SLOWMIST 2024

区块链安全与反洗钱年度报告

目录

一、概述

2024 是承压前行的一年。2024 年，全球宏观经济环境依然复杂多变，地缘政治的紧张局势未见明显缓解。美联储的货币政策调整、俄乌冲突的持续、中东局势的不稳定，以及全球数字资产监管的不断升级，都为区块链行业带来了前所未有的挑战。尽管如此，区块链行业依然展现出韧性与活力，在不确定性中探索着新的方向。在安全领域，2024 年延续了以往的严峻态势。黑客攻击事件频发，尤其是针对中心化平台的攻击占据着主导地位。与此同时，智能合约漏洞和社会工程学攻击仍是黑客的主要作恶手段，而钓鱼攻击的方式更加隐蔽，手段更加复杂，用户资产的保护仍面临重大挑战。供应链安全问题也在 2024 年引发更多关注，多个知名项目遭遇恶意代码注入攻击，导致大量用户资产丢失。

2024 是创新与变革的一年。尽管安全挑战严峻，2024 年的区块链行业在创新方面依然成绩斐然。去中心化金融（DeFi）继续拓展应用边界，用户数量和交易规模双双增长。链上资产的托管和管理工具更加丰富，跨链协议的技术方案也在逐步完善，为多链生态的协同发展铺平了道路。NFT 领域在 2024 年重新焕发活力，链游（GameFi）项目也逐渐从沉寂中崛起，吸引了大量用户和资本的关注。与此同时，以太坊和 Layer2 技术的深入发展进一步提升了区块链网络的效率，为更多创新应用提供了底层支持。另一个值得关注的趋势是区块链与人工智能（AI）的融合。越来越多的项目尝试将 AI 应用于链上分析、反欺诈监控以及用户体验优化，开辟了新的可能性。

2024 是监管深化的一年。随着区块链行业的快速发展，全球范围内的监管框架正在逐步成型。美国加强了对加密货币交易所的合规要求，中国内地则继续严格规范虚拟资产的金融活动，继续推进数字人民币的应用试点。中国香港对虚拟资产态度友好，逐步构建适合行业发展的监管体系，包括推出虚拟资产服务商牌照及 ETF 产品。此外，欧洲的 MiCA 法案正式落地，为区块链和加密资产的合规运营提供了清晰的指导。多个国家的中央银行也加速了数字货币的研发和推广，为未来的数字金融生态奠定基础。合规性是 2024 年行业发展的关键词之一，而安全性与合规性的结合则是行业健康发展的核心驱动力。

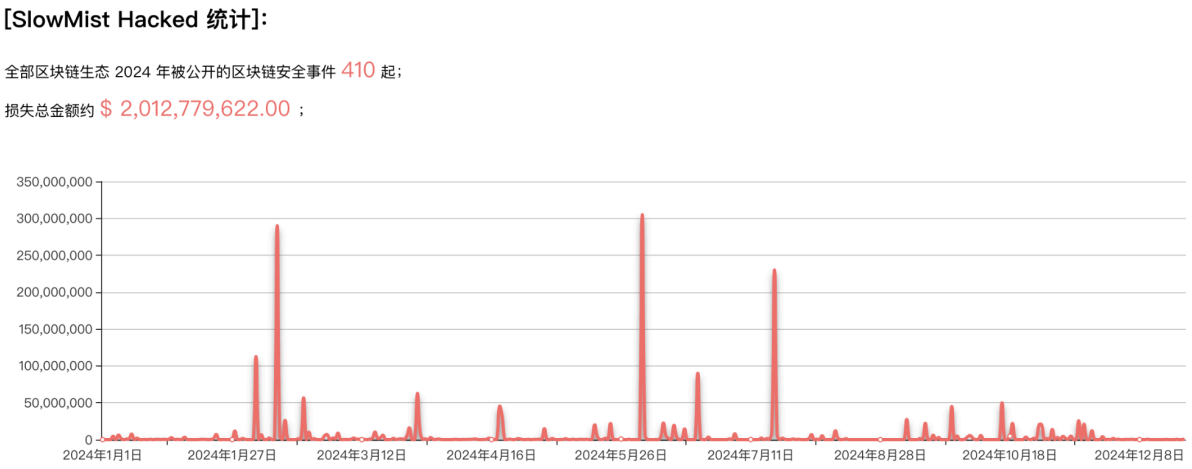
2024 年，区块链行业在安全与创新的交锋中前行。在这个背景下，本报告回顾了 2024 年区块链行业关键监管合规政策及反洗钱动态，总结了 2024 年区块链安全事件并对典型欺诈手法进行了梳理。此外，我们邀请了 Web3 反诈骗平台 ScamSniffer 撰写关于钓鱼 Wallet Drainers 的内容，同时，我们对朝鲜黑客的洗钱手法和获利情况进行了分析和统计。我们期望这份报告为读者提供有

益的信息，帮助从业者和用户更全面地了解区块链安全现状及解决方案，为促进区块链生态的安全发展贡献一份力量。

二、区块链安全态势

根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，2024 年共发生安全事件 410 件，损失高达 20.13 亿美元。对比 2023 年（共 464 件，损失约 24.86 亿美元），损失同比下降 19.02%。

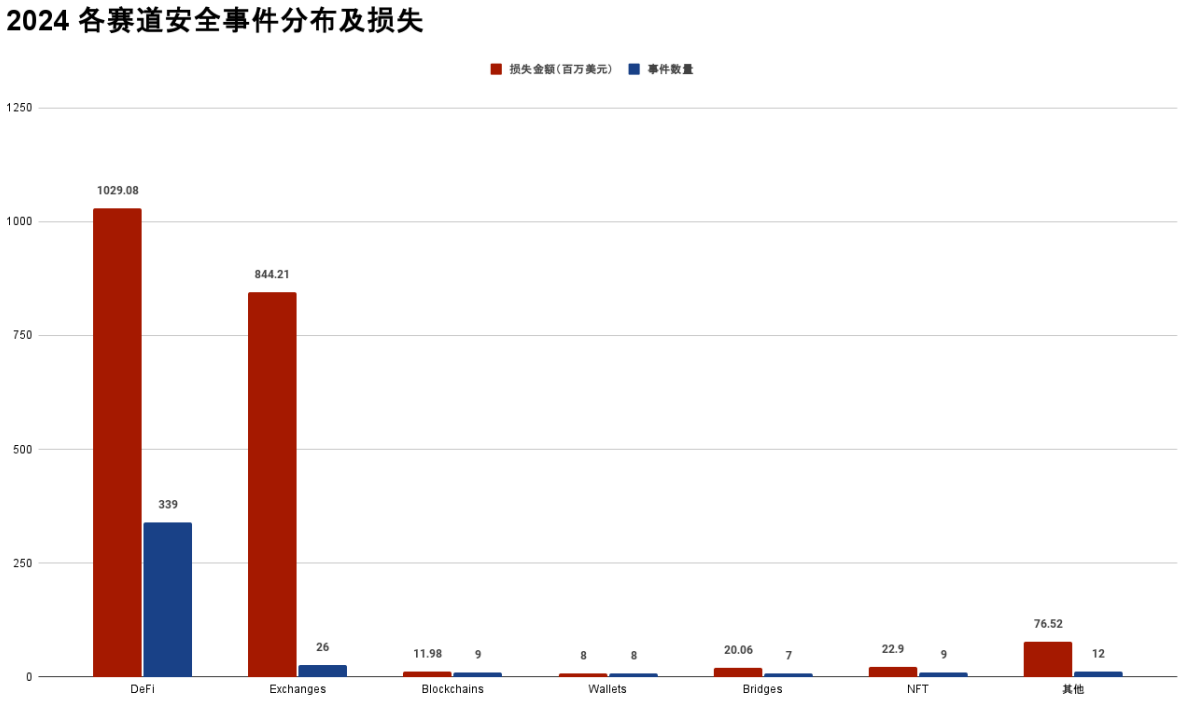
注：本报告数据基于事件发生时的代币价格，由于币价波动和部分未公开事件的损失未纳入统计等因素，实际损失应高于统计结果。



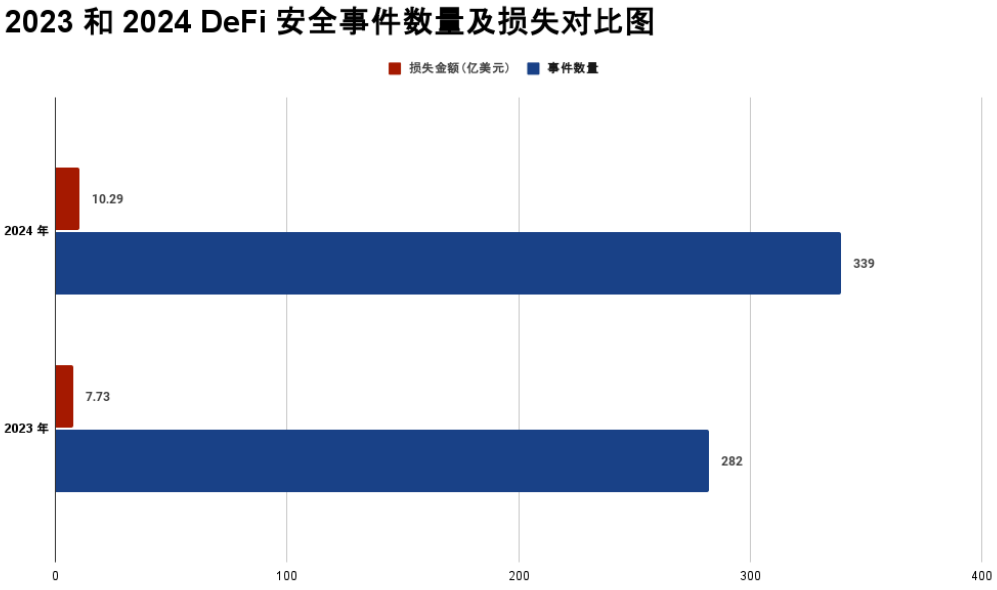
(https://hacked.slowmist.io/statistics/?c=all&d=2024)

2.1 区块链安全事件总览

从项目赛道来看，DeFi 仍然是最常受到攻击的领域。2024 年 DeFi 安全事件共 339 件，占总安全事件数的 82.68%，损失高达 10.29 亿美元，对比 2023 年（共 282 件，损失约 7.73 亿美元），损失同比上升 33.12%。

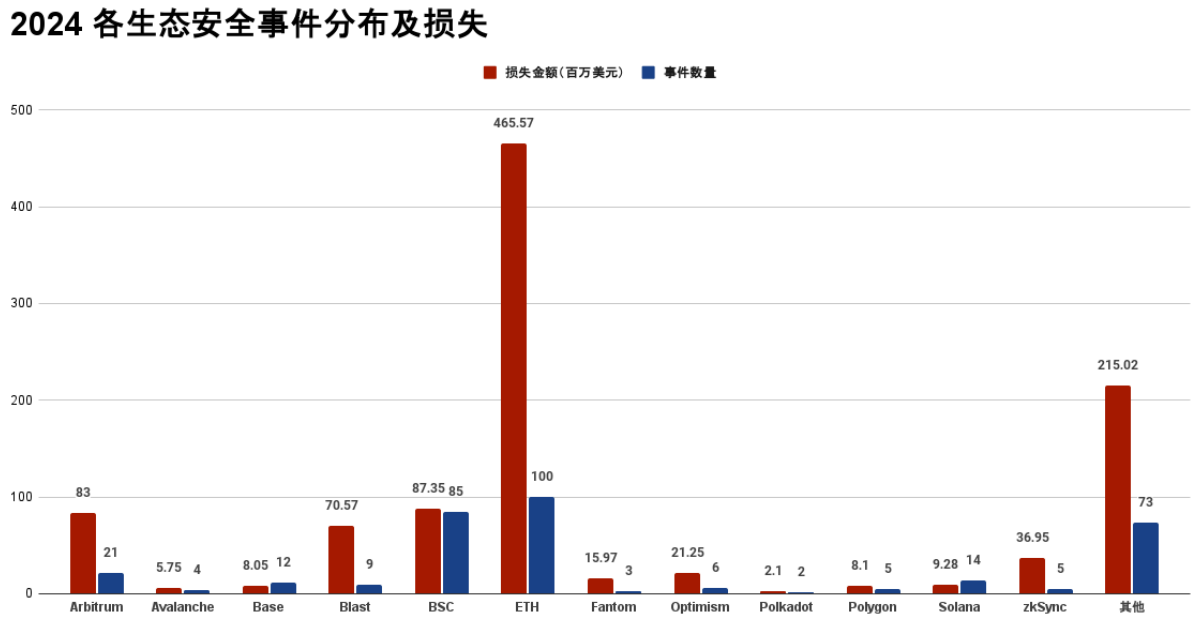


（2024 各赛道安全事件分布及损失）



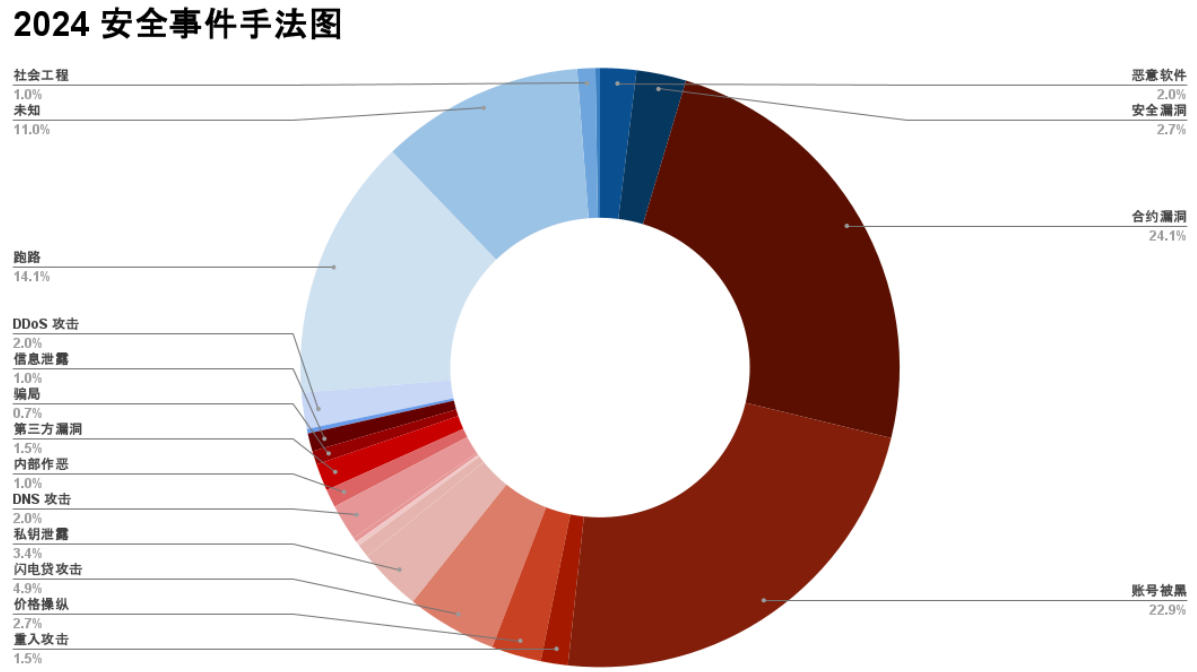
（2023 和 2024 DeFi 安全事件分布及损失对比图 ）

从生态来看，Ethereum 损失最高，达 4.65 亿美元。其次是 BSC，达 8,735 万美元。



（2024 各生态安全事件分布及损失）

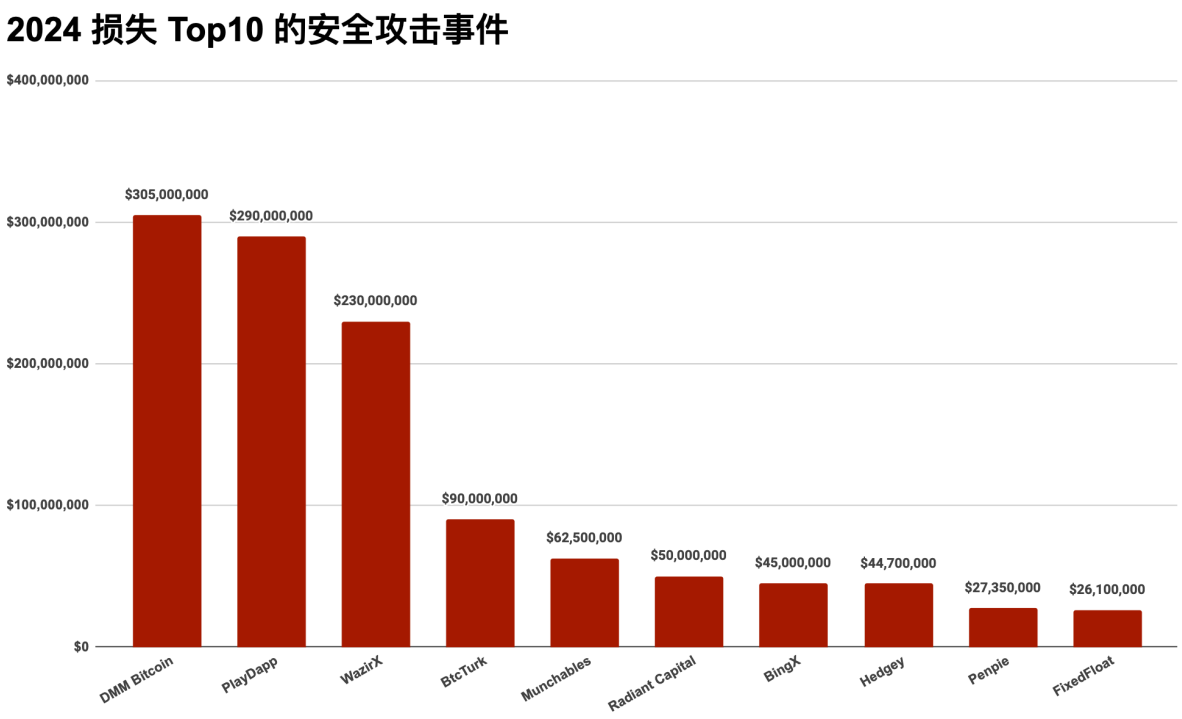
从事件原因来看，合约漏洞导致的安全事件最多，达 99 件，导致损失约 2.14 亿美元。其次为账号被黑导致的安全事件。



（2024 安全事件手法图 ）

2.2 典型攻击事件

此节选取了 2024 年损失 Top10 的安全攻击事件。



（2024 损失 Top10 的安全攻击事件）

2.2.1 DMM Bitcoin

2024 年 5 月 31 日，日本加密货币交易所 DMM Bitcoin 表示，其官方钱包中的 4,502.9 BTC 被非法转移，造成价值约 482 亿日元的损失。据悉，DMM Bitcoin 安全事件的损失金额在加密货币黑客攻击史上排名第七，是自 2022 年 12 月以来最大的一次攻击。同时，此前日本曾发生过两起重大加密货币交易所黑客攻击事件，即 2014 年的 Mt.Gox 事件和 2018 年的 Coincheck 事件，被盗金额分别为 4.5 亿美元和 5.34 亿美元。此次 DMM Bitcoin 攻击事件成为日本第三大此类案件。12 月 23 日，据美国联邦调查局（FBI）通报，美国联邦调查局（FBI）、国防部网络犯罪中心（DC3）以及日本警察厅（NPA）提醒公众，此次盗窃与 TraderTraitor 威胁活动相关，TraderTraitor 也被跟踪记录为 Jade Sleet、UNC4899 和 Slow Pisces。TraderTraitor 活动通常以针对同一公司多名员工的社交工程攻击为特征。

据悉，2024 年 3 月底，一名伪装成 LinkedIn 招聘人员的朝鲜黑客联系了 Ginco 公司的员工，Ginco 是一家总部位于日本的企业级加密货币钱包软件公司。黑客向目标员工发送了一个链接，指向一个托管在 GitHub 上的恶意 Python 脚本，声称这是一个入职测试。目标员工将 Python 代码复制到自己的 GitHub 页面上，结果遭到入侵。5 月中旬后，TraderTraitor 黑客利用会话 Cookie 信息冒充被攻击的员工，成功访问 Ginco 公司未加密的通信系统。5 月底，黑客可能利用此访问权限篡改了 DMM Bitcoin 员工的合法交易请求，导致 4,502.9 BTC 被盗。最终，盗取的资金被转移到 TraderTraitor 控制的钱包中。

2.2.2 PlayDapp

2024 年 2 月 9 日，区块链游戏平台 PlayDapp 遭攻击，黑客入侵了 PlayDapp (PLA) 代币智能合约。黑客非法获取了私钥，从而改变了智能合约的所有权和铸币权限，将其转移到自己的账户上。黑客移除了现有管理员的授权，并非法铸造了 2 亿个 PLA 代币。事发后不久，PlayDapp 通过链上交易向黑客发送消息，要求归还被盗资金并提供 100 万美元白帽奖励，但最终谈判失败。2 月 12 日，黑客再次非法铸造了 15.9 亿 PLA 代币，但由于交易所已采取冻结措施，市场流通已被停止，未能流通。4 月 1 日，据 PlayDapp 披露，2024 年 1 月 16 日，PlayDapp 团队收到了黑客伪造的邮件，该邮件精心设计，具有与其常收到的来自主要合作交易所的常规信息请求邮件完全相同的标题、发件人邮件地址（包括用户名和域名）以及内容。分析表明，当执行邮件附件中的恶意代码时，受害者的电脑安装了一个篡改的远程访问多会话工具，随后被黑客远程控制，导致管理员私钥被盗。

2.2.3 WazirX

2024 年 7 月 18 日，印度加密货币交易所 WazirX 的多签钱包被监测到发生多笔可疑交易。7 月 19 日，据 WazirX 在 X 平台发布网络攻击的初步调查结果，他们的一个多重签名钱包遭遇了网络攻击，损失超过 2.3 亿美元。该钱包共有六个签署人 —— 五名来自 WazirX 团队成员和一名来自 Liminal 的成员，负责交易验证。每笔交易通常需要 WazirX 团队三名签署人（这三名签署人都使用 Ledger 硬件钱包以确保安全）批准后，才会由 Liminal 的签署人进行最终批准。此次网络攻击源于 Liminal 界面上显示的数据与实际交易内容之间的差异，在攻击发生时，Liminal 界面显示的交易信息与实际签署的内容不符。WazirX 怀疑黑客通过替换载荷，将钱包控制权转移给了自己。

2.2.4 BtcTurk

2024 年 6 月 22 日，土耳其加密货币交易所 BtcTurk 遭攻击，损失约 9 千万美元。BtcTurk 在 6 月 22 日的声明中表示：“此次网络攻击影响了我们热钱包中 10 种加密货币余额的一部分，大部分存

储在冷钱包中的资产仍然安全。”据 Binance 首席执行官 Richard Teng 透露，Binance 已冻结了其中价值 530 万美元的被盗资产。

2.2.5 Munchables

2024 年 3 月 27 日，Blast 生态项目 Munchables 遭攻击，损失约 6,250 万美元。同日，Blast 创始人 Pacman 发推表示：“Blast 核心贡献者已通过多重签名获得 9700 万美元的资金。感谢前 Munchables 开发者选择最终退还所有资金，且不需要任何赎金。”

2.2.6 Radiant Capital

2024 年 10 月 17 日，Radiant Capital 在 X 发文表示意识到 BNB Chain 和 Arbitrum 上的 Radiant 借贷市场存在问题，Base 和主网市场已暂停交易。据慢雾安全团队分析，此次事件是 Radiant 黑客非法控制 3 个多签权限后，升级了恶意合约以窃取资金。10 月 18 日，Radiant 发布事件分析报告表示，此次事件导致约 5 千万美元的损失，黑客通过复杂的恶意软件注入技术，成功入侵了至少三位核心贡献者的设备，这些被入侵的设备随后被用来签署恶意交易。12 月 6 日，Radiant 发布被攻击事件的最近进展，Radiant 聘请的安全公司 Mandiant 将此次攻击归因于 UNC4736，通常被称为 AppleJeus 或 Citrine Sleet。Mandiant 高度认为 UNC4736 与朝鲜民主主义人民共和国（DPRK）有关。

2.2.7 BingX

2024 年 9 月 20 日，据加密货币交易所 BingX 公告，新加坡时间 9 月 20 日凌晨 4 点左右，BingX 的安全系统检测到针对一个热钱包的未经授权的入侵。据慢雾安全团队统计，此次事件导致的损失约达 4,500 万美元。根据 MistTrack 的分析，Indodax 黑客和 BingX 黑客之间疑似存在联系，这两起攻击事件的黑客使用了同一个地址洗钱，且都指向了朝鲜黑客 Lazarus Group。

2.2.8 Hedgey Finance

2024 年 4 月 19 日，Hedgey Finance 遭攻击，黑客进行了一系列恶意交易，导致其在 Ethereum 和 Arbitrum 两条链上损失总计约 4,470 万美元。此次事件的根本原因是缺少对用户参数输入的验证操作，使得黑客能够操纵并获得未经授权的代币批准。

2.2.9 Penpie

2024 年 9 月 4 日，去中心化流动性收益项目 Penpie 遭攻击，黑客获利约 2,735 万美元。据慢雾安全团队分析，此次事件的核心在于 Penpie 在注册新的 Pendle 市场时，错误地假设所有由 Pendle Finance 创建的市场都是合法的。然而，Pendle Finance 的市场创建流程是开放式的，允许任何人创建市场，并且其中的关键参数如 SY 合约地址，可以由用户自定义。利用这一点，黑客创建了一个含有恶意 SY 合约的市场合约，并利用 Penpie 池子在获取奖励时需要对外部 SY 合约调用的机制，借助闪电贷为市场和池子添加了大量的流动性，人为放大了奖励数额，从而获利。

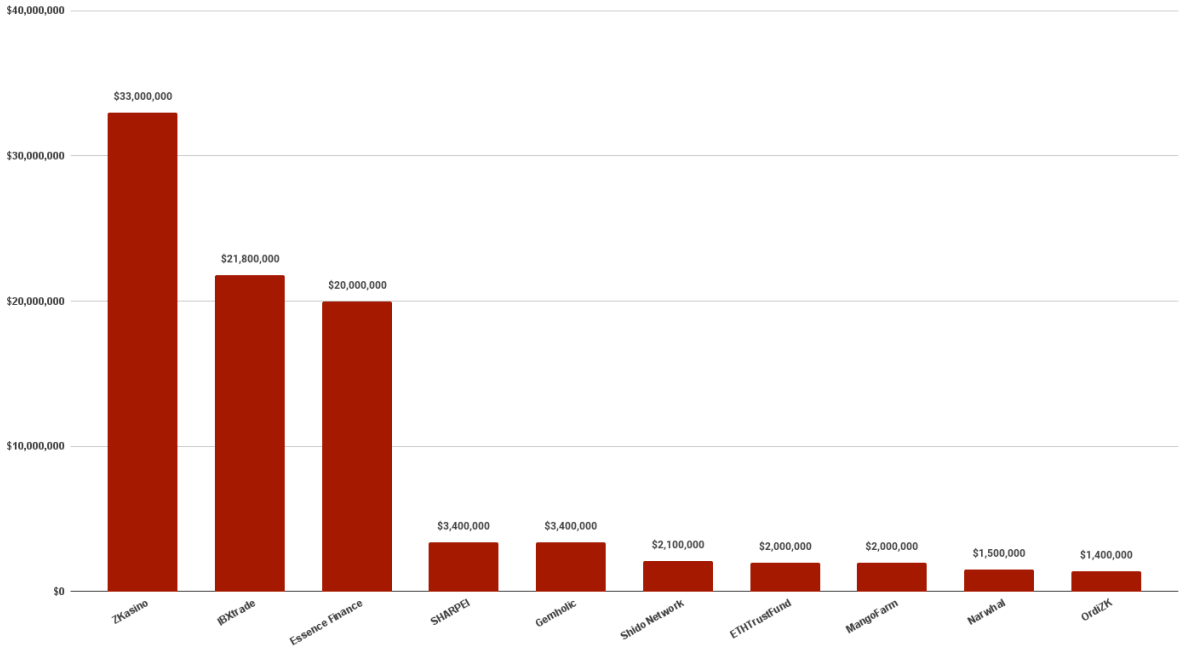
2.2.10 FixedFloat

2024 年 2 月 16 日，根据链上数据，加密货币交易平台 FixedFloat 遭攻击，损失约 409 枚 BTC（约 2,117 万美元）和 1,728 枚 ETH（约 485 万美元）。FixedFloat 针对此次攻击事件表示：这次黑客攻击是由于安全结构中的漏洞引起的外部攻击，并不是由员工所实施，用户资金并未受影响。4 月 2 日，FixedFloat 在 X 平台表示其再次遭受了 2 月 16 日攻击事件的黑客的攻击。黑客设法利用了 FixedFloat 使用的第三方服务中的漏洞。这两次攻击事件给 FixedFloat 造成总计约 2,900 万美元损失。

2.3 Rug Pull

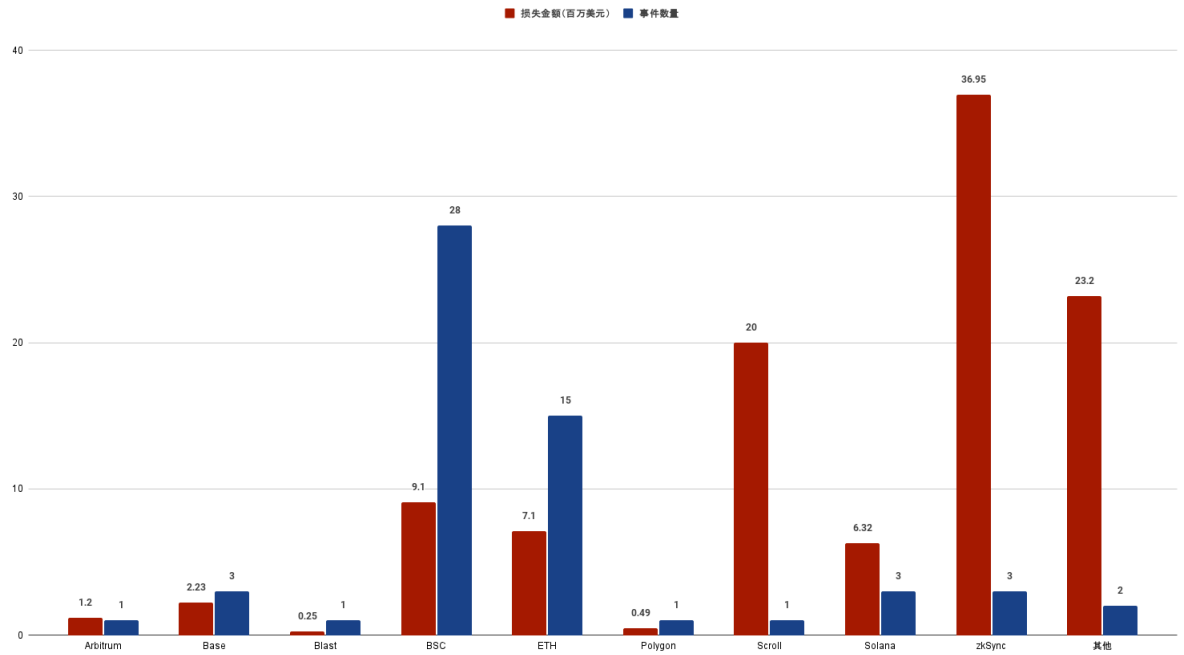
Rug Pull 是一种骗局，其本质是恶意项目方造势吸引用户投资，等到时机成熟便“拉毯子”，卷款跑路。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，2024 年 Rug Pull 事件达 58 起，导致损失约 1.06 亿美元。其中，zkSync 生态损失最高，达 3,695 万美元，BSC 生态发生了最多的跑路事件，达 28 起。

2024 损失 Top10 的跑路事件



（2024 损失 Top10 的跑路事件）

2024 各生态跑路事件分布及损失



（2024 各生态跑路事件分布及损失）

一些项目方在造势时，不惜重金邀请名人或圈内 KOL 为其站台、背书，以达到吸引关注、快速积累用户群体、提升项目知名度的目的。然而，也有一些项目方从一开始的宣传就充满造假行为，以此将作恶成本压到最低。例如，2024 年 10 月 23 日推出的 SHARPEI (SHAR)，该项目通过沙皮狗的卡通艺术作品进行推广，并借助 KOL 的推动，使其市值迅速飙升至 5,400 万美元。然而，SHARPEI 不久后突然套现 340 万美元，导致代币价格在数秒内暴跌超过 96%。泄露的宣传文件显示，该项目包含多项虚假信息，包括虚假的 KOL 雇佣声明以及关于与多个平台和项目合作的虚假声明。

随着 Meme 币热潮的到来，许多用户在投机和 FOMO 情绪驱使下，忽视了潜在风险。一些发币方甚至无需向用户描绘愿景或提供白皮书，仅凭一个概念或口号，便能炒作出热度吸引用户购买代币。低廉的作恶成本导致跑路事件层出不穷。用户资金被恶意项目方 Rug 后，往往面临漫长且困难的追回过程。对此，慢雾安全团队建议用户在参与项目之前，充分了解项目的背景和团队信息，谨慎选择投资项目，以规避潜在风险。

2.4 钓鱼

注：本小节专注分析 EVM 兼容链上的 Wallet Drainer 攻击，由 ScamSniffer 倾情撰写，在此表示感谢。

2.4.1 概述

Wallet Drainer 是一种部署在钓鱼网站上，通过诱导用户签署恶意交易来盗取加密资产的攻击方式。2024 年，此类攻击造成约 4.94 亿美元损失，同比增长 67%。虽然受害者数量仅增长 3.7%（达到 33.2 万地址），但单次攻击损失显著增加，最大单笔被盗金额达 5548 万美元。

2.4.2 关键数据对比

（2024 年 Wallet Drainer 攻击的关键数据指标）

(1)2024 年关键指标

- 总损失：4.94 亿美元，增长 67%
- 受害者数量：33.2 万地址，增长 3.7%
- 最大单笔被盗：5548 万美元
- 大额被盗数量：30

(2)年度重大事件

- Q1：比特币价格创历史新高，链上活动增加，钓鱼同步上升
- Q2：Pink Drainer 宣布退出
- Q3：行情调整，钓鱼活动降温，但偶有超大额受害事件
- Q4：Inferno Drainer 声称退出，由 Angel Drainer 接管

接下来，我们将详细分析这些事件背后的损失数据，以揭示趋势和潜在的风险。

2.4.3 损失分析

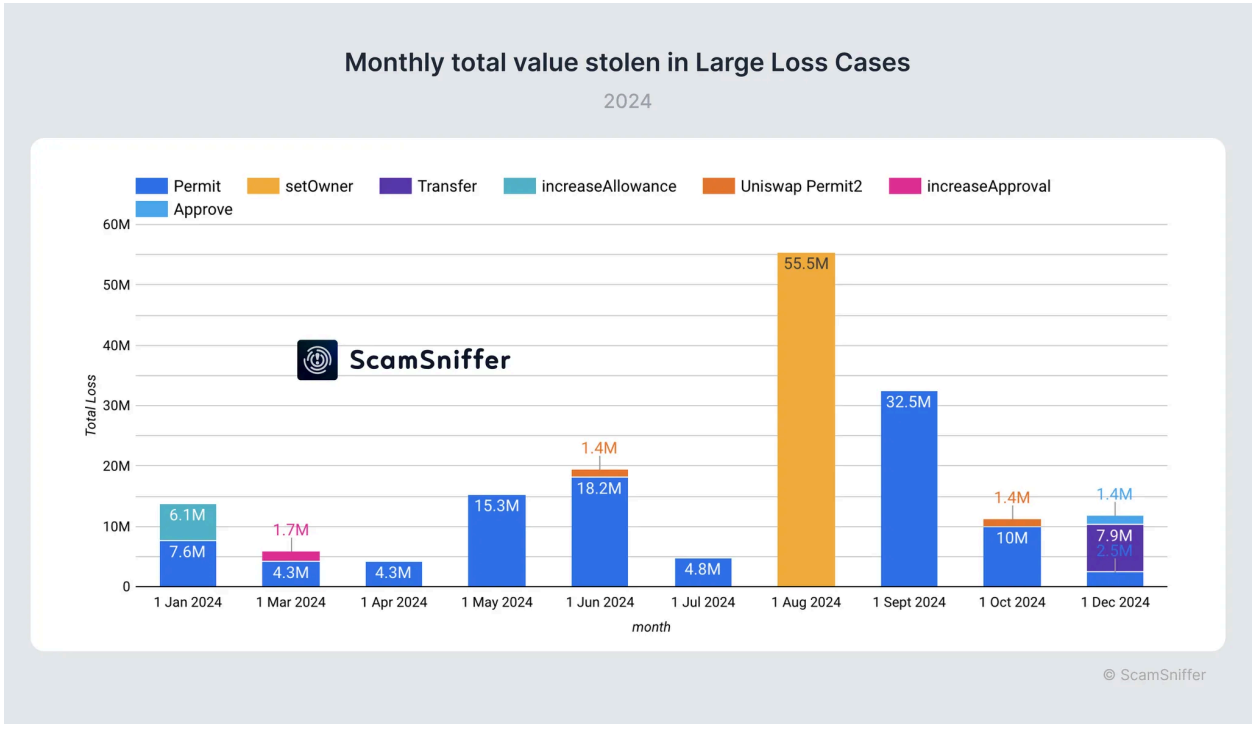
(1)按月总体损失趋势

全年攻击活动分为三个阶段：第一季度损失最重，达到 1.87 亿美元，受害者 17.5 万。3 月损失最高，7500 万美元。第二、三季度损失合计 2.57 亿美元，受害者降至 9 万人。第四季度损失降至 5100 万美元，受害者降至 3 万人，表明安全性提升。

(2) 大额案件分析

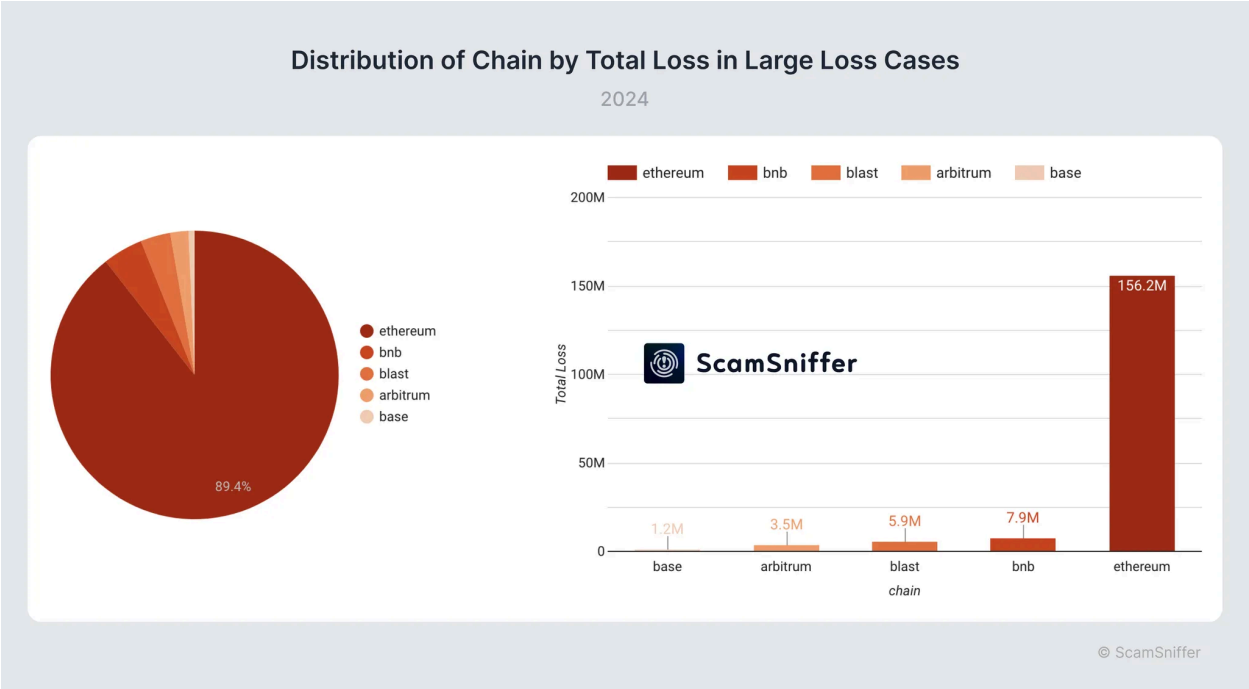
全年发生 30 起超 100 万美元案件，总损失 1.71 亿美元，平均每个受害者损失 570 万美金，最大单笔被盗 5548 万美元。

- 大额被盗月度趋势分析：

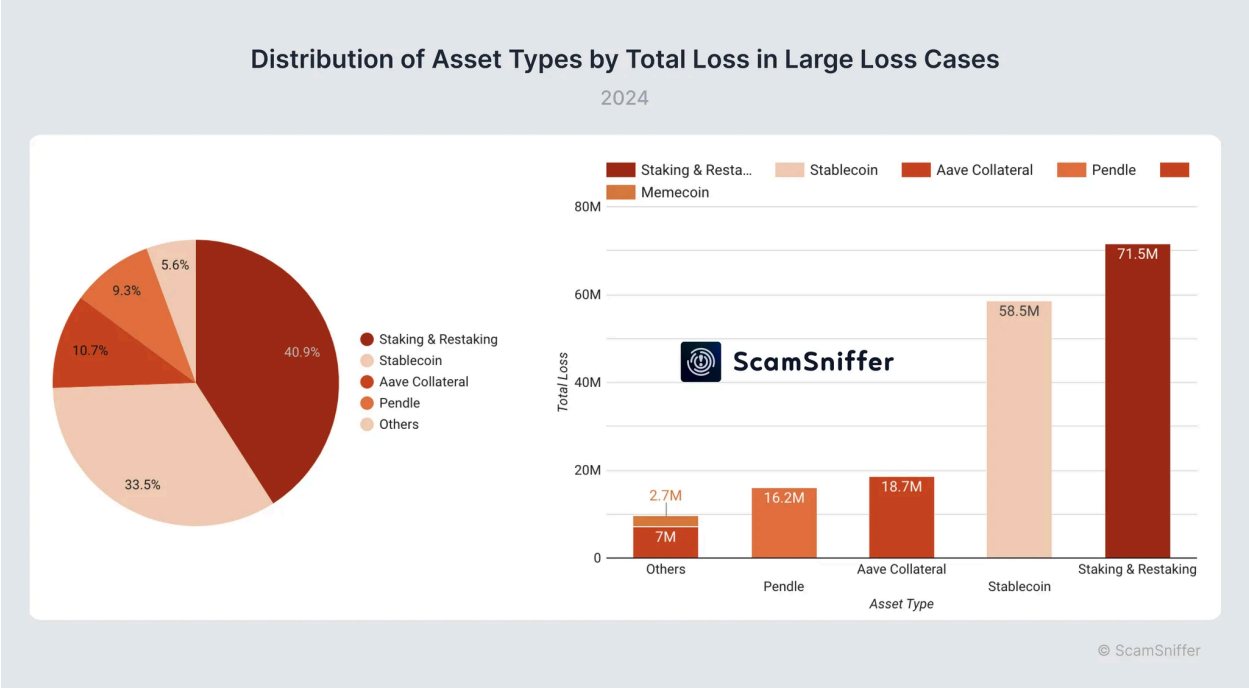


大额被盗案件在 2024 年呈现明显的阶段性变化。上半年（1 - 6 月）频发但规模较小，单笔金额多在 100 - 800 万美元区间。7 - 9 月进入高发期，8 月和 9 月分别出现 5548 万和 3251 万美元的重大损失，这两个月占全年大额案件总损失的 52%。最后一个季度攻击频率和规模明显收缩，单笔金额多降至 200 - 600 万美元区间，显示出市场安全意识的整体提升。

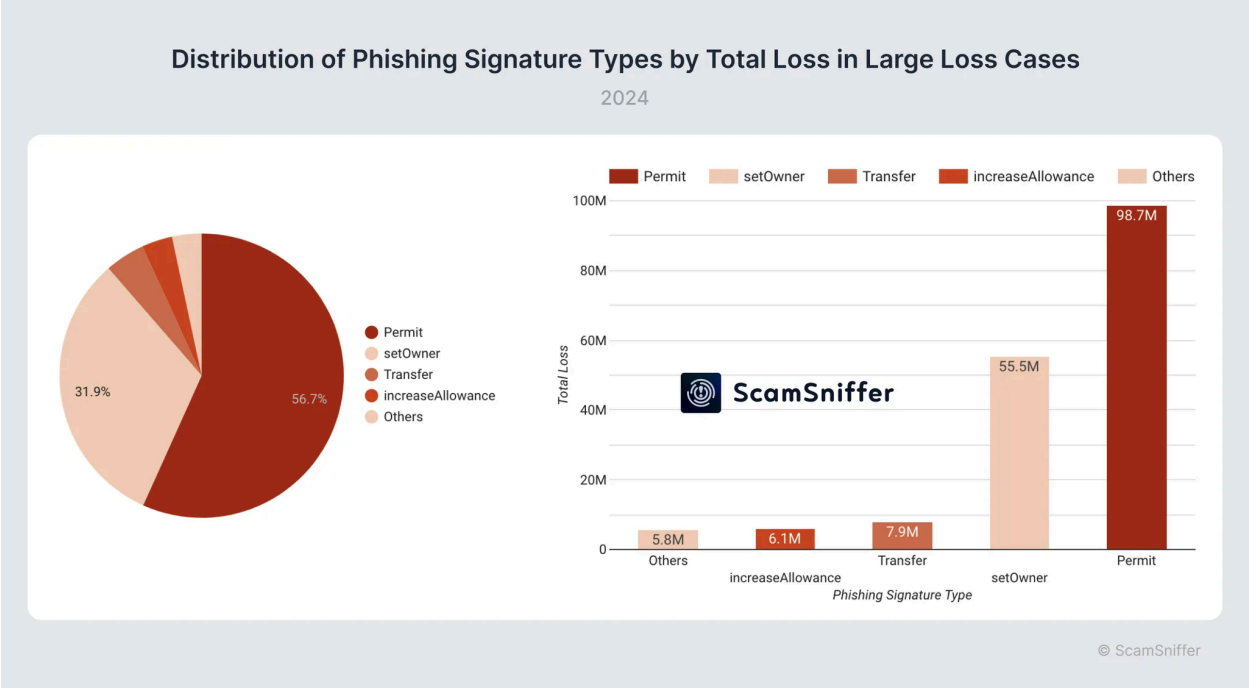
- 损失分布特征：



- 链分布：
  - Ethereum（25 起，占 85.3%），损失 1.56 亿美元
  - Arbitrum（2 起，355 万美元）
  - Blast（1 起，590 万美元）
  - Base（1 起，120 万美元）
  - BNB Chain（1 起，790 万美元）

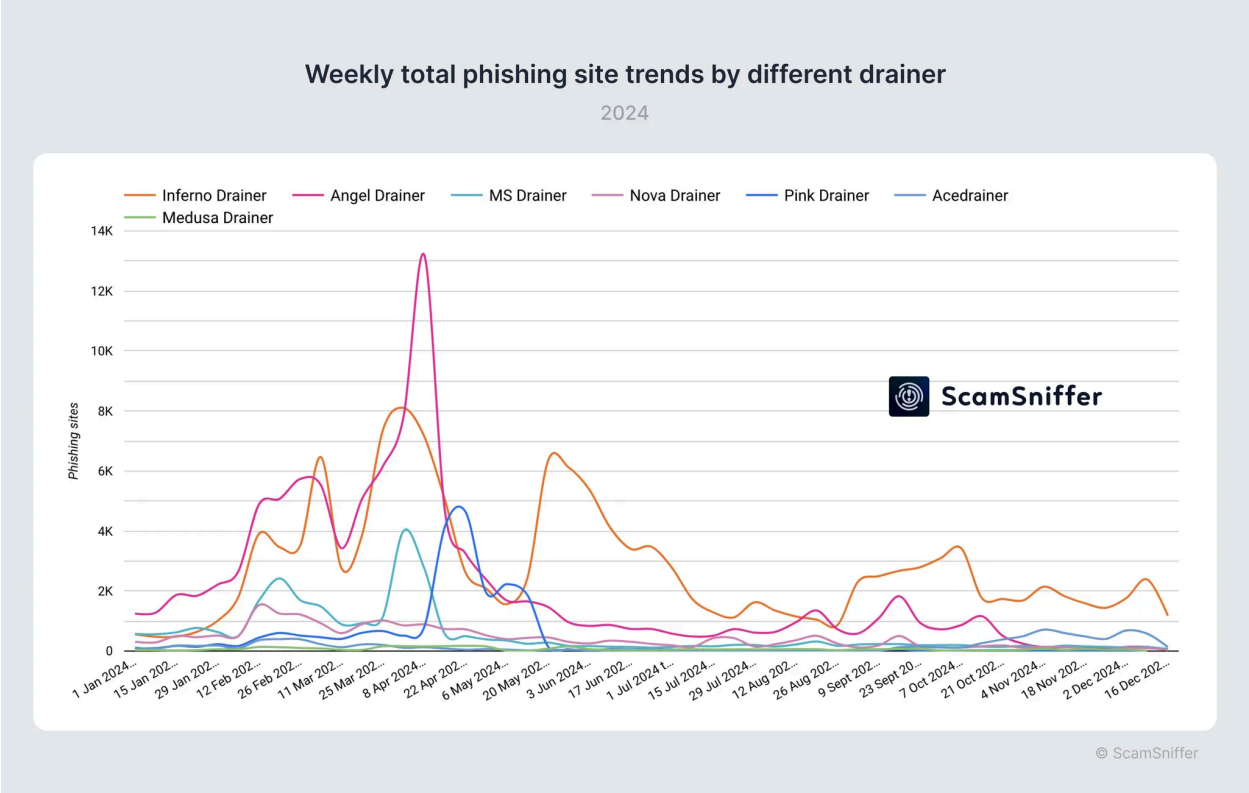


- 资产类型：
  - Staking & Restaking（40.9%）
  - Stablecoin（33.5%）
  - Aave Collateral（10.7%）
  - Pendle Yield (9.3%)
  - Others (5.6%)



- 钓鱼签名类型：
  - Permit（56.7%）
  - setOwner（31.9%）
  - Transfer (4.5%)
  - increaseAllowance（3.5%）
  - Others（3.4%）

2.4.4 Wallet Drainer 演变



(1)重要节点

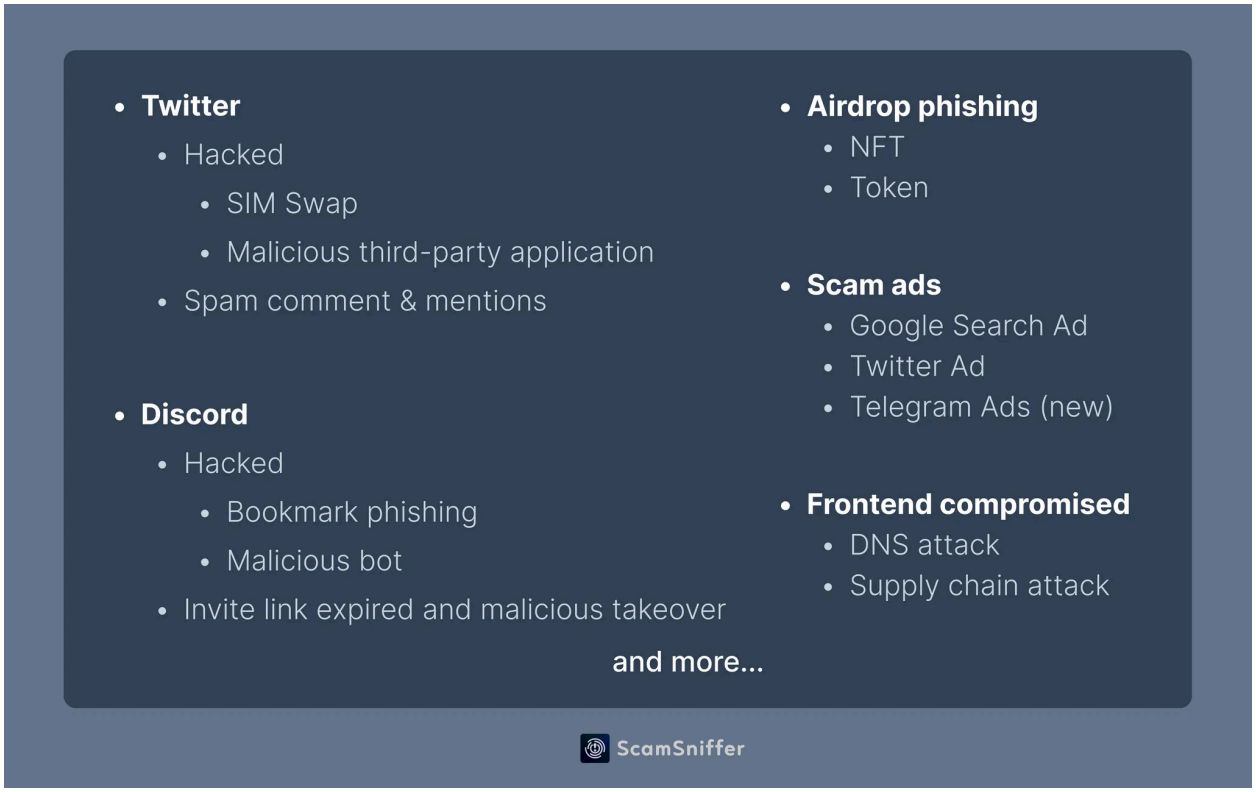
- Pink **退出**(5 **月底**):**市占** 28%，**份额被** Inferno **吸收**。
- Angel **接管** Inferno(10 **月底**):Angel **份额下降**，Inferno **维持** 40 - 45% **市占**。

(2)市场格局演变

- Q1-Q2:**三大主导**(Angel:42%，Pink:28%，Inferno:22%)
- Q3:**双头竞争**(Inferno:43%，Angel:25%)
- Q4:**新格局**(Inferno **及** Angel:45%，Acedrainer:20%，**其他新** Drainer:25%)

2.4.5 传播渠道分析

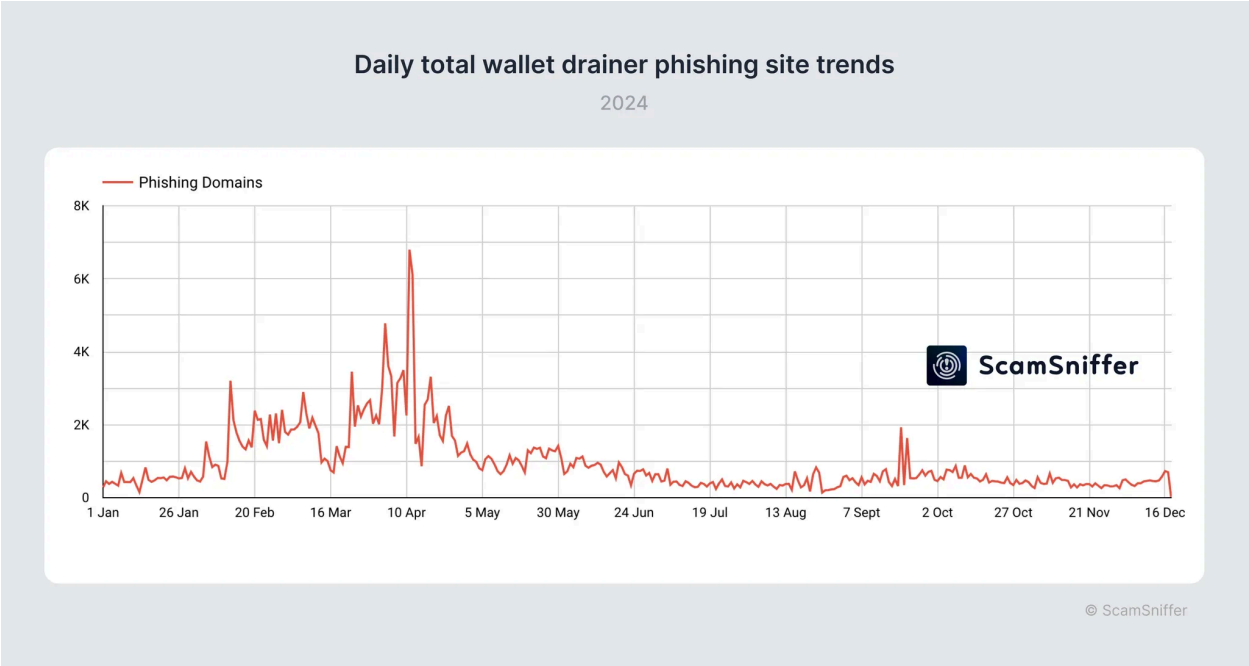
(1)钓鱼网站获取流量的常见方式



钓鱼网站主要通过以下方式获取流量：

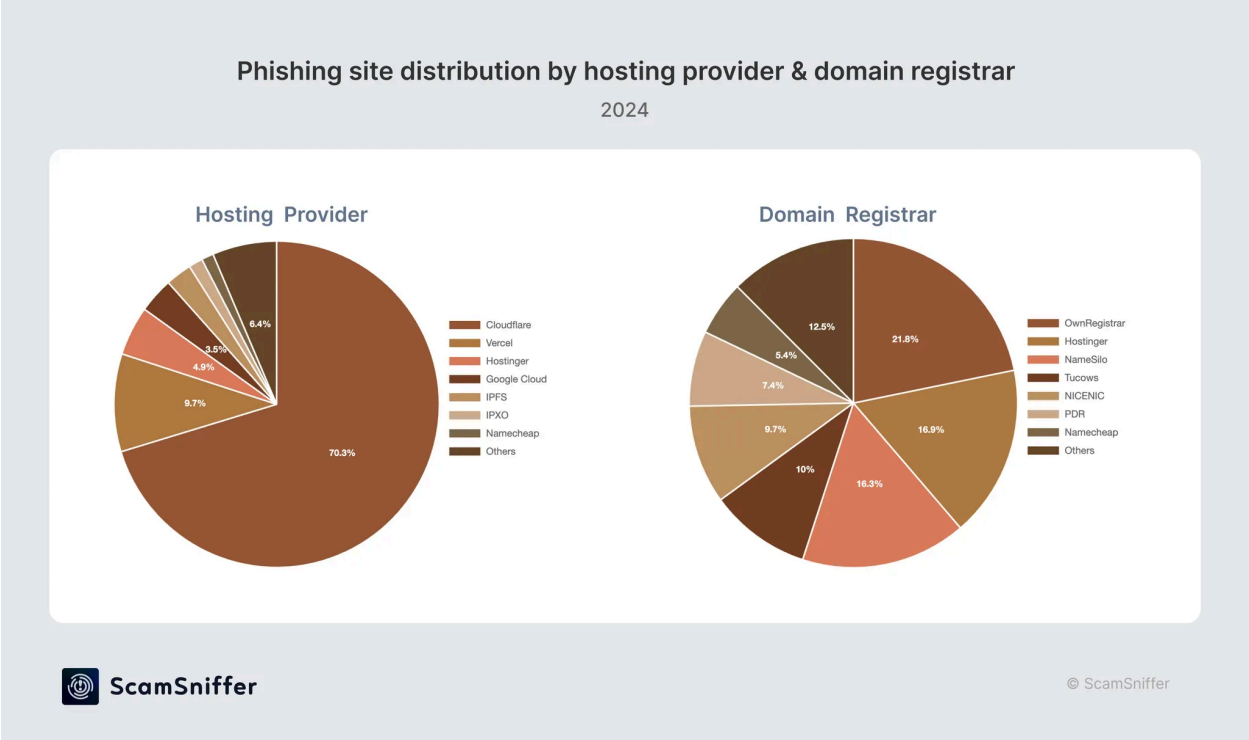
- 黑客攻击：官方项目 Discord 和 Twitter 账号被黑客入侵，前端或供应链攻击。
- 自然流量：NFT 或代币空投，过期 Discord 链接被接管。
- 付费流量：Google 搜索 / Twitter / Telegram 广告。
- 其他：Email / 社交 / IM 私信/其他

(2)钓鱼网站活跃度分析



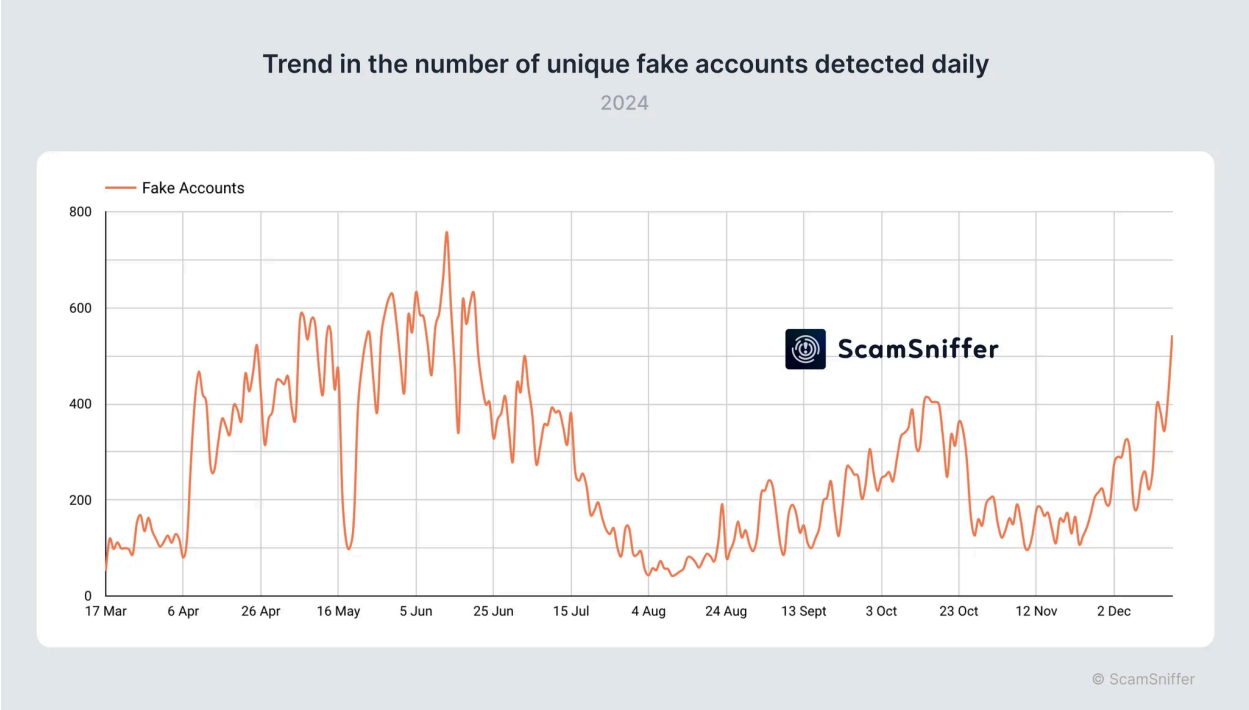
Q1 的钓鱼网站活跃度全年最高，解释了该季度的高被盗损失。下半年因行情调整，加上因 Pink、Inferno 等 Drainer 相继退出，整体活跃规模均较低于上半年。

(3)钓鱼网站托管服务&域名注册商分布



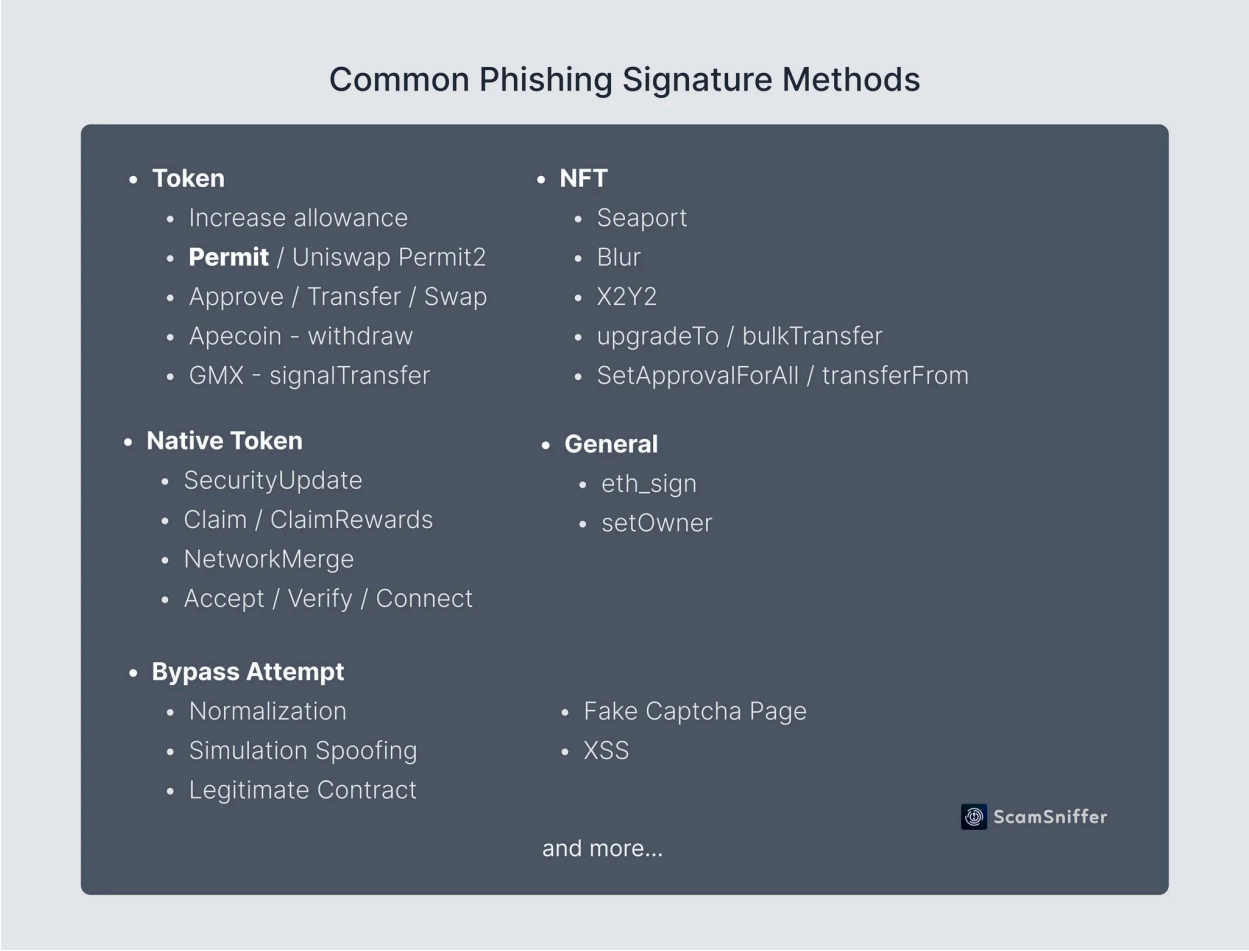
大部分钓鱼网站部署都使用了 Cloudfalre 和 Vercel，然后 IPFS。主要使用的域名注册商有 OwnRegistrar, Hostinger, NameSilo, Tucows 等。

(4)X 平台假冒账户趋势



和钓鱼网站活跃度基本一致，上半年整体较活跃，7 月份因 X 平台加大了假冒账户的打击力度，以及加上加密货币整体市场在调整，假冒账户整体下降。但随着 9 和 10 月份之后随着行情的回暖而逐步增加。

2.4.6 常见钓鱼签名方式



在钓鱼签名方面 Permit 依旧是代币被钓鱼的主要原因。

其中还值得一提的是针对 Proxy 修改其所有权地址的 setOwner，这一钓鱼签名在 8 月份直接导致一名受害者因此损失 5500 万美金的 DAI。

(1)检测绕过

随着更多的钱包加大在钓鱼安全这块的投入。对钓鱼 Wallet Drainer 而言他们也在持续的投入研究一些绕过方式比如：

- 利用钱包规范化过程发起钱包能处理，但安全检测层未必能处理数据的签名请求
- 利用合法合约，网站增加 Cloudfalre 或虚假验证码页面来防止被检测
- 利用 XSS 漏洞来试图绕过钱包黑名单
- 对钱包的模拟结果进行结果欺骗

总之这是一场持续的猫捉老鼠的游戏。

2.4.7 安全建议

(1)用户安全建议

Web3 的安全不仅需要工具的保护，更需要用户建立正确的安全意识和行为习惯。在享受 Web3 创新带来便利的同时，请始终将安全放在首位，保持警惕，做好防护。毕竟在去中心化的世界里，每个人都是自己资产的最终守护者。

(2)钱包开发安全建议

钱包作为用户进入 Web3 世界的重要入口，在用户资产安全保护中扮演着关键角色。通过建立完善的安全策略、持续升级防护能力，并积极采用行业领先的安全解决方案，钱包可以为用户提供更安全可靠的服务环境。这不仅是责任，更是在竞争激烈的市场中保持优势的必要条件。

2.4.8 未来展望

截至 2024 年，基于钓鱼签名的已知损失达 7.9 亿美元。尽管下半年此类攻击有所减少，但这可能预示着攻击者正在转向其他攻击方式，如恶意软件等更具隐蔽性的手段。

随着 Web3 生态的发展，保护用户资产安全的挑战依然存在。无论攻击方式如何变化，持续的安全意识和防护能力建设始终是保护资产安全的关键。

2.5 欺诈手法

根据慢雾 AML 团队收集到的用户被盗表单数据来看，欺诈仍然是导致用户资产受损的主要原因之一。特别是在牛市的推动下，大量新人涌入 Web3，这一现象变得更为突出。许多新用户由于未意识到区块链“黑暗森林”的危险，往往在一开始就因欺诈而蒙受损失。骗子主要利用了新用户对加密货币市场的认知不足，以及对高收益的渴望。通过一系列看似可信的设计和操作，成功引导这些用户投入资金。对于缺乏经验或者安全意识不足的用户而言，这些套路极具迷惑性，往往难以辨别其背后的风险。而且，近期较为高发的假 Zoom 钓鱼攻击手法还结合了社会工程学攻击和木马攻击技术，用户稍有不慎便会中招。鉴于此，我们将介绍几类常见的欺诈手法，帮助用户了解和规避常见的风险。

2.5.1 挖矿诈骗

这类骗局通常依赖于“资金需要在池子里存放一段时间才能产生收益”的机制，使得用户在短时间内难以察觉自己受骗了。在骗子的引导下，用户为了追求更高的利息，往往还会持续投入更多资金。当用户无法继续提供资金时，骗子便会威胁说这样会导致无法赎回本金，最终用户在重重压力下不断受损。

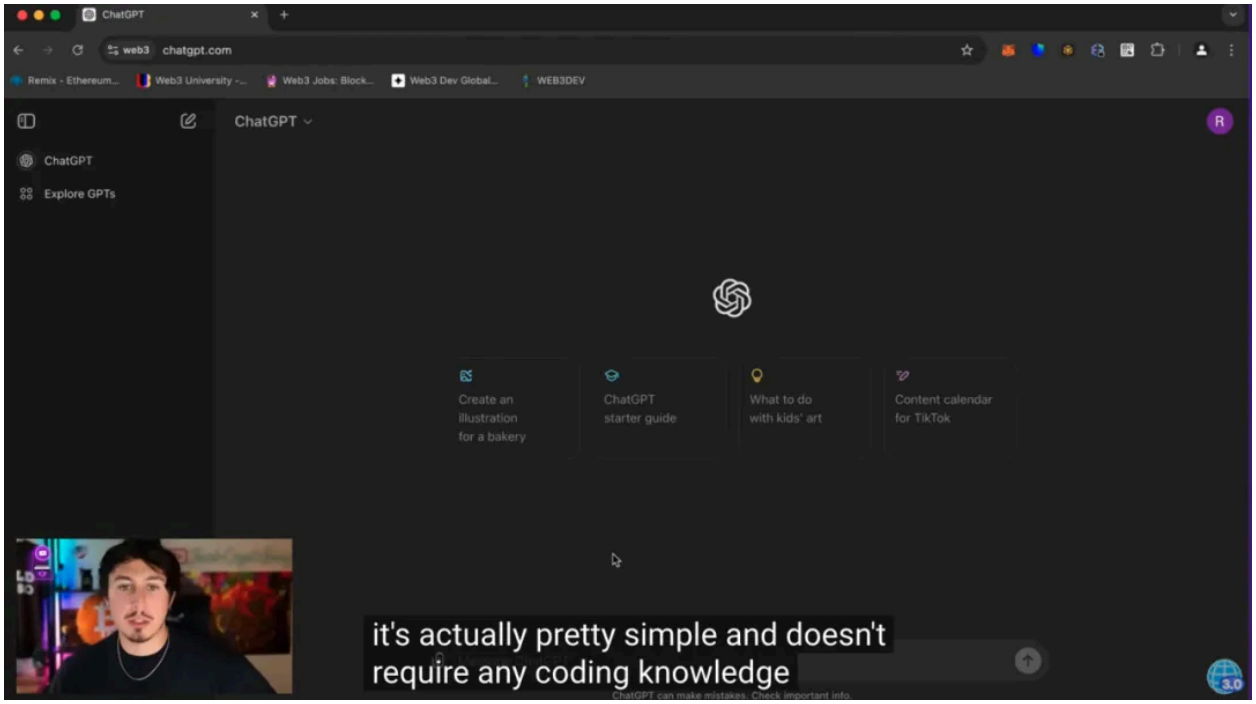
根据多位受害者的描述，骗子在 Telegram 上冒充知名交易所建立诈骗群组，这种诈骗群的组员动辄几千上万人，很容易让人放松警惕。不少用户在 Telegram 上搜索官方账号时会把群人数当作辨别账号真伪的因素之一。官方群的人数会比较多是没错，但是这个逻辑倒推回来就不一定对了。难以想象，骗子建立一个有上万人的群竟是为了骗几只“羊”，甚至里面的“闲聊”都是诱饵。值

得注意的是，一个有五万多人的群，在线人数却不足一百人，参考其他万人群的在线人数情况，用户们或许能意识到有些不对劲了。

对于新手用户，骗子还贴心配备了详细的操作教程，教用户如何查看矿池质押情况、如何下载钱包以及如何把资金转入骗子的合约地址。利用流动性挖矿经济激励机制的假象，骗子成功吸引到用户投入资金。用户往合约地址打款后，收到了返利，便想投入更多的资金以获得更多的收益，此举正中骗子的圈套，最后用户投入的资金都被骗子卷走。更可恶的是，还有些骗子在给用户返利时，返回的甚至是假币，不明所以的新用户以为真的收到了返利，直到尝试交易返利的币时才发现这是假币，毫无价值。此外，骗子还可能诱导用户进行恶意授权，从而盗取用户资金。

2.5.2 套利诈骗

AI 已经成为越来越多人提升生产力的工具，骗子也深谙这一点，给自己的骗局带上了 ChatGPT 这个标签，既吸引注意力，又显得靠谱高级。然而，ChatGPT 只在骗子的视频教程里短暂出现过。骗子声称套利机器人的代码是他利用 ChatGPT 生成的，顺带打消了一部分用户对代码作恶的怀疑。



骗子声称，他的这个机器人可以监控 Ethereum 上的新代币和大的价格变化，寻找套利机会，用户只需要坐等收钱就行。而用户首先得有个 MetaMask 钱包，然后打开教程中提供的 Remix 链接（假 Remix）。接着，用户需要粘贴骗子提供的代码、编译机器人和部署智能合约。到了这一步，骗子表示用户得为合约提供初始资金，且往合约里存越多的 ETH，就能获得越多的利润。而在用户按上述流程操作并点击了“start”后，钱就“消失”了，打入的套利本金都进入骗子钱包地址，因为代码有后门。

我们使用链上追踪和反洗钱平台 MistTrack 分析骗子的地址，发现骗子采取的是广撒网，积小利的模式，因此虽然受害者众多，但因损失相对较少，花费精力去追究不太现实，这类骗子便能够长期逍遥法外，给骗局换个“皮”便可继续进行类似的欺诈活动。

2.5.3 空投诈骗

Web3 项目方为了增加项目的知名度和实现初期用户的积累，常常会免费向特定钱包地址分发代币，这一行为被称为“空投”。空投能够在短时间内将项目从默默无闻推向大众视野，迅速积累用户基础，提升市场影响力。用户在参与 Web3 项目时，需要点击相关链接、与项目方交互以获取空投代币，然而从高仿网站到带后门的工具，黑客早已在用户领空投过程的上下游布满了陷阱，以下是几类常见的空投骗局。

- 假空投

此类骗局又可以细分为以下几种：

1、黑客盗取项目方的官方账号发布假空投的消息。我们经常可以在资讯平台上看到“某项目的 X 账号或者 Discord 账号被黑，请广大用户不要点击黑客发布的钓鱼链接”的安全提醒。用户通常是基于对官方账号的信任而点击这些链接，进而被引导至伪装成空投的钓鱼网站。一旦在钓鱼网站上输入了私钥/助记词或授权了相关权限，黑客就能盗走用户的资产。

2、黑客使用高仿的项目方账号在项目方官方真实账号的评论区刷留言，发布领取空投的消息，诱导用户点击钓鱼链接。此外，在真项目方发布空投的消息后，黑客也会紧随其后，在社交平台上使用高仿账号大量发布包含钓鱼链接的动态，许多用户因未仔细辨别而安装了虚假 APP 或打开钓鱼网站进行了签名授权的操作。

3、骗子潜伏在 Web3 项目的群组里，挑选目标用户进行社会工程攻击，有时以空投为诱饵，“教”用户按照要求转移代币以获取空投。请广大用户提高警惕，不要轻易相信主动联系你的“官方客服”或是“教”你如何操作的网友，这些人大概率是骗子，你只是想领个空投，结果却损失惨重。

- “白给”的空投代币

前文提到，用户往往需要完成某种任务才能获取空投，我们接下来看看“白给“用户代币的情况。黑客会向用户的钱包空投没有实际价值的代币，用户看到这些代币，可能会尝试与之交互，例如转移、查看或在去中心化交易所上进行交易。然而我们逆向分析一个 Scam NFT 的智能合约发现，当尝试挂单或转移这个 Scam NFT 时会失败，然后出现错误提示“Visit website to unlock your item”，诱导用户访问钓鱼网站。

ByteCode Decompilation Result:

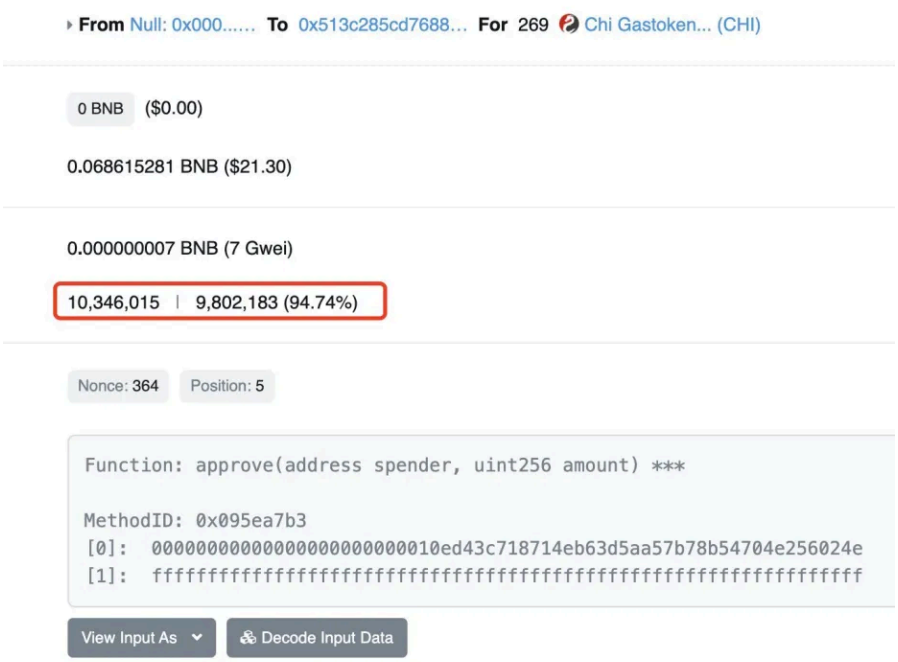
```
80  def initialize() payable:
81    if _owner:
82      require caller == _owner
83    _owner = caller
84
85  def unknownaa58d5a6(uint256 _param1) payable:
86    require calldata.size - 4 >=ΓC 32
87    require _param1 == addr(_param1)
88    require caller == _owner
89    unknownc1fec681Address = addr(_param1)
90
91  def unknowneed866f9(uint256 _param1) payable:
92    require calldata.size - 4 >=ΓC 32
93    require _param1 == addr(_param1)
94    require caller == _owner
95    unknownd493465aAddress = addr(_param1)
96
97  def setApprovalForAll(address _to, bool _approved) payable:
98    require calldata.size - 4 >=ΓC 64
99    require _to == _to
100   require _approved == _approved
101   revert with 0x8c379a000000000000000000000000000000000000000000000000000000000000000, 'Visit website to unlock your item.'
102
```

如果用户访问了 Scam NFT 引导的钓鱼网站，黑客便可能进行以下操作：

- 批量“零元购”有价值的 NFT，见“零元购” NFT 钓鱼分析
- 拿走高价值 Token 的 Approve 授权或 Permit 签名
- 拿走原生资产

此外，黑客还可以通过精心设计的恶意合约窃取用户的 Gas 费。首先，黑客在 BSC 上创建了一个名为 GPT 的恶意合约 (0x513C285CD76884acC377a63DC63A4e83D7D21fb5)，通过空投代币吸引用户进行交互。

用户与该恶意合约交互时，出现了需要批准该合约使用钱包中代币的请求。如果用户批准了这个请求，恶意合约会根据用户钱包中的余额，自动提高 Gas 限额，这使得后续的交易消耗更多的 Gas 费。利用用户提供的高 Gas 限额，恶意合约使用多余的 Gas 来铸造 CHI 代币（CHI 代币可以用于 Gas 补偿）。恶意合约积累了大量的 CHI 代币后，黑客可以通过燃烧 CHI 代币，获得合约销毁时返还的 Gas 补偿。黑客巧妙地利用用户的 Gas 费为自己牟利，而用户可能并未察觉到他们已经支付了额外的 Gas 费。用户本以为可以通过出售空投代币获利，结果却被盗取了原生资产。



- 带后门的工具

领空投的过程中，一些用户需要下载翻译或查询代币稀有度之类的插件，这些插件的安全性不仅存疑，且有的用户下载插件时没有从官方渠道下载，这就使得下载到带有后门的插件的可能性大大增加。此外，我们还注意到网上有出售领空投脚本的服务，声称可以通过运行脚本完成自动批量交互，听起来挺高效的，但是请注意，下载未经审查和验证的脚本存在极大的风险，因为你无法确定脚本的来源和它的真实功能。脚本可能包含恶意代码，潜在的威胁包括盗取私钥/助记词或者执行其他未授权的操作。而且，一些用户在执行相关类型的风险操作时，未安装或是关闭了杀毒软件，导致未能及时发现设备中了木马，进而受损。

2.5.4 盗 X 行骗

与市场火热，众多新用户带着 FOMO 情绪涌入 Web3 相随的是账号被黑事件频发，众多新用户或是安全意识不足的用户蒙受损失。黑客利用知名账号的影响力和名人的号召力，发布操纵代币价格的虚假消息，含有钓鱼链接或推广虚假代币的动态，一旦用户点进了钓鱼链接进行交互或是购买了黑客推广的代币，便会受损。据慢雾安全团队统计，2024 年发生了 94 起账号被黑事件，占总安全事件数的 22.9%。

值得注意的是，黑客的攻击对象不再局限于区块链知名项目和成员，还包括传统行业的知名品牌和知名官方机构等，如 2024 年 1 月，美国证券交易委员会（SEC）的 X 账户遭未经授权接管，黑客

发布了来自 SEC 主席的虚假消息(比特币 ETF 已被批准)，结果导致比特币(BTC)的价格短时飙升 1,000 美元。2024 年 11 月 27 日，链上侦探 ZachXBT 在 X 发文表示:“在过去的几个月里，我一直在 X 和 IG 上追踪针对麦当劳、Usher、Kabosu Owner、Andy Ayrey、Wiz Khalifa、SPX 6900 等的一系列相关攻击，这些攻击通过推出 Pump.Fun Meme 币导致约 350 万美元的资损失。”

ZachXBT
@zachxbt

1/ Over the past few months I have been tracking a series of related compromises for McDonald's, Usher, Kabosu Owner, Andy Ayrey, Wiz Khalifa, SPX 6900, etc on X & IG which has resulted in an estimated $3.5M+ stolen via launching Pump Fun meme coins.

由 Google 翻译自 英语

1/ 在过去的几个月里，我一直在 X 和 IG 上追踪针对麦当劳、Usher、Kabosu 老板、Andy Ayrey、Wiz Khalifa、SPX 6900 等的一系列相关攻击，通过推出 Pump Fun 模因币，估计有超过 350 万美元被盗。

翻译得准确吗？请提供反馈，以便我们加以改进：

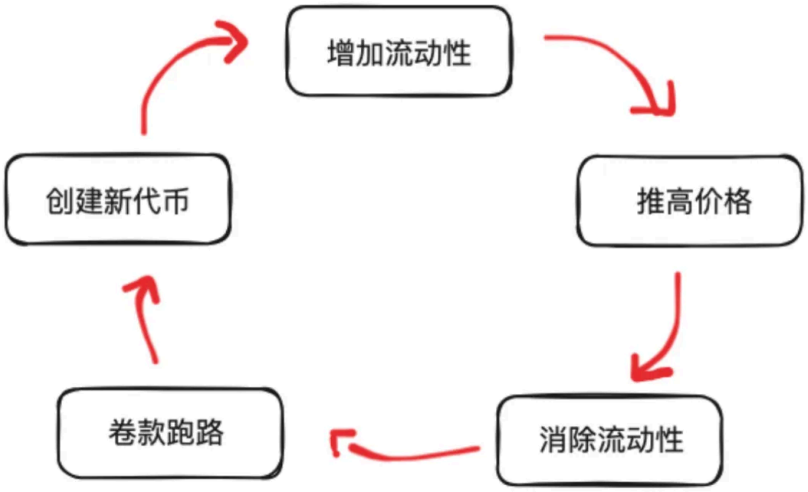
Account	Platform	Date	Token
McDonald's	IG	Aug 21, 2024	GRIMACE
Dean Norris	X/Twitter	Sep 3, 2024	SCHRADER
Usher	X/Twitter	Sep 12, 2024	USHER
Ken Carson	X/Twitter	Sep 28, 2024	KEN
SPX 6900	X/Twitter	Oct 11, 2024	QQQ420, NASDAQ420
Enoshima Aquarium	X/Twitter	Oct 15, 2024	SEAL
Kabosu Owner	IG	Oct 17, 2024	KAI
Andy Ayrey (Truth Terminal)	X/Twitter	Oct 29, 2024	IB, RNA, TRUTH, INFINITY, REALNIGGA, WOAH
Wiz Khalifa	X/Twitter	Nov 3, 2024	WIZ, WIZZLE

上午12:41 · 2024年11月27日 · **195.1万** 查看

(https://x.com/zachxbt/status/1861450263925559399)

2.5.5 貔貅盘

传说中，貔貅是一种神奇的生物，据说吞入的财宝无法再从其体内取出。这一形象恰如其分地描述了貔貅盘骗局:用户购买貔貅币后，通常会看到代币快速升值，于是想等到代币的涨幅足够大了再尝试兑换，然而合约本身却用多种方式限制用户卖出，如将买家地址加入黑名单，更改地址内的代币数量或是设置苛刻的卖出门槛等，最终用户发现自己无法卖出，资金被套牢。



以下用户陷入貔貅盘的几个常见原因：

- 仿盘：不单现实世界里有假币，虚拟货币也有假币。一些仿盘项目会复制知名项目的名称和标识，创建相同名称的代币合约。用户可能因为没有仔细检查代币的合约地址而误入貔貅盘，结果陷入无法卖出的困境。

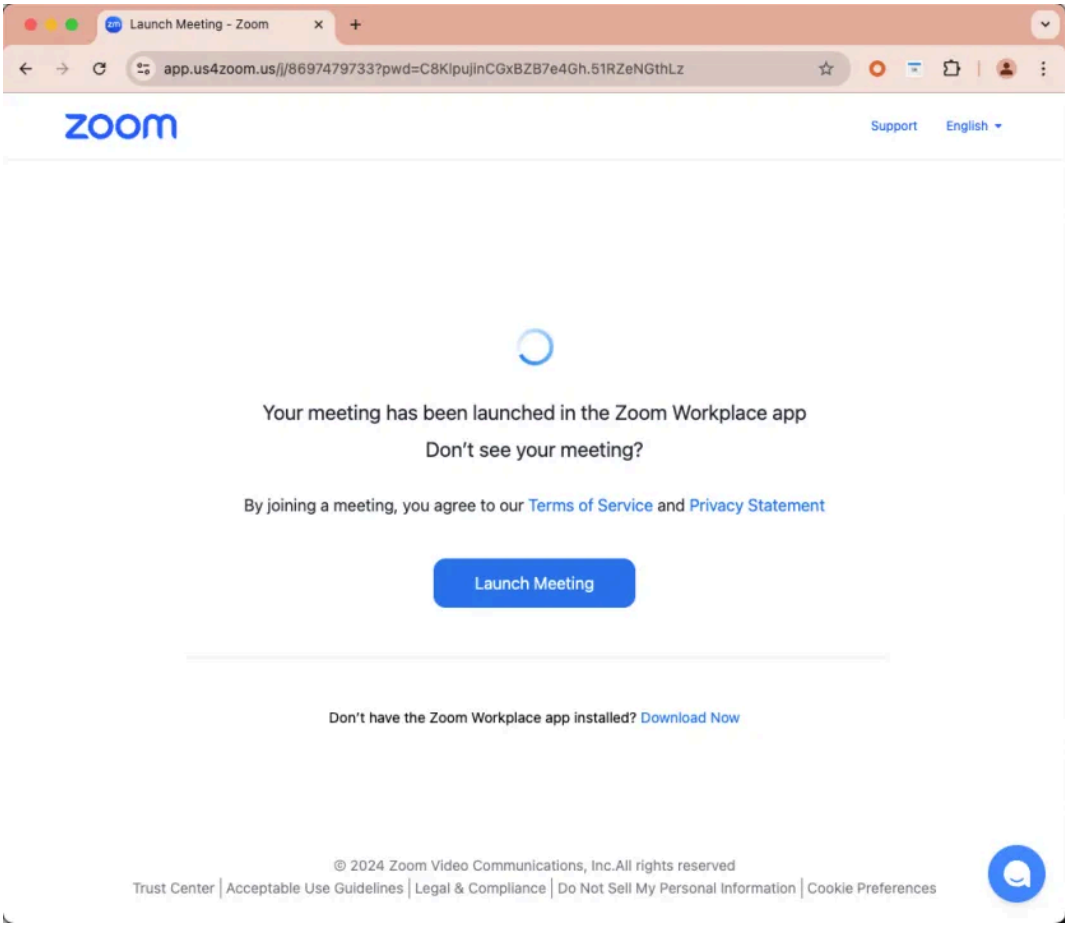
- “赛跑”心态：有些用户明知项目不可靠，甚至已经察觉其中的可疑之处（蜡烛图的柱体是接连的绿色），但抱有“跑得快就没事”的侥幸心理，实际上进去就基本出不来了。用户原本以为可以在上涨趋势中迅速买入，再择机卖出，那不是稳赚不赔的吗？但当他们试图卖出时，要么完全无法操作，要么只能卖出极少量的代币。

- 受骗子诱导投资：还有一种常见的情况是用户被骗子的花言巧语所诱惑，继而投资了貔貅盘。

2.5.6 恶意木马

2024 年，多位用户都曾遭遇一种伪装成 Zoom 会议链接的钓鱼攻击手法。其中一受害者在点击恶意 Zoom 会议链接后安装了恶意软件，导致加密资产被盗，损失规模达百万美元。恶意软件通常具备收集系统信息、窃取浏览器数据和获取加密货币钱包信息等多重危害功能，并将数据传输至黑客控制的服务器。这类攻击通常结合了社会工程学攻击和木马攻击技术，用户稍有不慎便会中招。

据慢雾安全团队分析，黑客使用形如“app[.]us4zoom[.]us”的域名伪装成正常 Zoom 会议链接，页面与真 Zoom 会议高度相似，当用户点击“启动会议”按钮，便会触发下载恶意安装包，而非启动本地 Zoom 客户端。



恶意代码采集完系统信息、浏览器数据、加密钱包数据、Telegram 数据、Notes 笔记数据和 Cookie 数据等信息后，会将它们压缩并发送至黑客控制的服务器。由于恶意程序在运行时就诱导用户输入密码，并且后续的恶意脚本也会采集电脑中 KeyChain 数据（可能包含用户保存在电脑上的各种密码），黑客收集后就会尝试解密数据，获得用户的钱包助记词、私钥等敏感信息，从而盗取用户的资产。慢雾安全团队建议用户在点击会议链接前谨慎验证，避免执行来源不明的软件和命令，安装杀毒软件并定期更新。

三、反洗钱态势

3.1 反洗钱及监管动态

2024 年，加密货币的监管环境发生了重大发展，其中最突出的是欧盟实施了 MiCA 法规，美国推进了稳定币立法。这些努力的推动力是人们对快速发展的加密行业中欺诈、洗钱和恐怖主义融资活动的担忧日益增加。今年，世界各地出台了更为严格的措施来打击非法活动，稳定币监管、跨境加密政策和针对加密领域主要参与者的执法行动取得了显著进展。

3.1.1 稳定币监管

随着全球金融当局认识到这些数字资产日益增长的影响力和风险，稳定币监管在 2024 年成为焦点。2022 年 TerraUSD 的崩盘清楚地提醒人们市场存在脆弱性，促使全球对稳定币的监管日趋严格和明确。今年是一个转折点，各地区通过立法和政策制定来应对稳定币带来的独特挑战，同时促进数字经济的创新。

- 中国：中国人民银行在 2024 年发布的《中国金融稳定报告》中，详细讨论了全球加密货币监管动态，特别提及香港的加密货币合规进展，强调了加强对加密资产的监管力度。
- 中国香港：2024 年 12 月 6 日，香港金融管理局（HKMA）和财经事务及库务局发布了《稳定币条例草案》，旨在为香港引入法币稳定币发行人的监管制度，完善虚拟资产活动的监管框架。
- 欧盟：欧盟批准了《加密资产市场监管法案》（MiCA），建立了全球首个完整且清晰的虚拟资产监管框架，计划于 2024 年底正式实施。其要求包括，稳定币发行人必须获得电子货币许可证、保持足够的储备并遵守严格的交易监管标准。世界上使用最广泛的稳定币 USDT 的发行人 Tether Limited 未能满足这些要求，导致 USDT 将于 2024 年 12 月 30 日起从欧盟合规平台上撤出。
- 巴西：巴西中央银行（BCB）计划 2025 年对稳定币和资产代币化进行监管。2024 年 11 月，BCB 提出监管提案，建议禁止用户将稳定币从中心化交易所提取至自托管钱包，但在 12 月表示若能改善交易透明度等关键问题，可能会撤销禁令。
- 美国：稳定币发行人现在必须维持 1:1 的储备，这一规定得到了正在进行的立法讨论的支持。

- 中东：阿联酋在其虚拟资产监管局（VARA）下引入了稳定币专用许可，表明该地区有意在监管透明度方面发挥带头作用。卡塔尔还将稳定币纳入其首个数字资产框架，标志着加密货币监管迈出了进步的一步。

3.1.2 SEC 执法

美国证券交易委员会（SEC）在 11 月公布了 2024 财年执法结果。报告显示，SEC 共提起 583 项执法行动，比 2023 年下降了 26%。执法行动共产生了 82 亿美元的罚款，这是 SEC 历史上的最高金额。在这些案件中，SEC 提起了 431 起"独立"诉讼，比 2023 年减少了 14%；93 起"后续"行政诉讼，旨在根据刑事定罪、民事禁令或其他命令禁止或暂停个人在证券市场担任某些职务，比 2023 年减少了 43%；59 起针对涉嫌拖欠向 SEC 提交所需文件的发行人的诉讼，比 2023 年减少了 51%。82 亿美元的财务补偿包括 61 亿美元的非法所得和判决前利息，这也是有史以来的最高金额，以及 21 亿美元的民事罚款，这是有史以来第二高的金额。82 亿美元的财务补偿中约有 56% 归因于美国证券交易委员会在陪审团审判中胜诉后获得的金钱判决，他们被指控犯有美国历史上最大的证券欺诈案之一。此外，在 2024 年，美国证券交易委员会获得命令，禁止124 名个人担任上市公司高管和董事，这是十年来禁止此类行为的第二高数字。2024 财年，SEC 向受害投资者发放了 3.45 亿美元，自 2021 财年开始以来，已向投资者返还了超过 27 亿美元。SEC 还在 2024 财年收到了 45,130 条举报、投诉和转介，这是一年中收到的最多的一次，其中包括 24,000 多条举报人举报，其中 14,000 多条由两名个人提交。SEC 发放的举报人奖励总额为 2.55 亿美元。SEC 表示 2024 年采取的多种执法行动表明，其紧跟人工智能虚假陈述、欺诈者利用社交媒体进行关系诈骗等新兴威胁，同时继续关注常青投资者风险，例如重大虚假陈述、内部控制不足和重大守门人失职。

以下是 SEC 在加密生态中采取的执法行动举例：

- Terraform Labs 和解：Terraform Labs 同意与美国证券交易委员会（SEC）就其 TerraUSD 和 Luna 加密货币的崩盘达成 45 亿美元的和解。和解包括 35 亿美元的非法所得、4.6 亿美元的利息、4.2 亿美元的民事罚款以及前首席执行官 Do Kwon 的 2 亿美元个人捐款。
- Jump Trading 罚款：高速交易公司 Jump Trading Group 同意向美国证券交易委员会支付 1.23 亿美元的和解金，因为该公司误导投资者了解 TerraUSD 的稳定性，TerraUSD 是一种于 2022 年崩盘的稳定币。美国证券交易委员会指控，Jump 旗下子公司 Tai Mo Shan 向投资者虚假保证了 TerraUSD 的稳定性，导致其垮台。

- SEC 起诉 Cumberland DRW：SEC 起诉高速交易公司 DRW Holdings 的加密货币部门 Cumberland DRW，因其未注册为证券交易商。诉讼称，Cumberland 在没有适当注册的情况下通过与对冲基金和大型市场参与者进行交易获得了数百万美元的利润。

3.1.3 反洗钱制裁

2024 年 5 月，香港对 Worldcoin 的指令：香港个人资料私隐专员公署向 Worldcoin 基金会发出强制执行通知，指示其因隐私和个人数据问题停止该地区的所有运营。Worldcoin 被指示停止扫描和收集公众的虹膜和面部图像，这反映了香港对保护加密领域个人数据的承诺。

2024 年 5 月，两名中国公民被捕：美国司法部逮捕了两名中国公民 Daren Li 和 Yicheng Zhang，罪名是策划一场名为"杀猪"的大规模加密货币骗局，导致洗钱金额至少达 7,300 万美元。

2024 年 5 月，美国财政部制裁伊朗虚拟货币挖矿活动：美国财政部通过其外国资产控制办公室（OFAC）扩大了对伊朗虚拟货币挖矿的制裁范围，特别是针对那些通过挖矿规避国际制裁的企业和个人。

2024 年 9 月，查获超过 600 万美元的加密货币信任计划：美国司法部宣布查获东南亚犯罪分子持有的超过 600 万美元的加密货币。这些人通过欺诈性的"杀猪"骗局瞄准美国居民。联邦调查局在区块链上追踪受害者资金，确定了持有非法资金的多个加密货币钱包地址。

2024 年 9 月，美国制裁俄罗斯网络犯罪分子：美国财政部对涉嫌俄罗斯黑客的 Sergey Ivanov 和 Cryptex 进行了制裁，原因是他们为网络犯罪分子和暗网供应商洗钱。美国财政部金融犯罪执法网络还将俄罗斯加密货币交易所 PM2BTC 列为重大洗钱威胁。

2024 年 12 月，美国对朝鲜虚拟货币洗钱网络的制裁：美国根据第 13382 号行政命令，对两名个人和一家实体实施制裁，旨在阻止朝鲜民主主义人民共和国通过虚拟货币洗钱为其非法大规模毁灭性武器和弹道导弹计划提供资金。

2024 年 12 月，美国指控 LockBit 勒索软件开发者：美国指控俄罗斯和以色列双重国籍的 Rostislav Panev 开发和维护 LockBit 勒索软件代码，并因其工作获得了超过 230,000 美元的加密货币。Panev 在以色列被捕，等待引渡到美国。

3.1.4 监管政策

3.1.4.1 亚太

- 中国：2024 年 12 月，中国人民银行发布了《中国金融稳定报告（2024）》，报告中详细讨论了全球加密货币监管动态，并重点提及了香港在加密货币合规方面的进展。鉴于加密资产对金融体系稳定可能产生外溢风险，各国监管部门不断加大对加密资产的监管力度。报告指出，全球已有 51 个国家和地区对加密资产出台禁止规定，部分经济体已调整原有法律或重新立法规范。此外，香港积极探索加密资产牌照管理，将虚拟资产分为证券化金融资产和非证券化金融资产，对虚拟资产交易平台运营者执行"双牌照"制度。
- 中国香港：2024 年 4 月，香港批准了比特币和以太坊的现货交易所交易基金（ETF），为投资者提供了新的投资渠道；香港证券及期货事务监察委员会（SFC）新增了 4 家虚拟资产交易所的牌照持有者，强化了对交易平台的监管；香港推出了稳定币沙盒和相关法案，旨在为稳定币的发行和使用建立明确的监管框架。
- 日本：先进的加密税改革将交易利润税降低至 20%，并强调加强交易所和发行人的反洗钱和 KYC 合规性。
- 韩国：制定《虚拟资产用户保护法》，加强投资者安全并规范跨境加密交易。
- 越南：越南政府发布了《国家区块链发展战略》，到 2030 年将自己定位为地区领导者。然而虚拟货币仍然未分类并被禁止作为法定货币，这促使人们努力在创新与预防犯罪之间取得平衡。
- 新加坡：新加坡金融管理局（MAS）修订了《支付服务法》，扩大了受监管的支付活动范围，包括数字支付代币服务，要求相关服务提供商申请相应牌照。MAS 已批准了至少 19 家加密服务提供商的主要支付机构牌照，允许其提供数字支付代币服务。
- 马来西亚：马来西亚证券委员会公布了 6 家获准运营的加密货币交易所名单，要求未经批准的实体立即停止活动并退还投资者资金。

3.1.4.2 北美

- 美国：比特币和以太坊 ETF 的批准标志着主流加密货币采用的一个里程碑。SEC 于 2024 年 1 月 10 日批准了现货比特币 ETF，并于 5 月 23 日批准了以太坊 ETF，以太坊现货 ETF 于 7 月 23 日正式交易。截至今年，美国比特币现货 ETF 的净资产价值为 1050.8 亿美元（占比特币市值的 5.7%），而以太坊现货 ETF 的净资产价值总计为 120.5 亿美元（占以太坊市值的 2.94%）。在立法方面，《21 世纪金融创新和技术法案》（FIT21）明确了加密货币分类且对 SAB 121 的否决保留了当前的加密托管会计准则。特朗普政府的创新友好政策包括

任命保罗·阿特金斯（Paul Atkins）等加密货币倡导者担任 SEC 主席，表明对该行业的大力支持。

- 加拿大：加拿大继续完善其加密货币监管框架，强调对加密货币交易所和服务提供商的监管，确保其遵守反洗钱（AML）和了解客户（KYC）规定。加拿大证券管理机构（CSA）加强了对加密资产投资产品的监管，要求提供更高的透明度和投资者保护措施。

3.1.4.3 欧洲

- 俄罗斯：2024 年，俄罗斯加快了加密货币监管，以减轻西方制裁的影响，重点是利用数字资产进行国际贸易。总统弗拉基米尔·普京将加密货币挖矿合法化，并允许使用挖矿资产进行跨境交易，从而使俄罗斯得以绕过传统金融体系。当局还考虑使用稳定币（特别是与人民币或金砖国家货币挂钩的稳定币）进行跨境支付，并在央行监督下建立了两个加密货币交易所，以促进对外贸易。
- 欧盟：《加密资产市场（MiCA）》法案于 2024 年 12 月 30 日在欧盟范围内全面生效，标志着欧洲成为全球首个实施统一加密货币监管框架的地区。它对稳定币发行人制定了严格的要求，包括储备支持和严格的运营标准，同时加强了对消费者的保护。
- 英国：英国金融行为监管局（FCA）将在欧盟 MiCA 框架的基础上，于 2026 年制定全面的加密监管制度。

3.1.4.4 中东和非洲

- 阿拉伯联合酋长国：阿联酋通过其虚拟资产监管局（VARA）巩固了其在加密货币监管领域的全球领先地位，并于 2024 年颁发了 13 个新许可证。它还推出了针对稳定币的许可，以适应不断变化的市场需求。
- 沙特阿拉伯：成为该地区增长最快的加密经济体，利用区块链创新并试行中央银行数字货币（CBDC）计划。
- 卡塔尔：推出了其首个数字资产监管框架，标志着向数字资产和稳定币的接受迈出了重大一步。

3.1.4.5 拉丁美洲

- 阿根廷：采用虚拟资产服务提供商（VASP）的合规框架，并计划实现包括比特币在内的货币自由流通。
- 巴西：推进其 CBDC (DREX) 试点阶段，重点关注现实世界资产（RWA）开发，以增强金融包容性。
- 萨尔瓦多：扩大其比特币法定货币政策，并与阿根廷合作开发跨境加密解决方案。

综上，由于加密货币本身的复杂性，监管政策成为了一个包含金融稳定、消费者保护以及反洗钱等多个层面的复杂讨论。不过可以肯定的是，随着区块链和加密货币技术的普及化，更多的政府和机构正在介入，监管政策的实施也正在转向更为具体和全球化的方向。

3.2 反洗钱数据

3.2.1 资金冻结数据

3.2.1.1 SlowMist 协助冻结

在 InMist 情报网络合作伙伴的大力支持下，2024 年度 SlowMist 协助客户、合作伙伴及公开被黑事件冻结资金共计超过 1.12 亿美元。

3.2.1.2 USDT 和 USDC 冻结

(https://dune.com/misttrack/2024)

2024 年 Tether 冻结的 USDT 金额为 540,195,442 美元；2024 年 Circle 冻结的 USDC 金额为 13,359,597 美元。

3.2.2 资金归还数据

2024 年发生了 410 起安全事件，在遭受攻击后能全部或部分收回损失资金的事件共有 24 起，根据已披露的数据，共计约 1.66 亿美元被返还，占总安全损失（约 20.13 亿美元）的 8.25%。

基于 Blast 的 Web3 游戏平台 Munchables 收回的 6,250 万美元占总收回资金的 37.65%，这起事件中也有朝鲜黑客的影子。Munchables 于 2024 年 3 月 27 日遭遇攻击，据悉，攻击者是伪装成开发人员的朝鲜黑客，通过长期潜伏获取了核心代码和敏感密钥。据链上侦探 ZachXBT 监测，Munchables 团队雇佣的四个的开发人员可能是同一个人，因其：互相推荐对方做这份工作；定期转账到相同的两个交易所存款地址；为彼此的钱包充值。此外，Aavegotchi 创始人 CoderDan 也于 X 平台表示：我们（@PixelcraftStuds）实际上在 2022 年试用聘用了这个人，让他从事一些游戏开发工作，但他当时就显得非常可疑，给人的感觉就像是朝鲜黑客。我们在一个月内就解雇了他。他还试图让我们雇佣他的一个“朋友”，而这个朋友很可能也是黑客。

所幸由于社区和团队的压力，Munchables 黑客最终归还了所有被盗资金。Blast 创始人 Pacman 发推表示：“Blast 核心贡献者已成功将 9,700 万美元资金转移至多签钱包。这背后付出了巨大的努力，但令人欣慰的是，前 Munchables 开发人员最终选择归还了所有资金，无需任何赎金。”

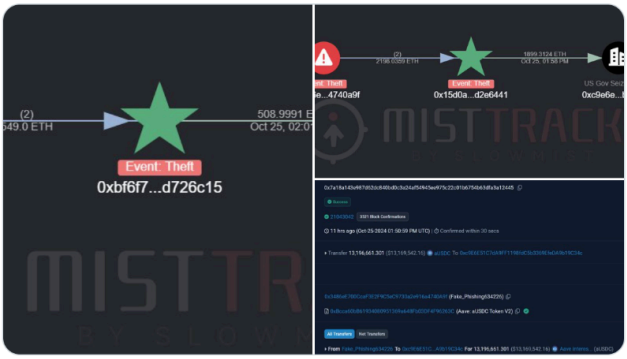
值得注意的是，黑客不仅将攻击目标瞄准 DeFi 项目方，交易所等资金体量大的对象，还盯上了政府钱包。2024 年 10 月 25 日，美国政府关联地址（0xc9E6…C34c）遭到攻击，约 2,000 万美元的加密货币被转移至黑客地址（0x3486e…0A9f），受攻击地址曾接收过从 9 个美国政府查封地址转来的资金，这些资金与 Bitfinex 黑客案件相关。不过，在 25 号当天，黑客便开始向美国政府返还了共计约 1,319 万枚 aUSDC 和 2,408 枚 ETH，总价值约 1,930 万美元。

MistTrack 🚨 ✅
@MistTrack_io

A little late but better late than never.

Most of the fund has now been returned to Uncle Sam.

翻译帖子



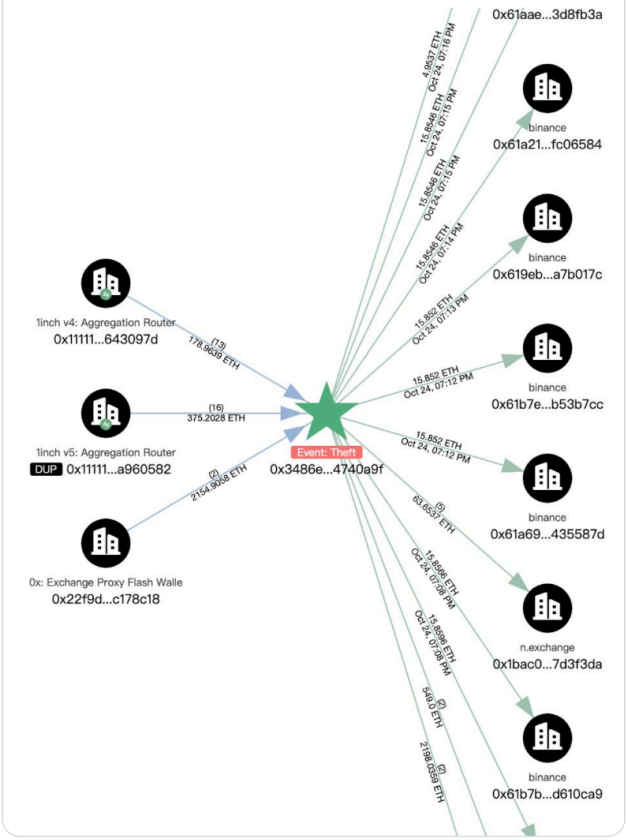
MistTrack 🚨 ✅ @MistTrack_io · 2024年10月25日

🚨MistTrack Alert🚨

Suspicious Outflow from U.S. Government-Controlled Wallet (0xc9E...34c):

~$20M was transferred to 0x3486ee700ccaf3e2f9c5ec9730a2e916a4740a...

显示更多



上午9:38 · 2024年10月26日 · **2,902** 查看

(https://x.com/MistTrack_io/status/1849989016755765702)

3.3 朝鲜黑客

2024 年，朝鲜黑客组织涉嫌多起网络盗窃案，导致超过数亿美元的加密货币被盗。以下是朝鲜黑客组织所犯下的重要事件列表（数据来源 SlowMist Hacked）：

Date	Target	Loss	Link
Sep, 2024	Linkedin Job Dev Scam	Unknown	Link
Apr-29, 2024	Rain.com	$14,800,000	Link
May-15, 2024	ALEX Labs	$4,300,000	Link
May-31, 2024	DMM Bitcoin	$305,000,000	Link
Jul-18, 2024	Wazirx	$230,000,000	Link
Sep-10, 2024	Indodax	$22,000,000	Link
Sep-19, 2024	BingX	$45,000,000	Link
Sep-25, 2024	Truflation	$5,600,000	Link
Oct-16, 2024	Radiant	$50,000,000	Link
	TOTAL	$676,700,000	

3.3.1 攻击手法

除了技术漏洞之外，许多攻击还通过社会工程学来获取初始访问权限或绕过安全措施。例如，DMM Bitcoin 和 Radiant 漏洞涉及攻击者在部署恶意软件之前通过冒充和网络钓鱼与目标建立信任。

- 疑似朝鲜黑客通过 Telegram 攻击区块链社区

一种常见的手法是针对区块链和天使投资社区的网络钓鱼活动。攻击者在 Telegram 上冒充知名投资公司的代表。他们主动发起对话并获得受害者的信任，使用 Calendly 等平台安排虚假会议，并以解决技术问题或共享敏感数据的幌子说服受害者下载恶意 App。

- 朝鲜 IT 工作者的威胁

朝鲜网络行动的另一个维度是将 IT 工作者部署到合法角色中。据谷歌威胁情报小组称，朝鲜特工以虚假借口渗透到 IT、区块链和自由职业平台。这些特工使用伪造的凭证和投资来获得职位，从而破坏敏感系统或发起更广泛的攻击。

- BeaRAT 恶意软件的新变种

研究人员发现了 BeaverTail 恶意软件的新变种，该变种归因于与朝鲜有关的攻击者，它通过伪装成合法的基于浏览器的视频通话应用程序来攻击 macOS 用户。这种复杂的恶意软件旨在从受感染的机器中窃取敏感信息，包括加密货币钱包数据和钥匙串文件。新版本的 BeaverTail 嵌入在模仿合法的 MiroTalk 视频通话服务的 macOS 磁盘映像中，该服务基于浏览器，无需下载应用程序。

3.3.2 洗钱手法

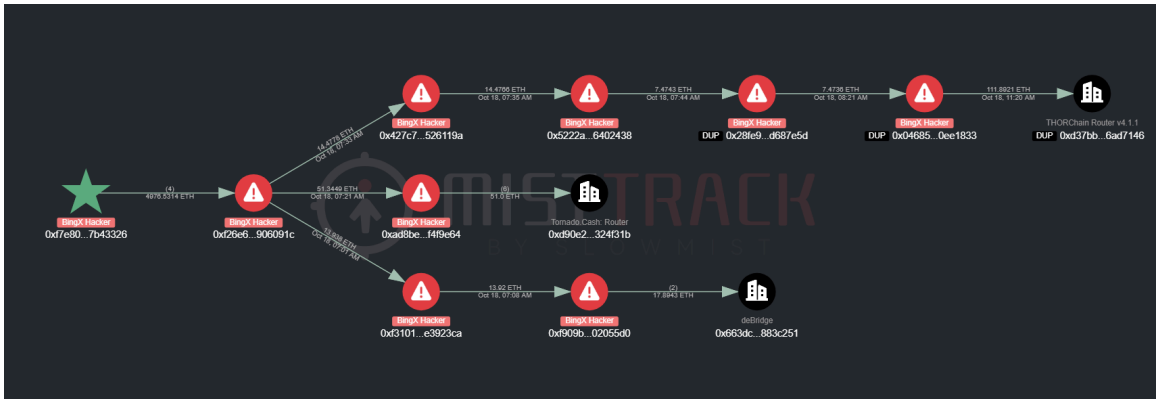
虽然各种区块链网络上的漏洞利用有所增加，但 Ethereum、Bitcoin 和 TRON 仍然是洗钱的主要网络，因为它们流动性高，生态系统支持广泛。此小节以 SlowMist 跟进的 BingX 事件为例，出于隐私原因，本调查重点介绍了这些方法的基础知识，而没有深入研究高级策略。

- BingX 事件中被盗资金的路径：

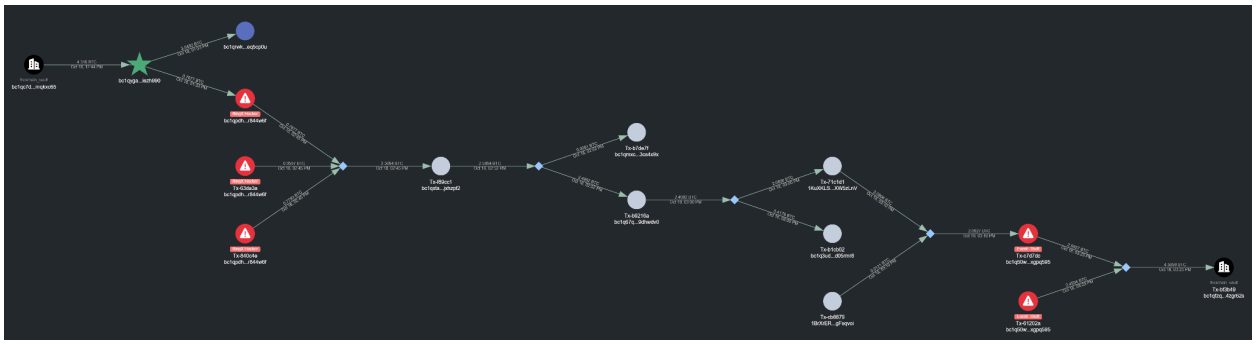
(1)初始转换：被盗资金首先被转移到犯罪者控制的钱包中，然后从山寨币转换为 ETH。

0x6df5ed7adb2...	20790945	2024-09-20 9:36:35	DODO: Fee Route	BingX Exploiter 1	0.89736009 ETH
0x123bdb8b36...	20790941	2024-09-20 9:35:47	DODO: Fee Route	BingX Exploiter 1	0.96968345 ETH
0x2f595308cfe...	20790914	2024-09-20 9:30:23	DODO: Fee Route	BingX Exploiter 1	0.75320577 ETH
0x5d6018d3f27...	20790906	2024-09-20 9:28:47	DODO: Fee Route	BingX Exploiter 1	1.04313494 ETH
0xf36f3700fb7...	20790900	2024-09-20 9:27:35	DODO: Fee Route	BingX Exploiter 1	1.21231438 ETH
0x584c67c441...	20790848	2024-09-20 9:17:11	DODO: Fee Route	BingX Exploiter 1	0.02071859 ETH
0xaf00bf8e464...	20790841	2024-09-20 9:15:47	DODO: Fee Route	BingX Exploiter 1	0.10075913 ETH
0xf4730979480...	20790834	2024-09-20 9:14:11	DODO: Fee Route	BingX Exploiter 1	0.9573791 ETH
0x38f750093fd...	20790818	2024-09-20 9:10:59	DODO: Fee Route	BingX Exploiter 1	0.68106979 ETH
0x3c3617469d...	20790809	2024-09-20 9:09:11	DODO: Fee Route	BingX Exploiter 1	0.72203465 ETH
0xed9139d971...	20790779	2024-09-20 9:03:11	DODO: Fee Route	BingX Exploiter 1	7.53144161 ETH
0xdb8c13f7f5b...	20790776	2024-09-20 9:02:35	DODO: Fee Route	BingX Exploiter 1	7.53473382 ETH
0xa6d55173df6...	20790773	2024-09-20 9:01:59	DODO: Fee Route	BingX Exploiter 1	0.91985954 ETH
0x1ffefd04cd2...	20790769	2024-09-20 9:01:11	DODO: Fee Route	BingX Exploiter 1	5.07314045 ETH
0x14e24dfcea9...	20790766	2024-09-20 9:00:35	DODO: Fee Route	BingX Exploiter 1	6.60528135 ETH

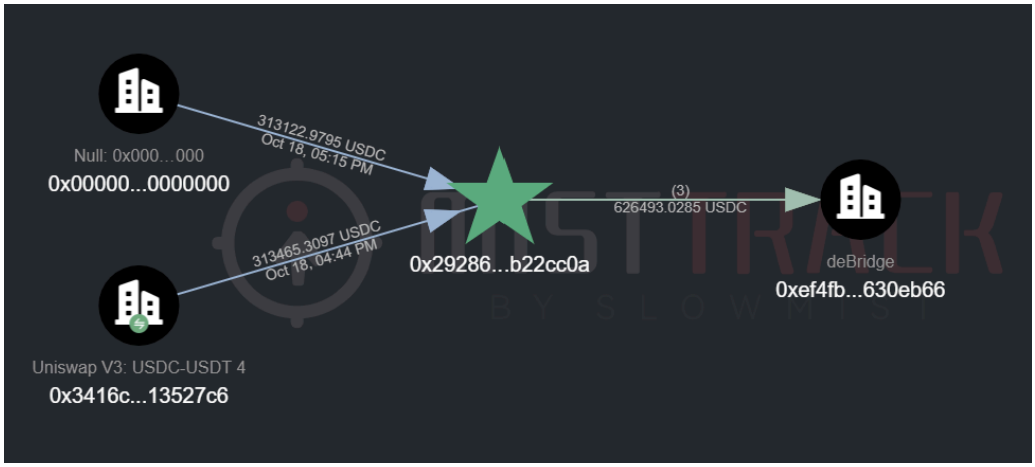
(2)拆分和存款:ETH 被分成多个钱包地址，并存入 Tornado Cash、Thorchain 和 Debridge 等平台。



(3)从 Bitcoin 网络提取资金后，资金被分散转移到多个地址，然后再次合并，并以 USDT 的形式跨链回 Ethereum 网络。



(4)最后，资金以 USDT 的形式通过 Debrige 跨链到 Solana 网络，随后黑客将其兑换为 USDC，然后存入 Debridge 并从 Solana 网络中提取。



值得注意的是，从 Solana 提款并不是追踪分析的结束。这种混淆资金路径的过程又重复了几次，最终资金被存入交易所或转移到 TRON 网络上的场外交易（OTC）市场。

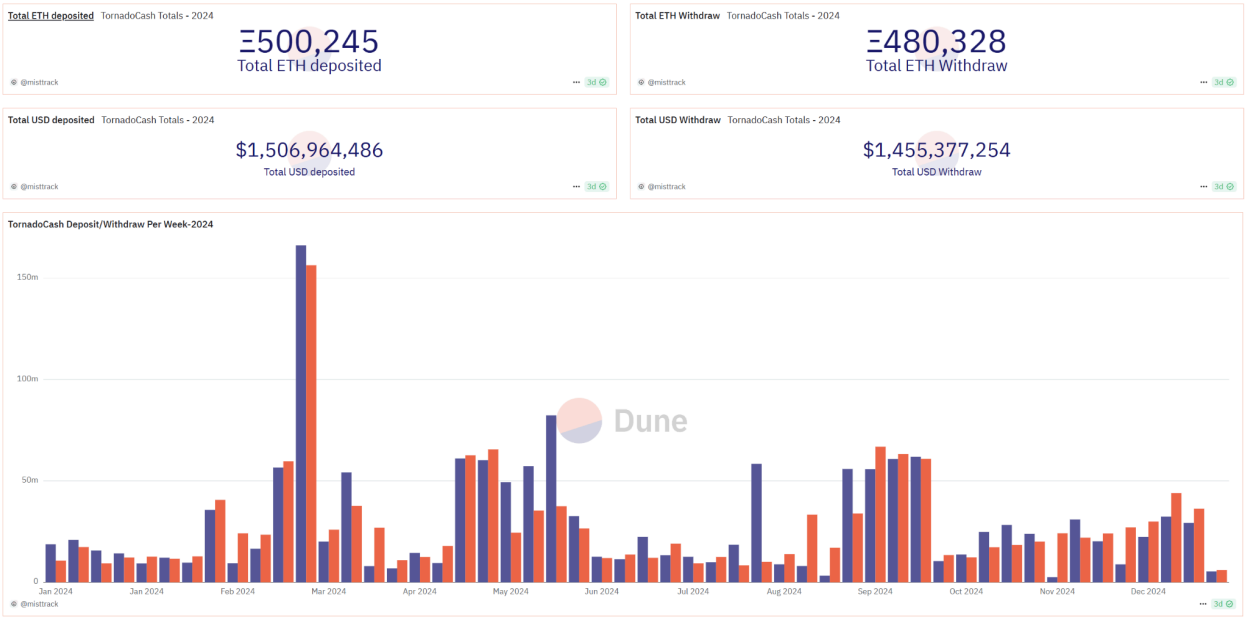
黑客为什么要跨多个网络桥接资金？主要原因是测试各个交易所的反洗钱（AML）系统。虽然大多数交易所都执行了解您的交易（KYT）协议，但自动化系统只能处理这么多。复杂的洗钱模式涉及多层和跨链转移，通常需要人工干预才能有效地提醒交易所。特别是混合器，增加了另一层复杂性。分离被盗资金通常需要大量的人工工作，并且难度会随着涉及的资金量而增加。使用的层级和网络越多，追踪和阻止被盗资产被清洗就越困难。这强调了对先进工具和专业知识的需求，以打击这些不断发展的洗钱技术。

虽然场外交易市场似乎是交易加密货币的便捷选择，但它们也伴随着巨大的风险。大多数场外交易市场并没有彻底审查被盗资金，参与这些市场的用户可能会无意中发现自己拥有非法资产。在这种情况下，资金通常会被冻结或扣押，用户成为受害者。

BingX 案例表明加密货币调查的复杂性日益增加。从被盗资金进入黑客钱包的那一刻起，它们被多次交换，从山寨币转移到 ETH，然后转移到 BTC，接着是 USDT（以太坊）、USDC（以太坊），最后是 USDC（Solana）。在此过程中，资金经过了超 12 个钱包地址，并跨四个区块链网络进行桥接。这条错综复杂的路径只是调查的一个分支，目前仍在进行中。随着越来越多的用户和公司采用加密货币，此类案件的频率和复杂性预计会增加。这凸显了采取强有力的预防措施的迫切必要性，例如先进的反洗钱系统和主动监控，以有效缓解这些挑战。

3.4 混币工具

3.4.1 Tornado Cash



(https://dune.com/misttrack/2024)

2024 年，用户共计存入 500,245 ETH（约 15.06 亿美元）到 Tornado.Cash，同比增长 47%；共计从 Tornado.Cash 提款 480,328 ETH（约 14.55 亿美元），同比增长 53%。

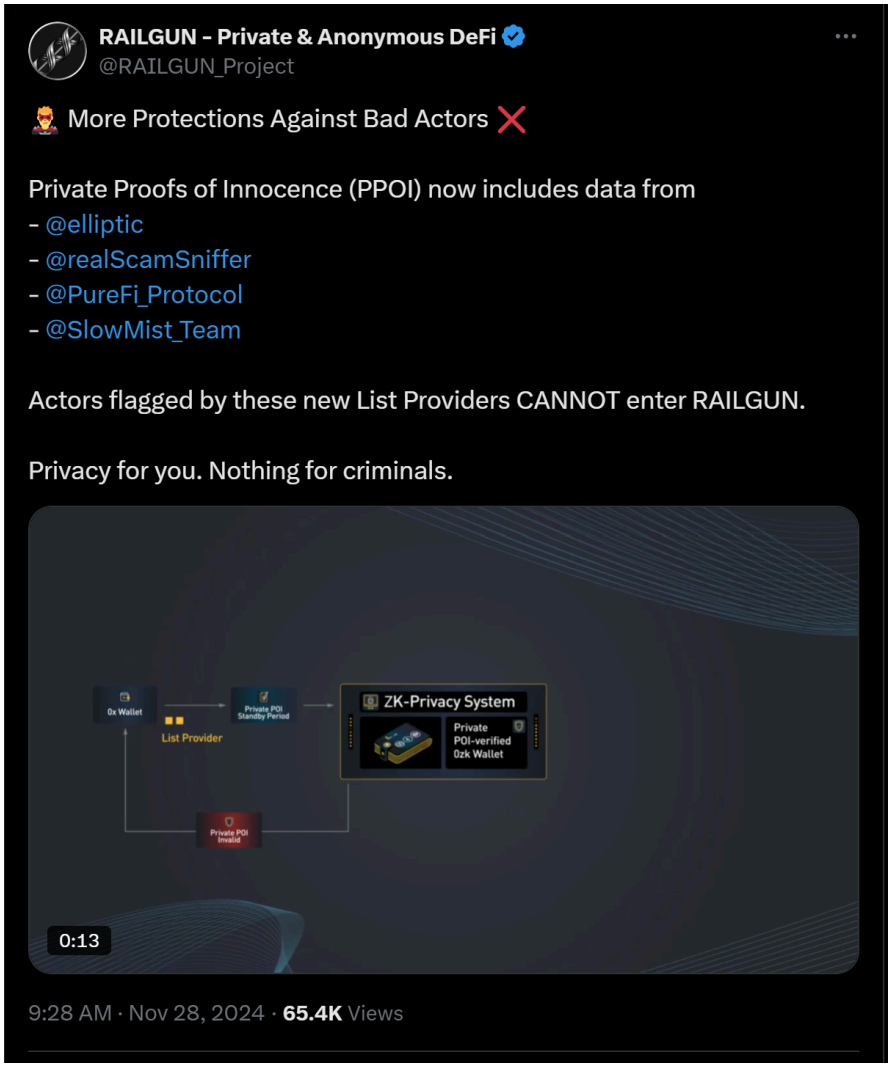
3.4.2 eXch

(https://dune.com/misttrack/2024)

2024 年，用户共计存入 214,918 ETH（约 6.33 亿美元）到 eXch，同比增长 355%；共计存入 173,106,107 ERC20 到 eXch，同比增长 579%。

2024 年 eXch 活动的增加主要是由于包括朝鲜附属实体在内的恶意行为者越来越多地使用它。与通常可以拆分用于大额交易的 Tornado Cash 不同，eXch 以不配合执法部门而闻名。eXch 提供了更高的匿名性和更低的资产追回风险，这些因素使 eXch 成为恶意行为者的首选平台，推动了 ETH 和 ERC20 代币存款的大幅增长。

3.4.3 Railgun



(https://x.com/RAILGUN_Project/status/1862141642989539397)

Railgun 已实施私人无罪证明（PPOI），利用零知识证明确保用户能够在不损害隐私的情况下验证其资金与非法活动无关。这项创新在隐私和合规性之间取得了关键的平衡，使恶意行为者更难利用该平台洗钱。

四、总结

2024 年，区块链行业在持续创新和变革的浪潮中面临新的机遇与挑战；种种安全事件和反洗钱动态为我们提供了深刻的警示，也促使我们更加重视行业规范与技术保障；通过对 2024 年区块链安全事件和洗钱案例的分析，我们希望能够唤起各方对行业安全的重视。

未来，随着监管框架逐步完善以及技术手段的不断升级，我们有理由相信，区块链行业将朝着更加安全、透明和合规的方向迈进。希望这份报告能为读者提供有价值的信息，帮助读者更全面地了解区块链行业的安全和反洗钱现状，也期待我们共同努力，为建设一个更加安全、稳定和可信的区块链生态贡献力量。

五、免责声明

本报告内容基于我们对区块链行业的理解、慢雾区块链被黑档案库 SlowMist Hacked 以及反洗钱追踪系统 MistTrack 的数据支持。但由于区块链的“匿名”特性，我们在此并不能保证所有数据的绝对准确性，也不能对其中的错误、疏漏或使用本报告引起的损失承担责任。同时，本报告不构成任何投资建议或其他分析的根据。本报告中若有疏漏和不足之处，欢迎大家批评指正。

六、关于 ScamSniffer

ScamSniffer 是一个专注于 Web3 反诈骗的安全平台，通过结合链下和链上监控数据，为用户提供实时反诈骗保护。ScamSniffer 的浏览器安全插件可以帮助用户识别钓鱼网站、可疑交易，为 Web3 用户提供全方位的安全保障。ScamSniffer 的安全解决方案已被 Binance、Bybit、OneKey、Phantom、TokenPocket 等钱包采用，每月保护数百万 Web3 用户免受钓鱼和欺诈威胁。致力于为下一个十亿用户打造更安全的 Web3 生态。

官网

https://www.scamsniffer.io/

X

https://x.com/realScamSniffer

Blog

https://drops.scamsniffer.io/

Email

b2b@scamsniffer.io

七、关于 SlowMist

慢雾(SlowMist) 是一家专注区块链生态安全的公司，成立于 2018 年 01 月，由一支拥有十多年一线网络安全攻防实战经验的团队创建，团队成员曾打造了拥有世界级影响力的安全工程。慢雾已经是国际化的区块链安全头部公司，主要通过"威胁发现到威胁防御一体化因地制宜的安全解决方案"服务了全球许多头部或知名的项目，已有商业客户上千家，客户分布在十几个主要国家与地区。

慢雾(SlowMist) 积极参与了区块链安全行标、国标及国际标准的推进工作，是国内首批进入工信部《2018 年中国区块链产业白皮书》的单位，是粤港澳大湾区"区块链与网络安全技术联合实验室"的三家成员单位之一，成立不到两年就获得「国家高新技术企业」认定。慢雾也是国家级数字文创规范治理生态矩阵首批协作发展伙伴。慢雾在新型加密货币犯罪调查方面有很多积累，研究成果被多个国际组织和政府部门引用，包括但不限于：联合国安理会、联合国毒品与犯罪问题办公室。

慢雾(SlowMist) 的安全解决方案包括：安全审计、威胁情报(BTI)、防御部署等服务并配套有加密货币反洗钱(AML)、假充值漏洞扫描、安全监测(MistEye)、被黑档案库(SlowMist Hacked)、智能合约防火墙(FireWall.X) 等 SaaS 型安全产品。基于成熟有效的安全服务及安全产品，慢雾联动国际顶级的安全公司，如 Akamai、BitDefender、RC²、天际友盟、IPIP 等及海内外加密货币知名项目方、司法鉴定、公安单位等，从威胁发现到威胁防御上提供了一体化因地制宜的安全解决方案。慢雾在行业内曾独立发现并公布数多起通用高风险的区块链安全漏洞，得到业界的广泛关注与认可。给区块链生态带来安全感是慢雾努力的方向。

慢雾安全解决方案

安全服务

智能合约安全审计

针对智能合约相关项目的源码及业务逻辑进行全方位的白盒安全审计

链安全审计

针对区块链资金安全、共识安全等关键模块进行全方位的安全审计

联盟链安全解决方案

从安全设计到安全审计再到安全监控及管理全周期进行联盟链安全保障

红队测试**(Red Teaming)**

超越渗透测试，针对人员、业务、办公等真实脆弱点进行攻击评估

安全监测

覆盖所有可能漏洞的动态安全监测体系，提供持续的、全方位的安全保障

区块链威胁情报

通过威胁情报整合，构建一个链上链下安全治理一体化的联合防御体系

防御部署

慢雾精选：因地制宜且体系化的防御方案、实施冷温热钱包安全加固等

MistTrack 追踪服务

数字资产不幸被盗，通过 MistTrack 追踪服务挽回一线希望

应急响应服务

旨在帮助 Web3 项目方快速且有效地应对安全事件和威胁

Hacking Time

聚焦区块链生态安全的闭门培训和主题峰会，打造硬核安全交流氛围

安全产品

慢雾 AML

阻拦洗币，规避风险

MistTrack

面向 C 端用户的加密货币追踪分析平台

被黑档案库

区块链攻击事件一网打尽

假充值漏洞扫描器

交易平台安全充提的保障利器

官网

https://slowmist.com

X

https://twitter.com/SlowMist_Team

Github

https://github.com/slowmist

Medium

https://slowmist.medium.com

Email

team@slowmist.com

微信公众号

Focusing on Blockchain Ecosystem Security