的故事

Poloniex遭受过两次严重的安全漏洞攻击。

2014 年 3 月，黑客利用软件漏洞盗走了 97 个比特币，占当时交易所比特币持有量的 12.3%。尽管遭受挫折，Poloniex 还是成功反弹，全额赔偿了受影响的用户。

时间快进到 2023 年 11 月，该交易所再次受到攻击，这次的攻击更加严重。攻击者疑似是与朝鲜有联系的 Lazarus 集团，他们窃取了私钥，从 Poloniex 的热钱包中窃取了约 1.26 亿美元。

作案手法包括利用社交工程和恶意软件来获取关键私钥。黑客入侵后，采取了复杂的策略，包括向特定地址发送不同的代币，并利用去中心化交易所洗钱，这使得追踪和恢复变得困难。

### 4. Bitstamp被盗事件

网络犯罪分子瞄准了 Bitstamp 的系统管理员 Luka Kodric，他在不知情的情况下下载了一个恶意文件，危及了交易所的安全。该恶意软件隐藏在无害的文档中，激活了一个脚本，感染了 Bitstamp 的服务器，使黑客能够访问关键的 wallet.dat 文件和密码。

Bitstamp 意识到这一漏洞后迅速采取行动，成立了应急小组并向全公司发出警报。尽管采取了这些措施，黑客还是成功从热钱包中盗取了 18,866 个比特币，导致黑客入侵时损失了约 500 万美元。

事后，Bitstamp 对其交易平台进行了大规模改造，选择彻底重建，而不是进行修补。他们将基础设施迁移到亚马逊位于欧洲的安全云服务器，实施多重签名钱包访问，并聘请 Xapo 进行冷钱包管理。

### 3. Bitfinex被盗事件

2016 年 8 月，Bitfinex 遭遇网络攻击。黑客利用了该交易所由 BitGo 支持的多重签名安全系统的漏洞。他们操纵安全协议，从 Bitfinex 的热钱包中非法提取了 120,000 比特币。

黑客攻击发生后，Bitfinex 对财务损失保持透明。损失分摊到用户账户，每个账户损失 36%。为了减轻损失，Bitfinex 向受影响的用户发行了 BFX 代币，可兑换美元或 iFinex Inc. 的股票，以促进逐步恢复。

### 2. Coincheck盗窃案

2018 年 1 月末，日本著名加密货币交易所 Coincheck 遭遇了史上最严重的中心化交易所黑客攻击之一。黑客入侵了该交易所的热钱包，盗走了 5.23 亿个 NEM 代币，当时价值约 5.34 亿美元。

尽管之前有过其他黑客攻击的教训，但 Coincheck 仍将大量资产存放在热钱包中，且缺乏足够的多重签名保护。攻击发生后，该交易所立即停止了所有存款和取款，以阻止被盗资金的流动。

加密货币社区迅速团结起来，阻止被盗资产被清算。ShapeShift 等交易所禁止交易被盗的 NEM 币，并标记相关地址以阻止进一步交易。尽管做出了这些努力，但资金的全面追回仍未可行。

### 1. Mt. Gox：无法忘怀的黑客事件

Mt. Gox 黑客事件仍可以说是最臭名昭著和最受关注的加密货币盗窃案，主要是因为其规模和发生时间。这一重大事件是顶级中心化交易所黑客事件的经典案例。

2011 年，当时全球最大的比特币交易所 Mt. Gox 首次遭遇重大安全漏洞，导致 25,000 比特币丢失。2014 年情况进一步恶化，最终发生灾难性的盗窃案，约 850,000 比特币被盗。

这次黑客攻击影响巨大，影响了比特币的价格和全球加密货币社区的信任。“我几乎失去了一切。它永远改变了我对数字货币安全的看法，”一位论坛用户分享道，强调了这次黑客攻击对个人和财务的深远影响。

### 交易所安全的防范措施

交易所的安全问题在近年来成为了整个加密货币行业的焦点，尤其是在一些重大安全事件和内部问题导致了交易所的倒闭或资金损失之后。为了提升安全性，交易所可以采取多种措施。

比如将大部分资产保存在离线的冷钱包中，只有少量资金存放在联网的热钱包中，以应对日常交易需求，这种方式能显著降低黑客成功窃取大量资金的风险。另一方面，通过要求多个密钥持有者签署交易，多重签名可以防止单一密钥的泄露导致资金的损失。