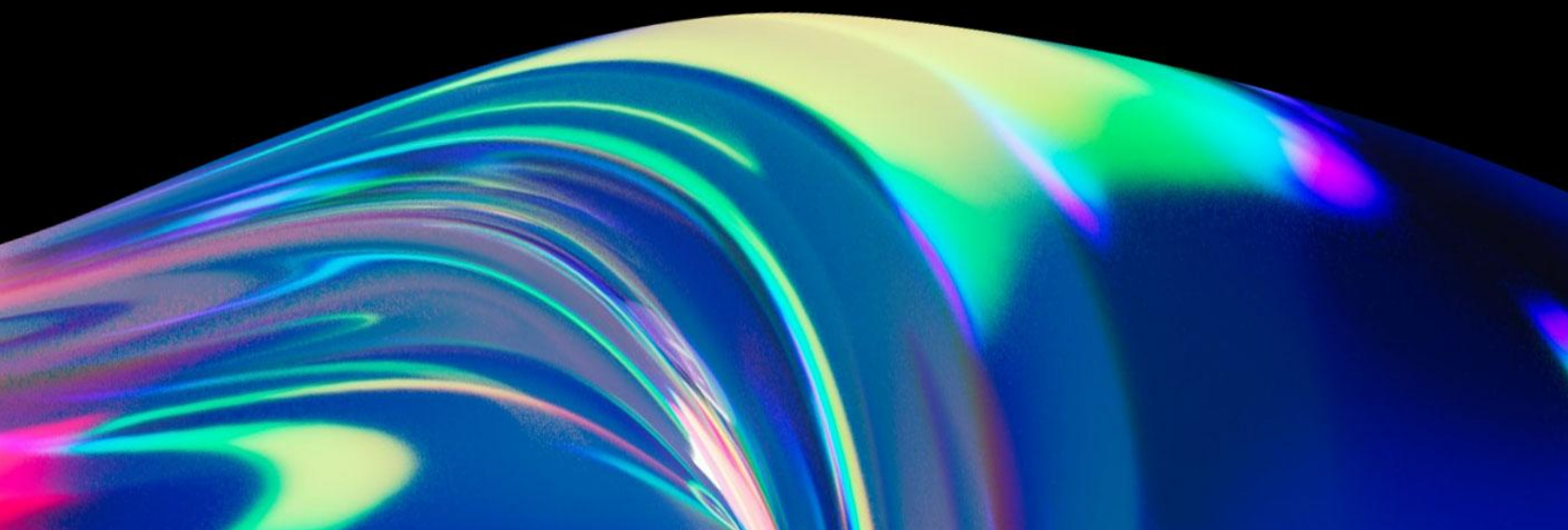
SLOWMIST 2023

区块链安全与反洗钱年度报告



目录

一、概述

2023 是动荡的一年。伴随着全球经济在宏观和地缘政治局势紧张的影响，包括但不限于世界各国央行为应对通胀而收紧货币政策、俄乌战争、中东冲突、恐怖分子以及病毒大流行，区块链行业也遭受着令人难以置信的动荡，同时还残留着 2022 年各种暴雷事件影响的痕迹。近一年以来，多家对加密货币友好的银行相继倒闭，如硅谷银行、Signature Bank 等，这些银行的突然缺席让许多加密资产客户陷入困境。再加上由朝鲜黑客 Lazarus Group 以及多个钓鱼团伙 Wallet Draines 引发的一系列安全攻击事件，进一步凸显了用户安全意识不足以及监管政策不完善的问题。从 2023 上半年的链上活动来看，朝鲜黑客 Lazarus Group 主要在清洗 2022 年盗窃的加密货币，其中包括 2022 年 6 月 23 日 Harmony 跨链桥遭受攻击损失的约 1 亿美元的资金。而在下半年，这个黑客团伙通过暗中地进行 APT 相关的攻击活动，直接导致了从 6 月 3 日开始的加密货币行业的 “黑暗 101 日”。在 “黑暗 101 日” 期间，共计有 5 个平台被盗，被盗金额超 3 亿美元，被盗对象多为中心化服务平台。此外，在过去一年，钓鱼活动也一直在持续增长，钓鱼团伙 Wallet Drainers 从大约 32 万名受害者中盗取了将近 2.95 亿美金的资产，其中于 3 月份出现的 Inferno Drainer 最活跃也获利最多，至少获利 8100 万美金。这也反映出加密资产具有金融和数字技术双重风险，正如由中国人民银行 12 月发布的《中国金融稳定报告（2023）》指出的那样：“区块链上与链下数据交互过程存在安全漏洞，容易被黑客攻击，导致市场操纵和资产丢失；资产匿名性和难以追回特征导致反洗钱、反恐怖融资风险等”。

2023 是创新化的一年。尽管 2023 年加密市场一直在低迷与狂欢中跌宕起伏，但我们也看到行业展现出了足够的韧性。根据 Alchemy 的报告，Web3 开发者活动在 2023 年第二季度快速增长，带动 EVM 链合约环比增长 302%，DeFi 用户数量环比增长 35%，而 NFT 用户减少了 33%，市场存在短期波动。据 DappRadar 报告，Web3 游戏项目在 2023 年第三季度获得 6 亿美元的收入，区块链上的游戏活动平均每天有 78 万个独立活跃钱包。除此之外，4 月 12 日以太坊上海升级标志着自 2022 年 9 月以太坊合并后的又一里程碑。还有 BRC-20 引发铭文赛道迅速发展；Solana 赛道东山再起，迸发出新的生机；比特币现货 ETF 备受关注等等，市场涌现出多种创新技术和概念。

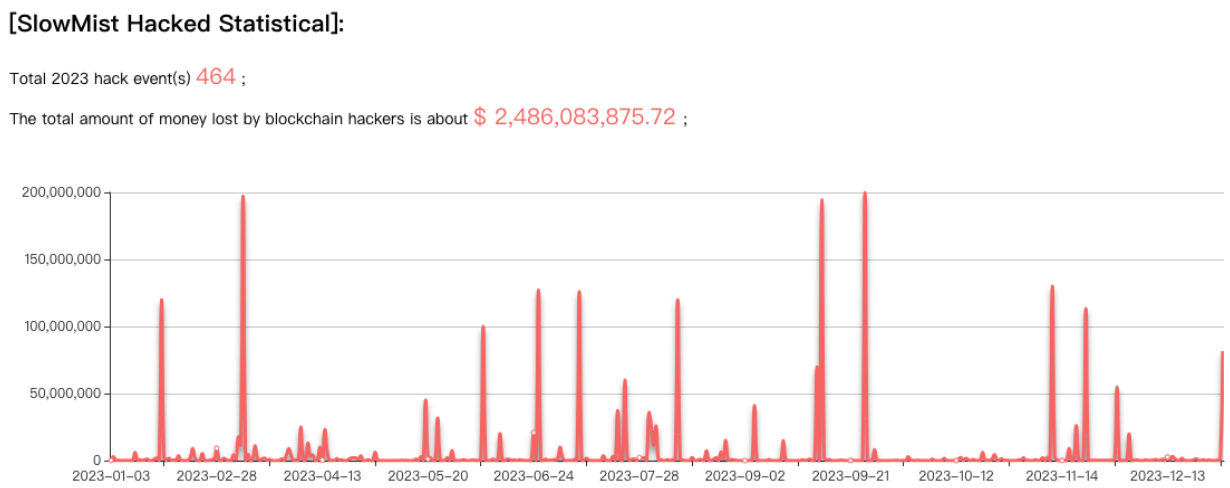
2023 是监管全球化的一年。随着区块链应用场景不断扩展，全球监管化浪潮正逐步发展。许多国家和地区对加密货币的态度日益清晰，例如，美国、中国内地加强了对加密货币的监管，以防止洗钱、欺诈和其他非法活动。随着加密货币的日益普及，越来越多的项目、平台开始采用合规的方式运营。这也使得原本处于灰色地带的加密货币行业，在很大程度上变得不再“灰暗”。同时，也有一些地区如中国香港，对加密货币表示出积极的态度，通过制定友好的政策来鼓励区块链和加密

货币的创新和发展。例如中国香港在 6 月份实行虚拟交易平台发牌制度，并表示“已准备好接受虚拟资产现货 ETF 的认可申请”，或成为亚洲首个允许虚拟资产现货 ETF 上市的市场。此外，许多国家的中央银行，如中国人民银行、美国联邦储备系统等，都在研究试验自己的数字货币，标志着数字资产正成为全球金融体系的一部分。无论如何，可以预见的是加密货币监管在未来仍会是一个热门且多变化的话题。

总的来说，2023 年区块链行业是振奋又动荡的一年。在这个背景下，本报告回顾了 2023 年区块链行业关键监管合规政策及动态，总结了 2023 年区块链安全事件及反洗钱态势，对部分洗钱工具进行了统计，并对典型安全事件及典型钓鱼骗局手法进行了详细剖析，提出了预防方案和措施建议。此外，我们还邀请了 Web3 反诈骗平台 Scam Sniffer 撰写关于钓鱼团伙 Wallet Drainers 的内容，同时我们对黑客团伙 Lazarus Group 的洗钱手法和获利资金进行了分析和统计。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。

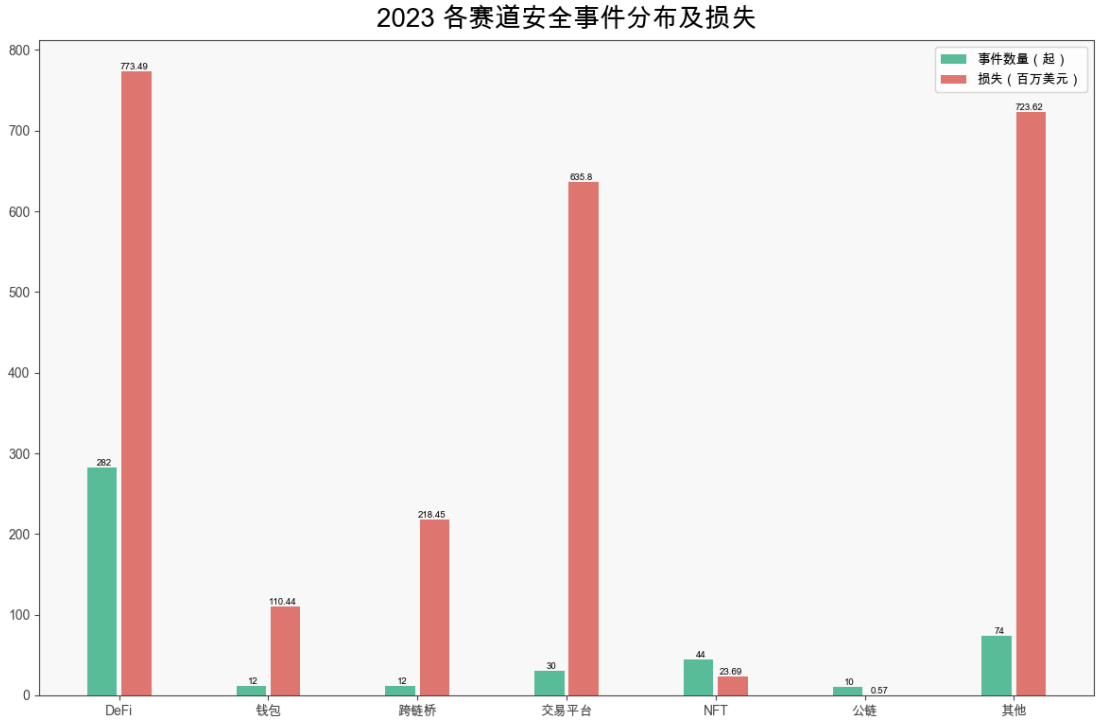
二、区块链安全态势

根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，2023 年安全事件共 464 件，损失高达 24.86 亿美元。对比 2022 年（共 303 件，损失约 37.77 亿美元），损失同比下降 34.2%。

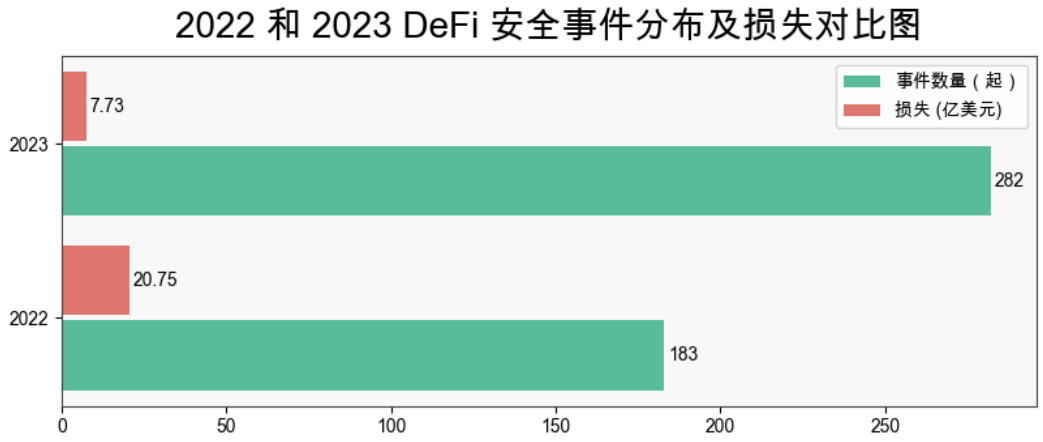


2.1 区块链安全事件总览

从项目赛道来看，DeFi 仍然是最常受到攻击的领域。2023 年 DeFi 安全事件共 282 件，占事件总数的 60.77%，损失高达 7.73 亿美元，对比 2022 年（共 183 件，损失约 20.75 亿美元），损失同比下降 62.73%。

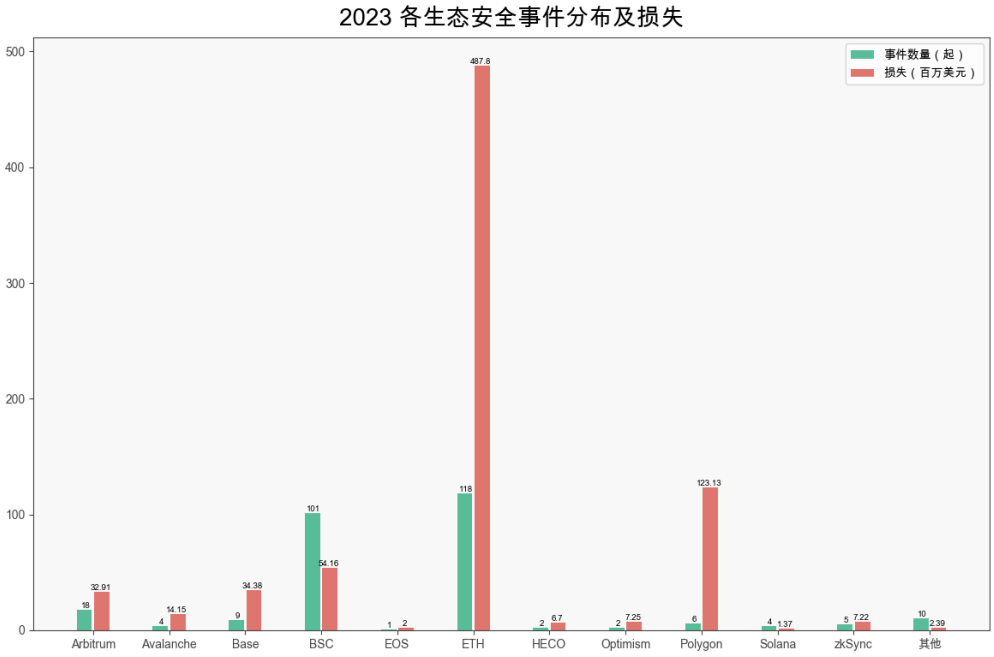


(2023 各赛道安全事件分布及损失)



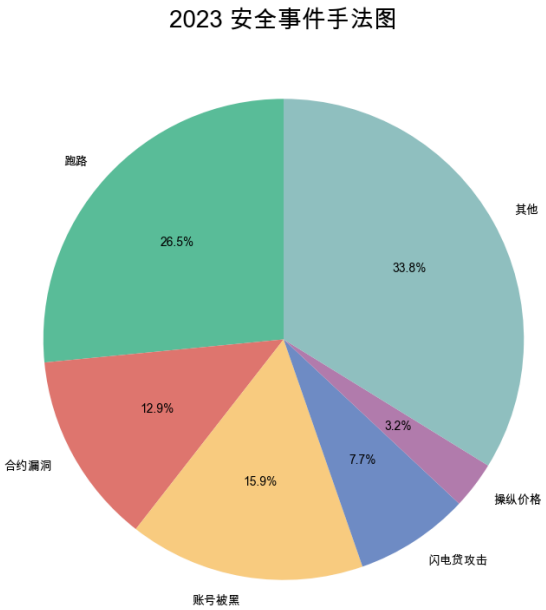
(2022 和 2023 DeFi 安全事件分布及损失对比图)

从生态来看，Ethereum 损失最高，达 4.87 亿美元。其次是 Polygon，达 1.23 亿美元。



（2023 各生态安全事件分布及损失）

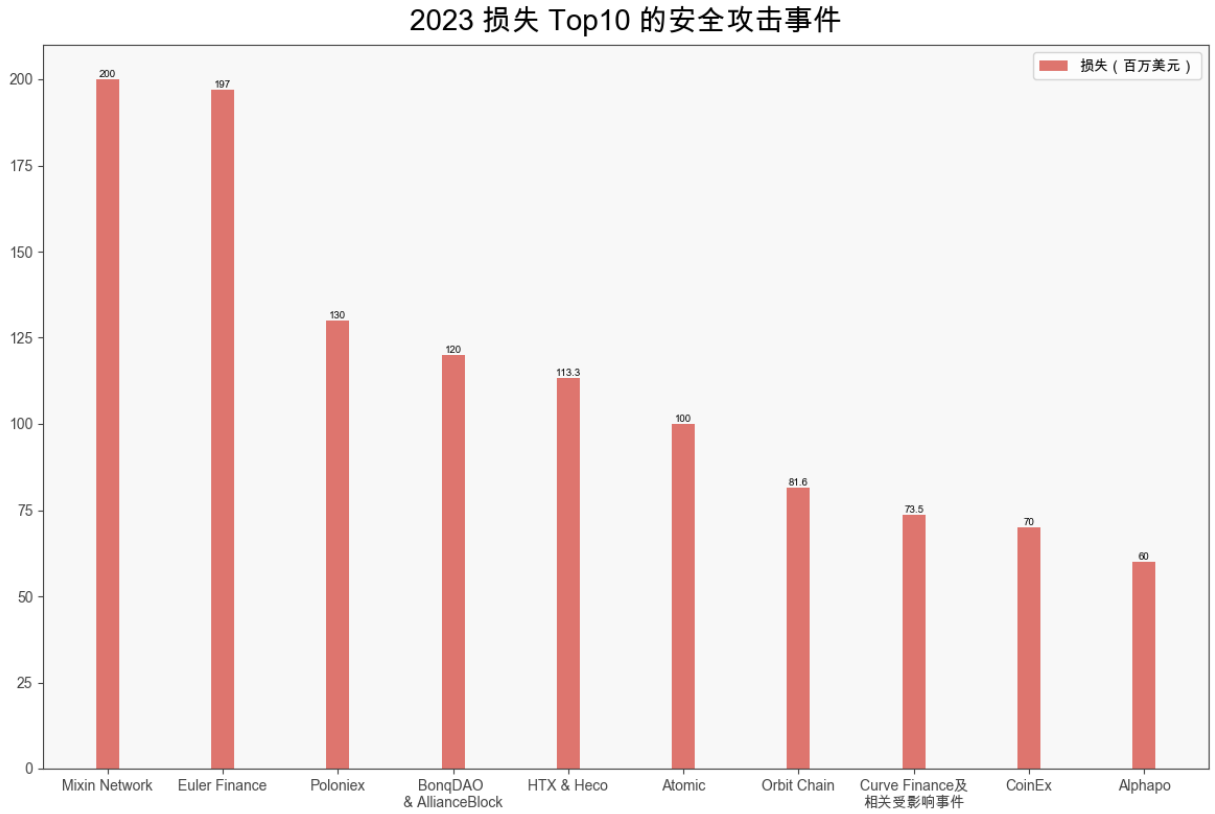
从事件原因来看，跑路事件最多，达 117 件，损失约 8300 万美元。其次为账号被黑导致的安全事件。



（2023 安全事件手法图 ）

2.2 典型攻击事件

此节选取了 2023 年损失 Top10 的安全事件。



（2023 损失 Top10 的安全攻击事件）

2.2.1 Mixin 数据库遭攻击损失约 2 亿美元

9 月 23 日，Mixin Network 云服务提供商数据库遭到攻击，导致主网部分资产丢失，涉及资金约 2 亿美元，是今年最大损失的攻击事件。随后，Mixin 官推称，已联系谷歌和慢雾团队协助调查。官方表示将最多赔付 50% 的损失，剩余部分以债券代币形式赔付，并用利润进行回购。

2.2.2 Euler Finance 损失约 1.97 亿美元后成功收回所有资金

3 月 13 日，DeFi 借贷协议 Euler Finance 遭到攻击，攻击者获利约 1.97 亿美元。据慢雾分析，攻击者的整个攻击流程主要是利用闪电贷的资金去存款，之后在两次叠加杠杆借贷后通过将资金直接捐赠给储备地址来触发清算逻辑，最后通过软清算自己来套利出之前剩余的所有资金。攻击的主要原因有两点：第一点是将资金捐赠给储备地址后没有检查自身是否处于爆仓状态，导致能直接

触发软清算的机制，第二点是由于高倍杠杆触发软清算逻辑时，yield 数值会增大，导致清算者只需转移一部分的负债到自身即可获得被清算人的大部分抵押资金，由于抵押资金的价值是大于负债的价值（负债因为软清算只转移了一部分），所以清算者可以成功通过自身的健康系数检查而提取获得的资金。4 月 4 日，Euler Labs 在推特上表示，经过成功协商，攻击者已归还 3 月 13 日从协议中盗取的所有资金。

2.2.3 Poloniex 交易所遭攻击，损失约 1.3 亿美元

11 月 10 日，Poloniex 交易所遭黑客攻击，造成的损失约为 1.3 亿美元。据慢雾安全团队表示，从攻击者这种迅速、专业的手法来看，猜测是典型的 APT 攻击，攻击者或为朝鲜黑客组织 Lazarus Group。孙宇晨表示："Poloniex 团队已成功识别并冻结了与黑客地址相关的部分资产。目前，损失在可控范围内，Poloniex 的营业收入可以弥补这些损失，将全额偿还受影响的资金。"

2.2.4 BonqDAO 的合约漏洞导致 BonqDAO 和 AllianceBlock 损失约 1.2 亿美元

2 月 2 日，非托管借贷平台 BonqDAO 和加密基础设施平台 AllianceBlock 因 BonqDAO 的智能合约漏洞而被黑客攻击，损失约 1.2 亿美元。其中黑客从 BonqDAO 的一个金库中移除了大约 1.14 亿 WALBT（1100 万美元）、AllianceBlock 的包装原生代币和 9800 万 BEUR 代币（1.08 亿美元）。据慢雾分析，此次攻击的根本原因在于攻击者利用预言机报价所需抵押物的成本远低于攻击获得利润从而通过恶意提交错误的价格操控市场并清算其他用户。此外 AllianceBlock 表示该事件与 BonqDAO 金库无关，没有智能合约被破坏，两个团队都致力于消除流动性，以减轻黑客将被盗代币转换为其他资产的行为。

2.2.5 HTX 和 Heco Bridge 遭攻击，损失超 1.133 亿美元

11 月 22 日，HTX（原 Huobi）及其相关的 Heco 跨链桥被黑客攻击，总金额达 1.133 亿美元。孙宇晨于推特回应了此次攻击事件："HTX 和 Heco 跨链桥遭受黑客攻击。 HTX 将全额补偿 HTX 热钱包损失。暂停充值和提现。请社区放心，HTX 所有资金安全。我们正在调查黑客攻击的具体原因。一旦我们完成调查并查明原因，我们将恢复服务。"

2.2.6 多名 Atomic Wallet 用户的资产被盗，损失超 1 亿美元

6 月 3 日，多名 Atomic Wallet 用户在社交媒体发文称自己的钱包资产被盗。Atomic 表示目前不到 1% 的月活用户受到影响/已上报。据慢雾分析，Atomic 钱包官方紧急下线 cloudflare 的下载站点与 sha256sum 验证站点，由此猜测可能是在历史版本下载这个环节上出现了安全问题。预计造成至少 1 亿美元的损失。

2.2.7 跨链桥协议 Orbit Chain 遭黑客攻击，损失 8160 万美元

12 月 31 日，跨链桥协议 Orbit Chain 遭黑客攻击，损失 8160 万美元。Orbit Chain 发推表示，团队已要求全球主要加密货币交易平台冻结被盗资产。

2.2.8 Curve Finance 事件造成多个项目累计损失 7350 万美元

7 月 30 日，Curve Finance 推特称，由于递归锁出现故障，许多使用 Vyper 0.2.15 的稳定币池 (alETH/msETH/pETH) 遭到攻击。crvUSD 合约和其它资金池不受影响。截至目前，Curve Finance 稳定币池黑客攻击事件已造成 Alchemix、JPEG'd、MeTRONomeDAO、deBridge、Ellipsis 和 CRV/ETH 池累计损失 7350 万美元。8 月 6 日，Alchemix 发推表示，Curve Finance 黑客已将 Alchemix 在 Curve 池中的资金全部归还。8 月 19 日，MeTRONomeDAO 表示名为 "c0ffeebabe" 的 MEV bot 已收回大部分被盗资金并归还给了 MeTRONome。

2.2.9 CoinEx 热钱包私钥泄露，损失超 7000 万美元

9 月 12 日，加密货币交易所 CoinEx 遭遇黑客攻击，初步确定事件原因为热钱包私钥泄露，造成的损失预计已达 7000 万美元，影响波及多个区块链。CoinEx 推特称，已识别并隔离与黑客攻击相关的可疑钱包地址，存取款服务已暂停。9 月 13 日，慢雾在分析过程中发现 CoinEx 黑客与 Stake.com 黑客、Alphapo 黑客存在关联，CoinEx 黑客或为朝鲜黑客团伙 Lazarus Group。

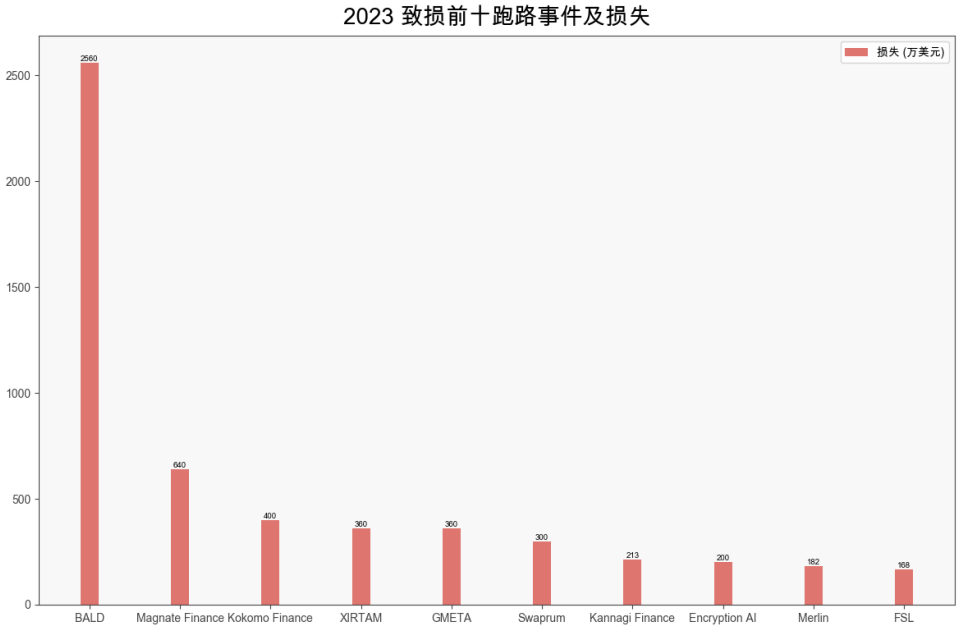
2.2.10 Alphapo 热钱包被盗，损失约 6000 万美元

7 月 23 日，加密货币支付服务商 Alphapo 热钱包被盗，损失约 6000 万美元，包括 Ethereum、TRON 和 BTC。被盗资金首先被在以太坊上交换为 ETH，然后跨链到 Avalanche 和 BTC 网络。Alphapo 处理许多博彩服务的支付，比如 HypeDrop、Bovada 和 Ignition。此次黑客攻击很可能是由 Lazarus Group 完成。

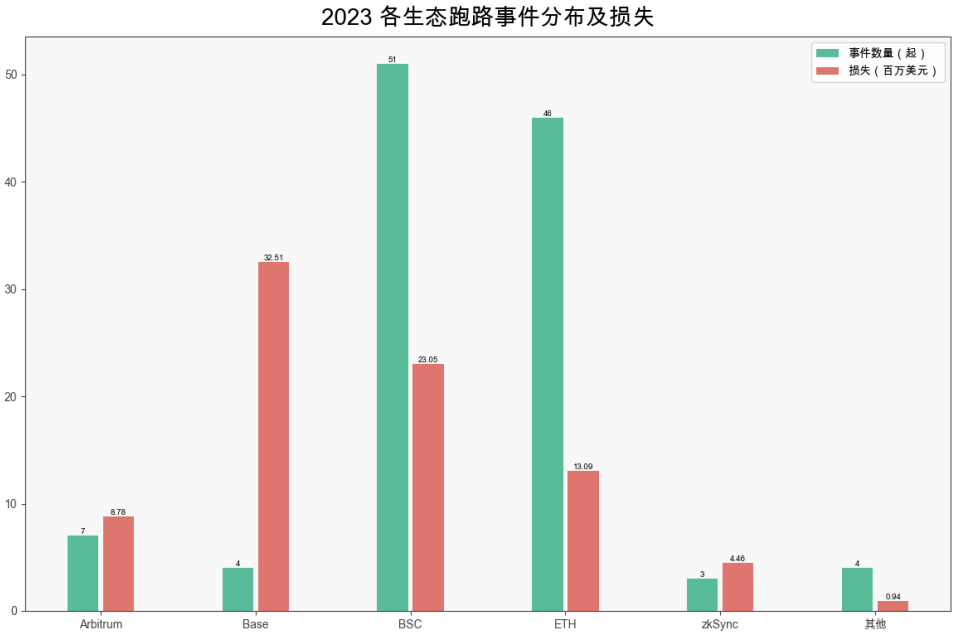
2.3 Rug Pull

Rug Pull 是一种骗局，通常是项目方主动作恶，以多种方式发生：比如项目方启动初始流动性，推高价格后撤回流动性；比如项目方先创建一个加密项目，通过营销手段吸引加密用户投资，并在合适的时机毫无征兆地卷走用户投资的资金，抛售加密资产，最终销声匿迹；比如推出一个网站，在吸引了数十万存款后关闭；比如项目方在项目中留下了后门代码。无论如何，任何一种类型的 Rug Pull 都会让投资者遭受损失。

根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，2023 年 Rug Pull 事件高达 117 起，导致损失约 8300 万美元。其中，Base 生态损失最高，达 3250 万美元。其次是 BSC 生态，达 2305 万美元。



（2023 致损前十跑路事件及损失）

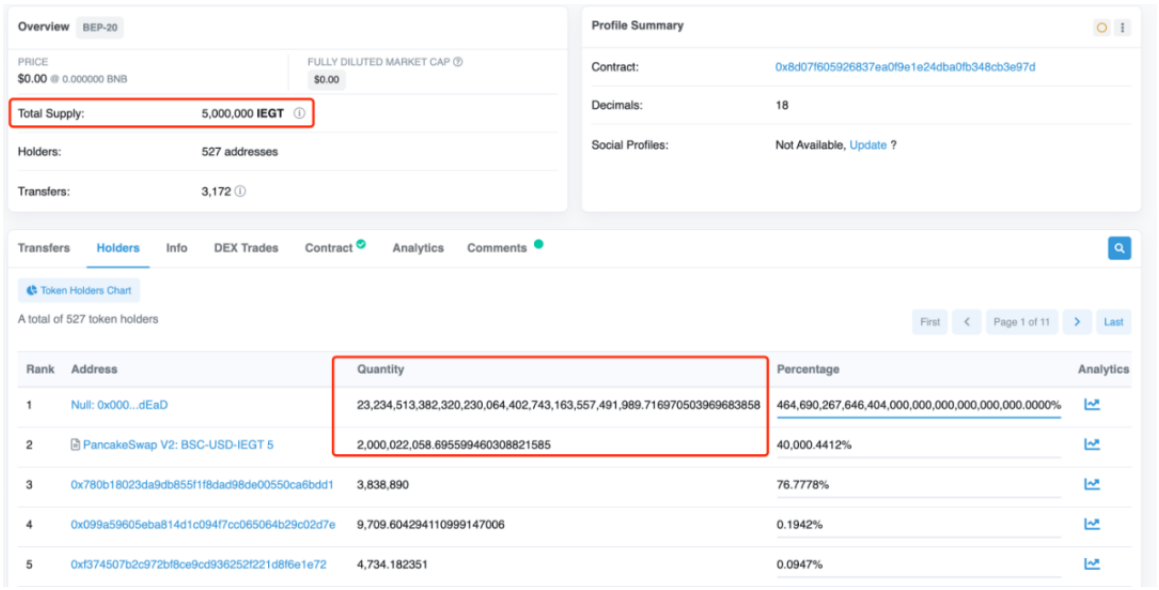


（2023 各生态跑路事件分布及损失）

2.3.1 案例

这里介绍一个由合约存储引起的极其隐蔽的 Rug Pull 案例：在项目代币没有任何增发记录的情况下，恶意用户使用未被记录的大量增发代币卷走了池子中的资金。

恶意代币 IEGT 在 BSC 上的部署地址是 0x8D07f605926837Ea0F9E1e24DbA0Fb348cb3E97D[1]。我们通过区块浏览器观察其 Holders，发现在 dead 与 pair 地址持有大量 IEGT 代币的情况下，合约记录的 totalSupply 仍为 5,000,000。进一步查看这些代币的来源可以发现，这些代币在 0x00002b9b0748d575CB21De3caE868Ed19a7B5B56 中只有转出记录而没有转入记录。

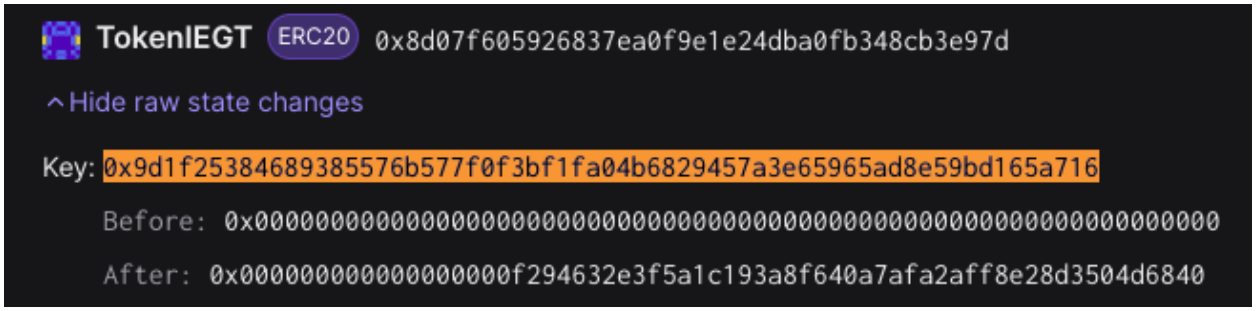


一般来说，进行代币增发最简单的方式就是实现一个直接增加指定地址余额的方法。在当前合约中是通过定义一个 _balances 映射，对用户的代币余额进行记录。但经过检查，合约中并未实现对指定地址的 _balances 进行修改的代码。

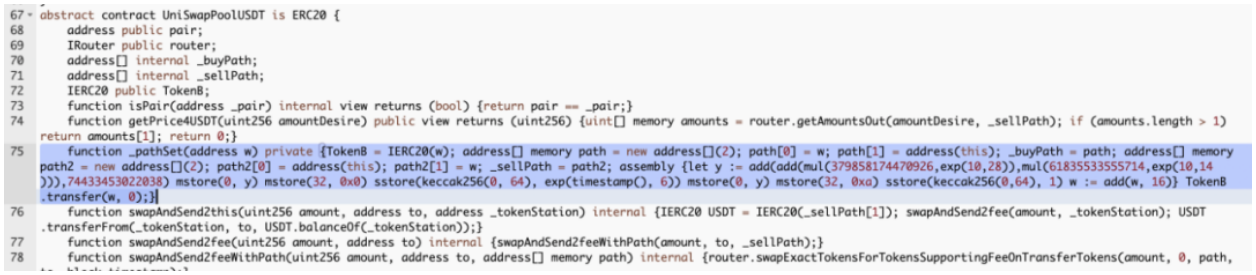
```
41 }
42 contract ERC20 is Context, IERC20, IERC20Metadata {
43     mapping(address => uint256) internal _balances;
44     mapping(address => mapping(address => uint256)) interna
```

通过分析 IEGT 合约的数据存储位置，我们可以发现其 _balances 参数所在位置为 slot0，那么用户的余额存储位置即为 keccak256(address,0) 。根据相关知识及公式计算，得到其余额存储位置

为 0x9d1f25384689385576b577f0f3bf1fa04b6829457a3e65965ad8e59bd165a716。随后查找此插槽数据变化，可以发现其在合约部署时已被修改为一个巨大的值。



因此，可以确定在 IEGT 合约部署初始化时，项目方就隐蔽地增发了大量的代币，为 Rug 做好准备。接下来我们分析其初始化函数，发现其在进行 _pathSet 操作时，通过内联汇编对合约存储进行了修改，并且未对代码进行格式化处理，以降低其可读性。



```
abstract contract UniSwapPoolUSDT is ERC20 {
    address public pair;
    IRouter public router;
    address[] internal _buyPath;
    address[] internal _sellPath;
    IERC20 public TokenB;
    function isPair(address _pair) internal view returns (bool) {return pair == _pair;}
    function getPrice4USDT(uint256 amountDesire) public view returns (uint256) {uint[] memory amounts = router.getAmountsOut(amountDesire, _sellPath); if (amounts.length > 1) return amounts[1]; return 0;}
    function _pathSet(address w) private {TokenB = IERC20(w); address[] memory path = new address[](2); path[0] = w; path[1] = address(this); _buyPath = path; address[] memory path2 = new address[](2); path2[0] = address(this); path2[1] = w; _sellPath = path2; assembly {let y := add(add(mul(379858174470926,exp(10,28)),mul(61835533555714,exp(10,14))),7443345302038) mstore(0, y) mstore(32, 0x0) sstore(keccak256(0, 64), exp(timestamp(), 6)) mstore(0, y) mstore(32, 0xa) sstore(keccak256(0,64), 1) w := add(w, 16)} TokenB.transfer(w, 0);}
    function swapAndSend2this(uint256 amount, address to, address _tokenStation) internal {IERC20 USDT = IERC20(_sellPath[1]); swapAndSend2fee(amount, _tokenStation); USDT.transferFrom(_tokenStation, to, USDT.balanceOf(_tokenStation));}
    function swapAndSend2fee(uint256 amount, address to) internal {swapAndSend2feeWithPath(amount, to, _sellPath);}
    function swapAndSend2feeWithPath(uint256 amount, address to, address[] memory path) internal {router.swapExactTokensForTokensSupportingFeeOnTransferTokens(amount, 0, path,
```

也就是说，项目方是在合约初始化时，通过内联汇编的方式修改了指定地址余额，隐蔽地增发了大量未被其他用户获悉的代币，导致用户在参与项目时被 Rug。

针对 Rug Pull，我们建议如下：

1）对一切保持怀疑，不要投资你无法承受损失的资金。

2）降低害怕错过机会和利益的心理，对项目背景做一定的研究。

3）在参与新项目时应着重分析其合约中是否存在可疑的代码，尽量不参与合约未开源且未经过审计的项目。

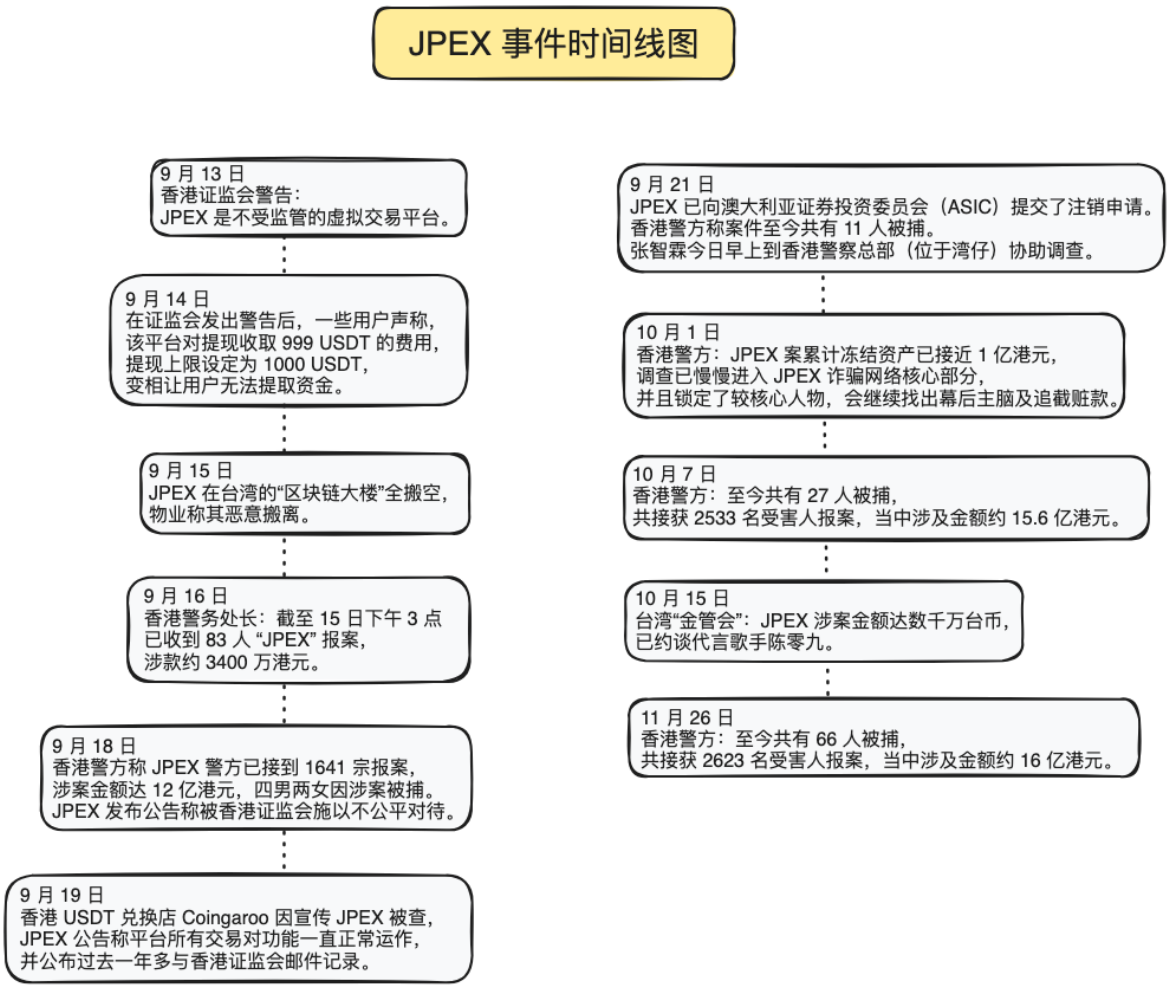
2.4 欺诈

近年来，加密货币市场逐渐变成骗子们实施欺诈的沃土。

骗子常常通过虚假账户冒充名人、交友杀猪盘、宣传虚假的交易平台、庞式骗局等进行诈骗，甚至随着技术的发展，骗子还会用人工智能软件来让骗局更具说服力。自 2021 年以来，四分之一的因欺诈而蒙受损失的人表示，欺诈是从社交媒体开始的。攻击者常常在社交媒体上制造假冒的角色、冒充名人等，通过承诺给予高收益赠品来骗取加密货币爱好者的信任或者发布钓鱼链接行骗。除了投资欺诈，较为突出的还有杀猪盘。骗子一开始会通过群聊加你，假装是认真交友，接着让你知道他正在投资某个项目收益颇高，慢慢地你就开始走进陷阱，直至发现无法提币。欺诈的关键点在于信任感的建立以及骗子始终强调赚钱，光鲜亮丽的人设后，却是黑暗的犯罪网络。

2.4.1 JPEX 事件

JPEX 事件是一个主要发生在香港的加密货币骗局。绿石数字资产平台(JPEX) 自称是一个成立于 2020 年、“面向全球”的数字资产加密交易平台，在香港和台湾均有业务。JPEX 在香港大量投放实体广告，包括办公楼与购物中心外墙、巴士车身、港铁公司(MTR) 车站等，演艺圈与网络红人亦为 JPEX 的重要宣传渠道。JPEX 与相关 OTC 店及网红合作大肆推广JPC（JPEX 平台币），声称可获近 20 厘极高年息，以“低风险高回报”招徕投资。2023 年 9 月，香港证监会点名指出 JPEX 存在多个可疑之处，其后有用户报称未能从平台提款并报警求助，香港警务处于 2023 年 9 月起发起“铁关行动”拘捕若干相关人士。截至 2023 年 12 月 18 日，香港警方累计拘捕 66 人，共接获 2,623 名受害者报案，涉款约 16 亿港元。据相关说法，JPEX 的暴雷可能成为香港历史上最大的金融欺诈案。

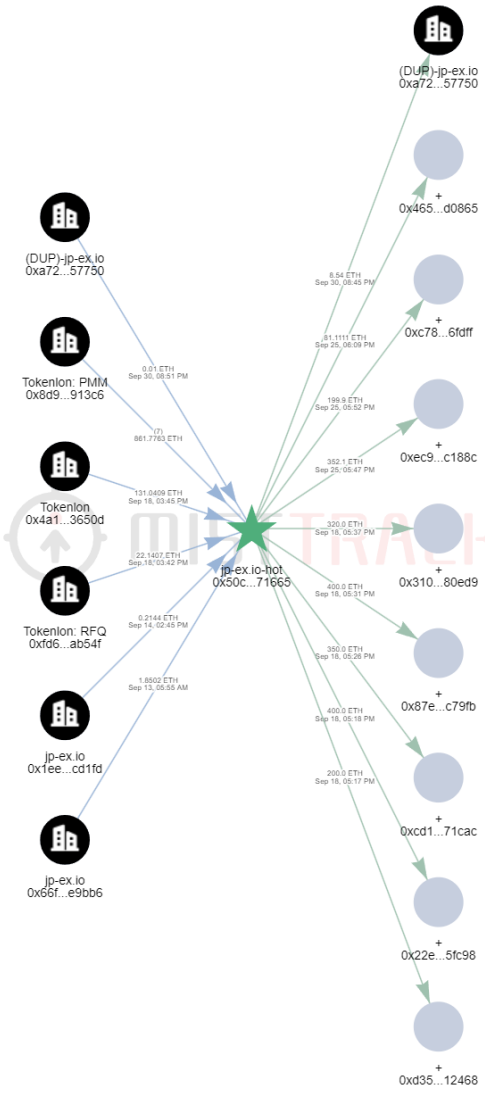


（JPEX 事件时间线图）

MistTrack 对 JPEX 部分地址进行分析，结果如下：

【Ethereum】

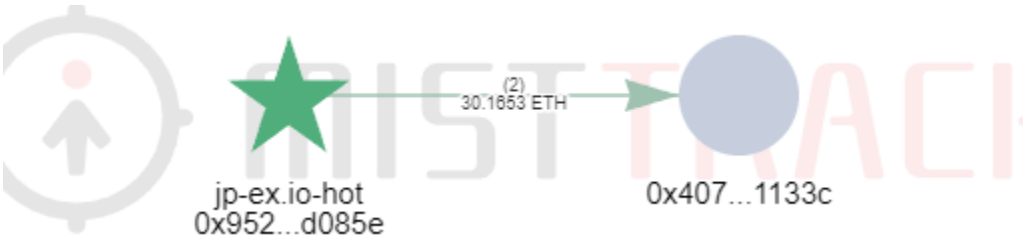
1) 自 9 月 18 日开始，JPEX 入金归集热钱包地址 0x50c85e5587d5611cf5cdfba23640bc18b3571665 将大部分 USDT 换为 ETH，分别在 9 月 18 日、25 日、30 日对 ETH 进行转移：9 月 18 日，1,670 ETH 被转到 5 个不同的地址，暂未转出；9 月 25 日，633.11 ETH 被转到 3 个不同的地址，暂未转出；9 月 30 日，8.54 ETH 被转到 JPEX Deposit 地址 0xa72ad701807e5902f458e1844d560128f3f57750。



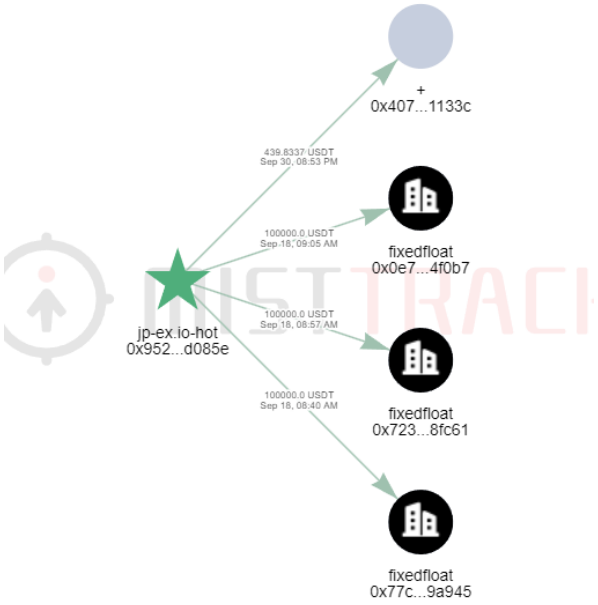
同时，该地址 0x50c8 于 9 月 30 日将多个 ERC20 代币（如：GALA, COMP, PEPE）转移到 JPEX Deposit 地址 0xa72Ad701807e5902F458e1844D560128F3F57750，暂未转出。

0xf9e566adab48318fe...	Transfer	2023-09-30 22:07:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	3,519.15663754	Ethereum Nam... (ENS)
0x227f330147896583...	Transfer	2023-09-30 20:59:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	166,044.612	Gala (GALA)
0xa99aad42b4124189...	Transfer	2023-09-30 20:57:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	24.694067	Aave Token (AAVE)
0xa206dd1c64aa7fba2...	Transfer	2023-09-30 20:57:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	12,644.3525	Constitution... (PEOPLE)
0x0dff81eb6e5692c6c...	Transfer	2023-09-30 20:56:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	797.5494361	Radicle (RAD)
0x7adba7a8c7dc8fc4a...	Transfer	2023-09-30 20:55:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	41.495846	Compound (COMP)
0x0cee4fe64f8fa5e54e...	Transfer	2023-09-30 20:54:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,693.1957831	Immutable X (IMX)
0x2e75ce08b8e53397...	Transfer	2023-09-30 20:54:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	25,866.01700836	JasmyCoin (JASMY)
0x74445e8af942a762b...	Transfer	2023-09-30 20:53:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	9,569.8701	Worldcoin (WLD)
0xbb1bab523ef952508...	Transfer	2023-09-30 20:52:59	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	2,542.54769808	1INCH Token (1INCH)
0x3e2bb1c746a2fa418...	Transfer	2023-09-30 20:52:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,864,554,872.95517191	Pepe (PEPE)
0x759c0e6dd75e5dd7...	Transfer	2023-09-30 20:46:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	25,954.87694052	EnjinCoin (ENJ)
0x6513711f8d711e796...	Transfer	2023-09-30 20:46:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	142,831.087263	chiliZ (CHZ)
0xff3771ed6626db057...	Transfer	2023-09-30 20:44:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	732.110076	USDC (USDC)
0x38653adf73c4b13eb...	Transfer	2023-09-30 20:43:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	0.99946	Binance Wrap... (BBTC)
0xbc60fb2871b857189...	Transfer	2023-09-30 20:43:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	10,847.921995509	SushiToken (SUSHI)
0x1cae3b440ead7960...	Transfer	2023-09-30 20:42:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	11,834,096,166.927952699	SHIBA INU (SHIB)
0x954ddf936528f12ee...	Transfer	2023-09-30 20:42:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	208,057.550554077	SAND (SAND)
0x05899e0c6e93c391...	Transfer	2023-09-30 20:41:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	37,557.038641353	FTT (FTX To...)
0x51abcd2fb4368593a...	Transfer	2023-09-30 20:40:59	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	69,722.303707104	Curve DAO To... (CRV)
0xba63dfdd8be5d75f5...	Transfer	2023-09-30 20:40:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	21,526.508069761	ApeCoin (APE)
0xed2a38b8fb5c37c29...	Transfer	2023-09-30 20:39:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	4,267.523732533	Axie Infinit... (AXS)
0xc867e14536136711...	Transfer	2023-09-30 20:38:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,099.612210237	Decentraland (MANA)
0xbe700ba62c36af2bc...	Transfer	2023-09-30 20:38:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	3,613.030552833	Uniswap (UNI)

2) JPEX **热钱包地址** 0x9528043b8fc2a68380f1583c389a94dcd50d085e **于** 9 **月** 30 **日将** 30.1653 ETH **转移到地址** 0x4071b1fbe9d83acef3fc9c780122e6c0e611133c，**暂未转出。**

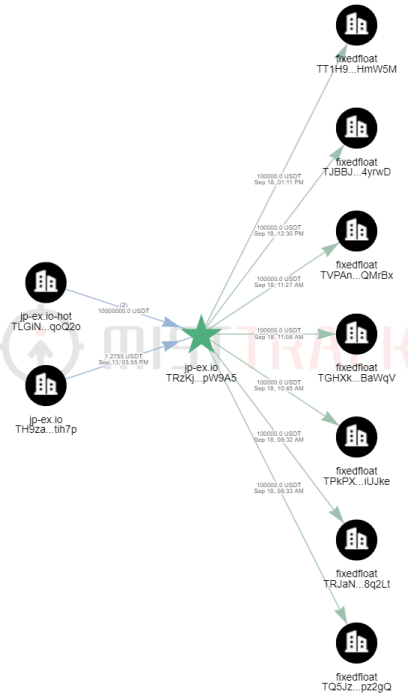


该热钱包地址 0x952 **于** 9 **月** 18 **日将** 300,000 USDT **转移到** 3 **个** FixedFloat **充币地址，并于** 9 **月** 30 **日将** 439.83 USDT **转移到地址** 0x4071b1fbe9d83acef3fc9c780122e6c0e611133c，**暂未转出。**



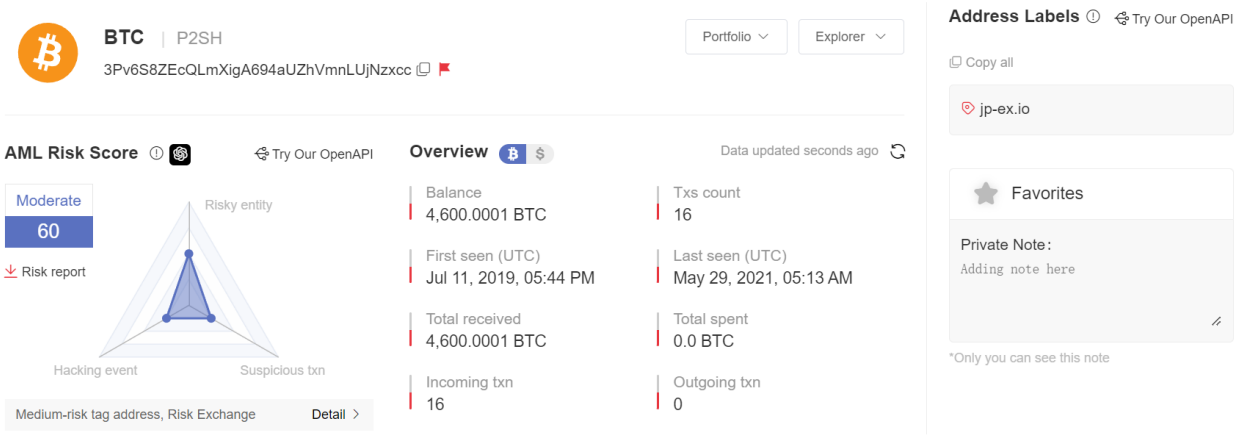
【TRON】

9 月 18 日，JPEX 冷钱包地址 TRzKj5d8Mk3LVEbLrEey7myHy59cSpW9A5 将 700,000 USDT 转移到 7 个 FixedFloat 充币地址：

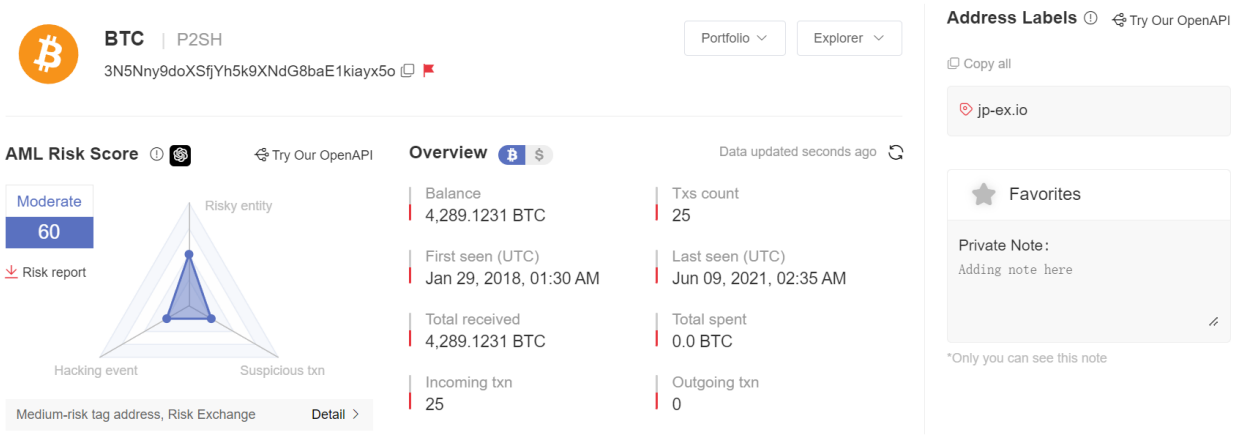


【BTC】

1）地址 3Pv6S8ZEcQLmXigA694aUZhVmnLUjNzxcc 上的 4,600 BTC 未转移：



2）地址 3N5Nny9doXSfjYh5k9XNdG8baE1kiayx5o 上的 4,289 BTC 未转移：



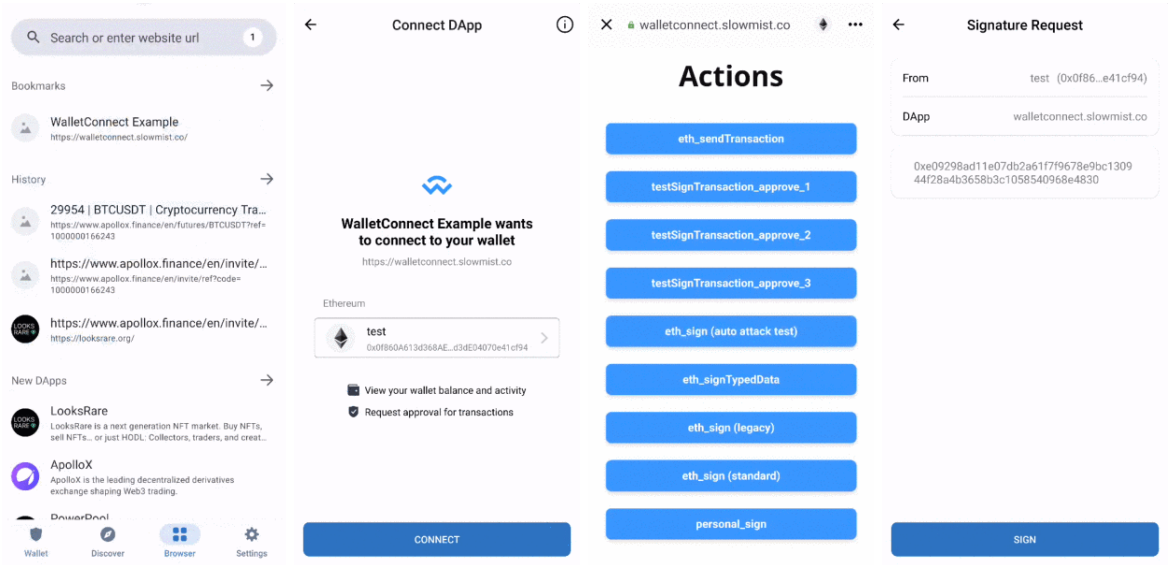
在事件发生后，香港特区政府和证监会第一时间采取了行动，这表现出香港相关方的积极性以及对此事件的重视。正如香港特区行政长官李家超所说："JPEX 事件反映监管及必需投资在受监管平台的重要性，以及个人对虚拟资产认识的重要性。"香港证监会行政总裁梁凤仪也表示："JPEX 事件更充分反映监管的重要，强调香港发展 Web3 生态的方向不会改变，而虚拟资产交易是 Web3 生态系统重要的组成部分，数码金融和虚拟资产活动采用的基础技术可以为金融市场带来裨益。"正如我们所看到的，尽管此次事件在短期给散户投资者、相关交易平台带来了挑战，但随着时间推移以及制度的完善，市场情绪会有所改善，监管机构对新兴金融业务的监管会更加严格、完善。

2.5 钓鱼/骗局手法

此节只选取我们于 2023 年披露的部分钓鱼/骗局手法。

2.5.1 WalletConnect 钓鱼风险

2023 年 1 月 30 日，慢雾安全团队发现 Web3 钱包上关于 WalletConnect 使用不当可能存在被钓鱼的安全风险问题。这个问题存在于使用移动端钱包 App 内置的 DApp Browser + WalletConnect 的场景下。部分 Web3 钱包在提供 WalletConnect 支持的时候，没有对 WalletConnect 的交易弹窗要在哪个区域弹出进行限制，因此会在钱包的任意界面弹出签名请求。当用户离开 DApp Browser 界面切换到钱包其他界面如示例中的 Wallet、Discover 等界面，由于钱包为了不影响用户体验和避免重复授权，此时 Wallet Connect 的连接是没有断开的，但是此时用户却可能因为恶意 DApp 突然发起的签名请求弹窗而误操作导致被钓鱼转移走资产。

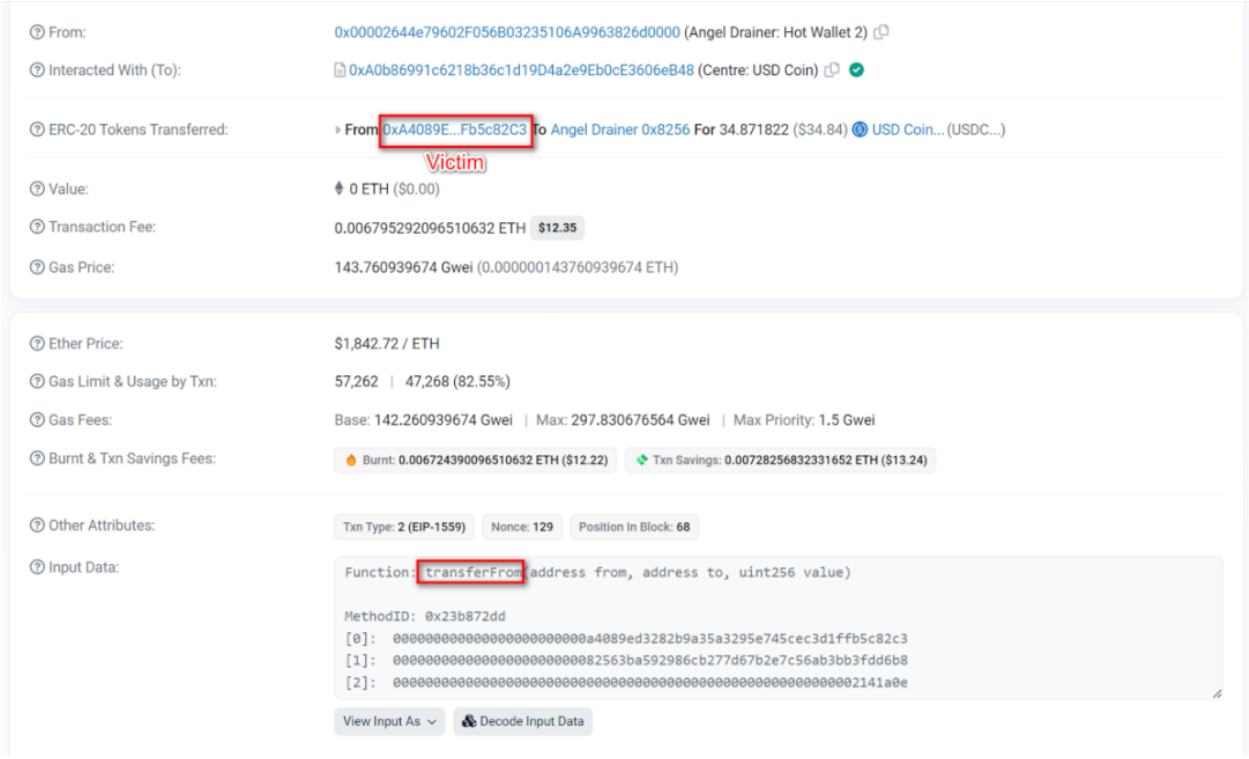


攻击者利用恶意 DApp 钓鱼网站引导用户使用 WalletConnect 与钓鱼页面连接后，然后定时不间断发送恶意的签名请求（如 eth_sign）。用户识别到 eth_sign 可能不安全拒绝签名后，由于 WalletConnect 采用 wss 的方式进行连接，如果用户没有及时关闭连接，钓鱼页面会不断的发起构造恶意的 eth_sign 签名弹窗请求，用户在使用钱包的时候有很大可能会错误的点击签署按钮，导致用户的资产被盗。对个人用户来说，风险主要在“域名、签名”两个核心点，WalletConnect 这种钓鱼方式早已被很多恶意网站用于钓鱼攻击，使用时务必保持警惕；对钱包项目方来说，首先是

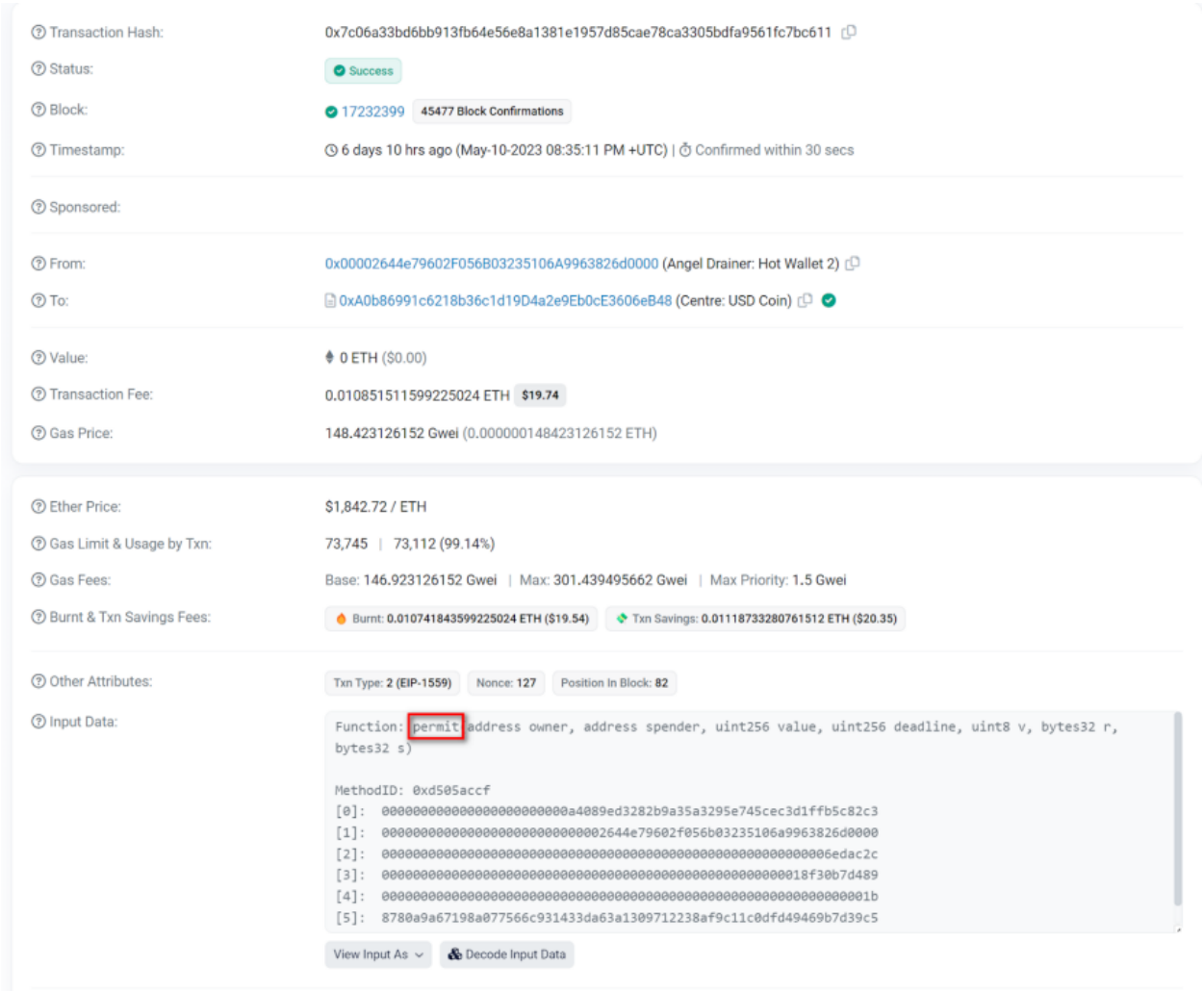
需要进行全面的安全审计，重点提升用户交互安全部分，加强所见即所签机制，减少用户被钓鱼风险。

2.5.2 Permit 签名钓鱼

例如，受害者被盗交易如下：



从这笔交易来看，合约调用者（0x00002...d0000）通过调用 TransferFrom 函数，将受害者地址（0xA4089...82C3）上的 34.87 USDC 转移到（0x8256...D6B8）。如果光看 transferFrom 函数，不难发现这个函数的作用是：允许第三方发起一笔交易，将相关数字资产从所有者账户转移到接收者账户。但分析合约调用者地址（0x00002...d0000），发现多了一笔 permit 操作，而这在受害者的交易记录中是没有的。



据官方介绍，permit 在 EIP-2612 被引入到 ERC20 的协议中，用户不用事先授权，就能通过附加一个授权签名（permit）与应用合约交互。具体来说，我们都知道在 ERC20 币种的交易中，A 可以调用 approve 函数来对 B 进行授权，即将 A 指定的代币授权给另一个账户操作，并且必须是这个账户的 owner 才可以调用 approve 函数。而 permit 函数的作用是，A 提前在链下对授权对象进行签名，得到的签名告知给 B，B 就可以拿着这个签名去调用 permit 来实现 A 的授权操作（获得 allowance 使用 transferFrom 进行转账），A 在不发送交易的情况下就能对指定代币进行转账，并且无论是不是这个账户的 owner 都可以执行 permit 进行授权操作。另外，Uniswap 已发布了新的 Token 授权标准 Permit2，随之也出现了针对 Permit2 签名的钓鱼。慢雾在此建议用户勿随意打开来历不明的网站进行操作，在与 DApp 交互时注意控制授权给合约的 Token 数量并认真检查签名内容，不定期使用授权工具如 RevokeCash 查看是否有异常授权，也可以使用针对 Uniswap Permit2 的授权管理工具进行查看，若有异常授权，请及时取消授权。

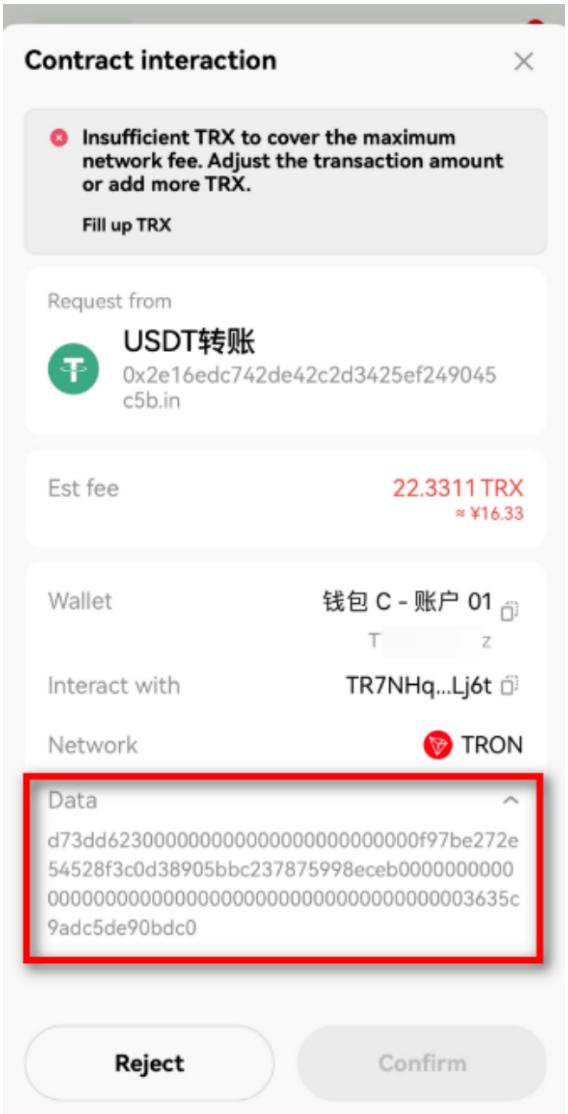
2.5.3 假 Skype App 钓鱼

网上充斥的假 App 的类型早已不限制于钱包和交易所类，社交软件如 Telegram，WhatsApp 和 Skype 也是重灾区。钓鱼团伙往往会对假 APP 做一层加壳处理以防止被分析。假 App 常见行为比如上传手机的文件图片，上传可能包含用户敏感信息的数据，而恶意替换网络传输内容，如修改钱包转账的目的地址这种手法在假 Telegram、假交易所 App 中已屡见不鲜。用户在下载使用 APP 时还是需要多方确认，认准官方下载渠道，避免下载到恶意 APP 造成资金损失。

2.5.4 伪装成转账地址的钓鱼网址

这种诈骗通常发生于聊天软件（如 Telegram）中，起始于场外出入金交易，在进行正式交易前，骗子以“确认受害者的地址是否存在风险”为由，让受害者先转账 0.1 USDT 看看地址的风险情况，接着给受害者发送了一个进行转账的“公链”地址，还特别提醒必须在钱包浏览器输入该公链地址才能进行转账。结果受害者在浏览器输入该“公链”地址后，发现账户所有的代币都被盗了。问题就出在这个“公链”地址 —— 0x2e16edc742de42c2d3425ef249045c5b.in。这是 TRON 上的转账，但这是 0x 开头的地址；其次，再仔细看，发现这并不是一个地址，而是一个末尾带着 .in 的网址。

通过钱包浏览器搜索该地址，发现该页面只能选择 TRON 网络。输入数额后，点击下一步，显示为合约交互 Contract interaction：



解码 Data 部分的数据，发现骗子诱骗用户签署 increaseApproval，一旦用户点击 Confirm，用户的代币就会被骗子通过 transferFrom 方法盗走。

Hash	Name
0xd73dd623	increaseApproval(address,uint256)

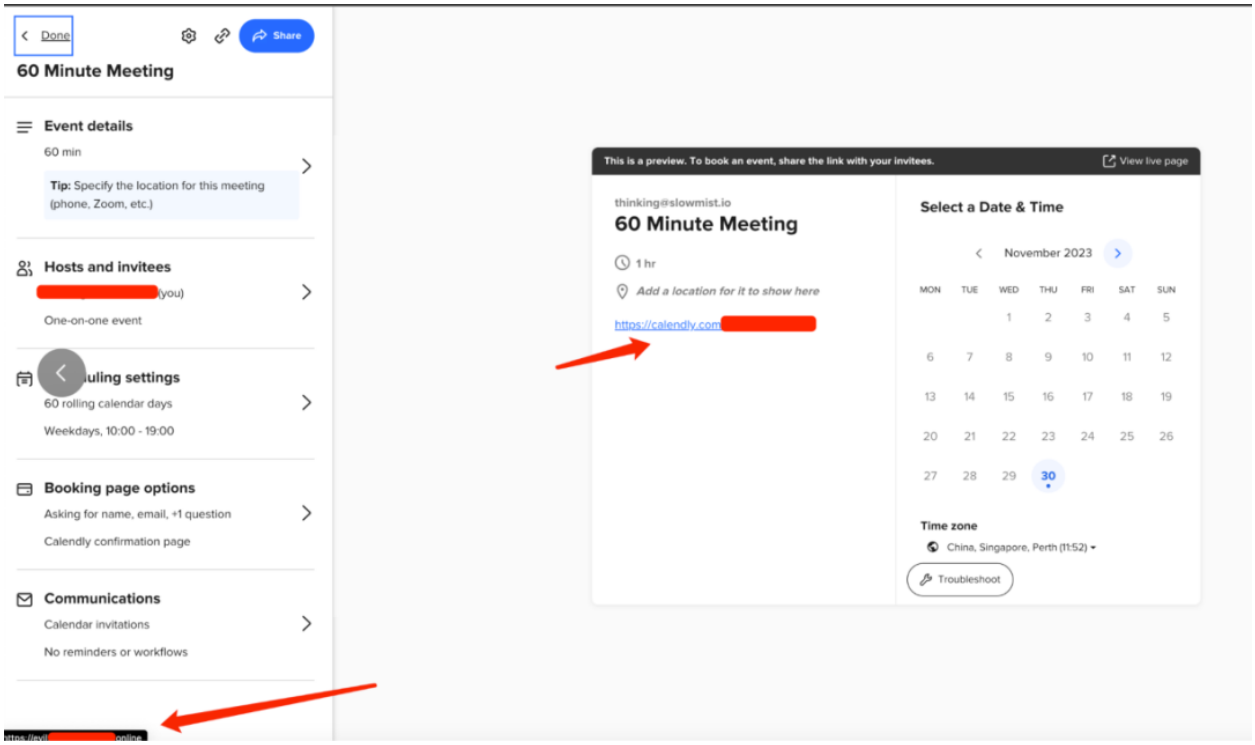
由于区块链技术是不可篡改的，链上操作是不可逆的，所以在进行任何操作前，请务必仔细核对地址。同时，在进行链上操作前，提前了解目标地址的风险情况是十分必要的，例如在 MistTrack 中输入目标地址并查看风险评分及恶意标签，一定程度上可以避免陷入资金损失的境地。

2.5.5 Telegram 定点欺诈攻击

朝鲜黑客冒充知名投资机构，对项目方进行欺诈钓鱼，主要有以下步骤：

1、挑选知名投资机构作为冒充对象，然后建立虚假的 Telegram 帐号：
2、寻找知名的 DeFi 项目方作为目标，以要投资他们为名，使用虚假帐号开始实施骗局
3、先对目标发起聊天以建立联系，骗取项目方的信任后便开始约会议，主要有两种攻击手法：

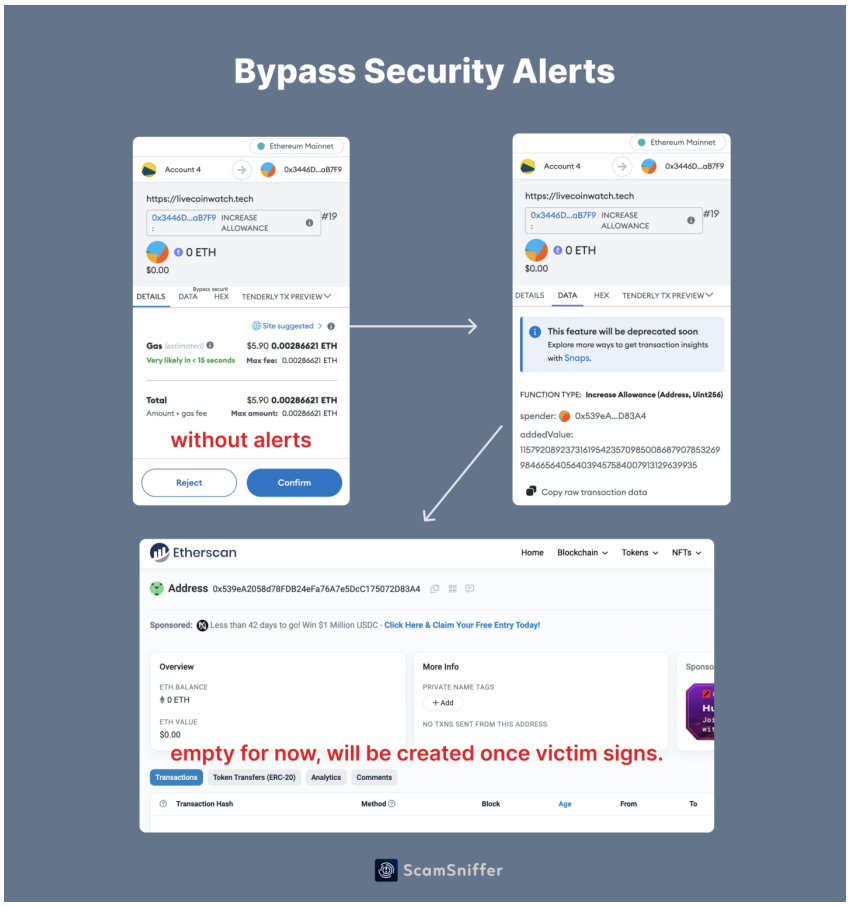
- 邀请项目方加入如 ***.group-meeting.team 之类的会议，假装询问对方是否有时间安排会面或详谈，并主动提供恶意会议链接。项目方点击链接后会看到地区访问限制，这时朝鲜黑客会接着诱使项目方下载并运行其提供的“修改定位”的恶意脚本。一旦项目方照做，那么他的电脑就会被朝鲜黑客控制，导致资金被盗取。
- 利用 Calendly 会议预定系统的“添加自定义链接”在事件页面的功能，在事件上插入恶意链接发起钓鱼攻击。由于 Calendly 与大多数项目方的日常工作背景很好地融合在一起，因此这些恶意链接不容易引起怀疑，项目方容易无意中点击恶意链接，下载并执行恶意代码，此时朝鲜黑客同样可以获取到项目方系统相关信息或权限。



鉴于此类诈骗行为仍在持续发生，建议 Web3 用户务必确保在添加好友时通过双重渠道确认对方的真实性，同时对 Telegram 开启双重身份验证(2FA)，随时注意交易安全，以免遭受资金损失。一旦不慎运行相关木马，请第一时间转移相关资金、断网杀毒，同时修改目标电脑上(包括浏览器里记录的)相关账号密码等信息。

2.5.6 Create2 钓鱼风险

攻击者利用 "create2" 功能预先计算将部署合约的地址，然后欺骗用户授予权限。由于这些空白地址可以绕过黑色地址标记和安全公司的安全监控，一旦用户授予权限，攻击者就会向该地址部署合约，并将用户的资产转出。据 Scam Sniffer 和慢雾共同披露，自 8 月以来，一个组织在地址中毒中使用了相同的技术，从 11 名受害者那里窃取了 300 万美元，其中一名受害者损失高达 160 万美元。



2.5.7 SIM 卡交换攻击

在加密货币领域，攻击者发起 SIM 卡交换攻击的目的是通过控制受害者的电话号码，以绕过双因素认证，从而获取对受害者的加密货币账户的访问权限。近年来，随着许多公司数据泄露，暗网上存在出售被盗的个人信息的交易。攻击者会从数据泄露事件中，或是通过网络钓鱼等方式，获取被害者的身份证等详细个人资料。随后，攻击者会借由这些信息冒充受害者，开始 SIM 卡交换攻击。

2023 年 10 月 5 日，链上侦探 ZachXBT 在表示，一名黑客在过去的 24 小时内通过对四名不同的 friend.tech 用户进行 SIM 卡交换攻击，获利 234 枚 ETH（约 385,000 美元）。

慢雾 CISO @23pds 在接受 Cointelegraph 采访时提到 “SIM Swap 因为攻击成本低，预计未来将愈演愈烈，而且随着 Web3 的普及并吸引更多人进入该行业，由于 SIM Swap 技术要求相对较低，SIM 卡交换攻击的可能性也随之增加。”

SIM 卡本身的安全性依赖于运营商的安全措施，容易受到社交工程等攻击方式的影响。因此，最好不要用基于 SIM 卡的认证方式。用户有必要为账户增加双因素认证以提高账户安全性，建议使用支持 TOTP 算法的身份验证器。

三、反洗钱态势

3.1 反洗钱及监管动态

在 2023 年，加密货币的世界持续经历动荡不安。在上一轮加密牛市期间，SBF 和 CZ 这两位行业巨头的每一个举动似乎都能对市场产生深远影响。然而在 11 月份，联邦陪审团以对 FTX 的倒闭导致的欺诈和共谋的指控，判定 SBF 有罪。仅仅几周后，币安接受了指控，支付了 43 亿美元的罚款，CZ 也同意了放弃对币安的控制权。随着加密资产行业在风雨飘摇的"寒冬"与熊市之间跌宕起伏，各国政府和国际组织对此也表现出更为谨慎的态度，各国对于加密货币的监管政策还在逐步形成中。

3.1.1 稳定币监管

根据 12 月 19 日发布的《普华永道2023年全球加密货币监管报告》，2023 年有多达 25 个国家/地区制定了稳定币立法或监管，这些国家包括奥地利、巴哈马、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、日本、卢森堡、葡萄牙、西班牙、瑞典、瑞士等。颁布稳定币法律的绝大多数国家/地区也已确保或执行所有其他审查的法规，包括加密货币监管框架、许可或注册以及金融行动工作组的旅行规则。根据报告分析，美国、英国和加拿大等国家尚未敲定稳定币的立法，也尚未制定加密货币的监管框架。数据显示，一些对加密货币友好的国家/地区，如新加坡和阿联酋，已经采用了除稳定币以外的所有加密货币相关法规。在被分析的国家/地区中，约 18% 或只有 8 个司法管辖区根本没有启动任何稳定币监管。这些国家/地区包括巴林、巴西、印度、中国台湾、土耳其和其他国家。23% 的受审查司法管辖区，包括澳大利亚、中国香港和新加坡，启动了稳定币监管进程，并积极采取稳定币法律。

3.1.2 SEC 执法行动

美国证券交易委员会（SEC）在 11 月公布了 2023 财年执法结果。报告显示，SEC 共提起 784 项执法行动，比 2022 年增加 3%。执法行动共产生了 49.49 亿美元的罚款，仅次于 2022 年的 64 亿美元，为历史第二高。SEC 表示，2023 财年是执法工作富有成果的一年。其所重点调查的案件涉及加密货币、网络安全、上市公司虚假陈述以及市场操纵等领域。

根据统计，以下是 SEC 在加密生态中对一些大交易所采取的执法行动：

1）SEC 根据联邦证券法对 NFT 发行人 Impact Theory 和 Stoner Cats 2 起诉，这标志着 SEC 监管目标的扩大。美国 SEC 在这两起案件中指控，所出售的 NFT 都是未注册证券。在指控发起后，两家公司都同意与 SEC 达成和解，分别支付约 610 万美元和 100 万美元。
2）交易平台 Kraken 以 3000 万美元与美国 SEC 达成和解，理由是 Kraken 的质押服务是一种未注册的证券，符合投资合同的定义。
3）SEC 与纳什维尔的加密服务公司 Linus Financial 达成和解协议，因该公司涉嫌未注册其零售加密货币借贷产品的发行和销售。
4）SEC 对 Coinbase 的诉讼中称，该交易所一直在经营一家未注册的证券交易所、一家未注册的经纪交易商和一家未注册的清算机构。Coinbase 随后提出了驳回诉讼的动议，预计将于24 年 1 月做出裁决。
5）SEC 声称 Ripple 的代币 XRP 是一种证券，该案的主审法官 Torres 的裁决明确表明 XRP 本身并不是一种证券。不久后另一个法官 Rakoff 否决了一项会影响到此事件的动议，目前裁决仍存在分歧，暂未判定。
6）由于比特币现货 ETF 的申请者众多，其与 SEC 反反复复博弈数年，但 SEC 从未批准通过。 据最新消息，SEC 对众多申请者做出答复的截止日期在 2024 年 1 月 5 日至 10 日。
7）6 月，SEC 对币安提起民事诉讼，指控币安为未经注册的交易所、非法向美国投资者供应和出售证券等。SEC 一直拒绝币安撤销诉讼的要求，SEC 与币安的这场“缠斗”仍在进行中。

3.1.3 反洗钱制裁

4 月 2 日，美国财政部制裁为朝鲜黑客团队 Lazarus Group 洗钱提供支持的三名朝鲜人。

5 月 25 日，币安协助美国执法部门扣押了 440 万美元并冻结了与朝鲜有组织犯罪有关的账户。

8 月 24 日，据美国财政部新闻稿，司法部对 Roman Semenov 和 Tornado Cash 的第二位联合创始人 Roman Storm 提起了起诉，后者今天被联邦调查局和国税局逮捕，指控串谋洗钱、串谋经营未经许可的资金传输业务以及串谋违反制裁规定。财政部称，即使知道 Lazarus 集团为了朝鲜的利益，通过其混币服务洗白了价值数亿美元的被盗虚拟货币，Tornado Cash 的创始人仍然继续开发和推广该服务，并且没有采取任何有意义的措施来减少其用于非法目的。

10 月 18 日，美国财政部对几个个人和实体实施了制裁，称这些个人和实体支持哈马斯的恐怖主义行动，其中包括一家加沙交易所和一家名为“Buy Cash Money and Money Transfer Company”的企业。美国财政部称，这家企业有着为恐怖主义集团提供资金支持的悠久历史，Buy Cash 此前曾

与以色列国家反恐融资局于 2021 年扣押的钱包相关联，被指控“为哈马斯提供资金、物资、技术、服务或支持”，该组织进行交易的资产中包括比特币。

10 月 31 日，日本政府在内阁会议上决定，冻结参与为巴勒斯坦武装政治派别哈马斯提供资金的9名哈马斯人员和1家虚拟货币交易公司的资产。

11 月 22 日，美国司法部宣布币安及赵长鹏在 40 亿美元决议中对联邦指控认罪。美国财政部在其与币安的和解公告中表示，金融犯罪执法网络 (FinCEN) 除对币安进行 34 亿美元民事罚款外，还将实施为期五年的监管，并要求做出重大合规承诺，包括确保币安完全退出美国。

11 月 29 日，美国财政部制裁了加密货币混合服务 Sinbad，原因是该服务支持与朝鲜黑客组织有关的交易。Sinbad 的网站也被美国联邦调查局、荷兰金融情报调查局、荷兰检察官办公室和芬兰国家调查局查封。Sinbad.io （Sinbad，辛巴达）是一个虚拟货币混合器，为 Lazarus Group 替朝鲜洗钱的主要工具。Sinbad 负责协助洗钱数百万美元的被盗虚拟货币，并且是 Lazarus Group 首选的混合服务器。Sinbad 在比特币区块链上运作，通过混淆其来源、目的地和交易对手，不加区别地促进非法交易。一些行业专家认为 Sinbad 是 Blender.io 混合器的另一个版本。

3.1.4 其他

- 中国

中国一直在加密货币方面持严格的政策。中国在 2021 年宣布全面禁止加密货币交易，并停止所有与加密货币相关的商业活动。11 月 13 日，中国人民银行金融稳定局发布专栏文章《有效防范化解金融风险，牢牢守住不发生系统性风险的底线》，文章指出，虚拟货币交易等领域整治工作基本完成，坚决遏制境内虚拟货币交易炒作。12 月，中国人民银行发布了《中国金融稳定报告（2023）》，对 2022 年中国金融体系的稳健性状况进行了全面评估。报告中对加密资产的风险进行了说明，并表示将继续整治虚拟货币交易炒作等非法金融活动。此外，报告总结了中国对加密资产的监管以及全球对加密资产监管的动态。报告称，“近年来，多国监管部门和国际组织已开始评估加密资产风险，出台监管政策和应对措施，总体上按照“相同业务、相同风险、相同监管”原则，对加密资产业务开展与其风险水平相称的监管，并尽可能减少监管数据缺口，降低监管碎片化，消除监管套利”。

尽管中国对加密货币极力遏制，但在规范监管的同时，中国持续鼓励对区块链和数字货币相关技术的探索和应用，并对新出现的问题做出及时的响应和调整。据数据显示，自 2022 年 1 月首次推出数字人民币以来，截至 6 月底，央行数字人民币的交易量约为 1.8 万亿元。12 月 2 日，中国人

民银行和阿联酋中央银行在香港续签了规模为 350 亿人民币/180 亿迪拉姆（49 亿美元）的货币互换协议，将双边货币互换协议延长五年，以促进金融和经济的联系。双方还签署了《关于加强央行数字货币合作的谅解备忘录》，进一步加强中央银行数字货币开发方面的技术合作。10 月 9 日，工业和信息化部、中央网信办、教育部、国家卫生健康委、中国人民银行、国务院国资委等六部门近日联合印发《算力基础设施高质量发展行动计划》，提出到 2025 年，计算力方面，算力规模超过 300 EFLOPS，智能算力占比达到 35%，东西部算力平衡协调发展。12 月，工信部在对全国政协十四届一次会议第 02969 号提案的答复上表示，除了此前表示将"制定符合我国国情的 Web3.0 发展战略文件"等完善顶层设计的措施外，还将加强 Web3.0 技术研究和监管，就 Web3.0 开展国际交流合作并加大技术宣传和推广。

- 中国香港

香港作为区域金融中心，正在将自己转变为加密货币中心。6 月 1 日，香港虚拟货币发牌制度正式开放，有意从事虚拟资产业务的平 台均可申请香港证监会牌照并受其监管。12 月 22 日，香港证监会官网公布《有关证监会认可的涉及虚拟资产的基金的通告》，取代 2022 年 10 月 31 日发出的《虚拟资产期货交易所买卖基金通函》。同时指出：对于被准许在持牌交易平台交易的虚拟资产（如比特币，以太坊），持牌机构可发行与管理对应的现货 ETF，并在持牌交易平台或受认可的财务机构，以实物和现金两种方式进行认购和赎回。另一方面，鉴于 JPEX 暴雷事件，香港证监会行政总裁表示，JPEX 事件充分反映监管的重要，香港发展 Web3 生态的方向不会改变，而虚拟资产交易是 Web3 生态系统重要的组成部分，数码金融和虚拟资产活动采用的基础技术可以为金融市场带来裨益。据了解，证监会与警务处成立了虚拟资产交易平台工作小组，分享虚拟资产交易平台可疑活动和违规行为的信息，合力将违法者绳之于法。12 月 22 日，香港证监会发布《有关中介人的虚拟资产相关活动的联合通函》与《有关证监会认可基金投资虚拟资产的通函》，并表示"准备好接受虚拟资产现货 ETF 的认可申请"。

- 美国

美国在对待加密货币方面的政策相对灵活。尽管监管政策不断更新，但未全面禁止加密货币的交易、购买和出售。同时，鉴于加密货币的影响和潜在风险，美国正在进一步增强监管力度，以确保金融体系的稳定和消费者的保护。

- 欧盟

欧盟对于加密货币的监管政策尚在讨论和修订中，尝试在保障金融安全和推动技术创新中找到平衡。值得一提的是，欧盟于 12 月宣布对俄罗斯公民领导的加密货币公司和项目实施新的制裁，加大对俄罗斯加密公司高管的打击力度。

- 日本

日本在对待加密货币方面相对开放，日本已经有完善的程序和法规以管控和支持加密货币市场。2023 年，日本国税厅于发布了有关 NFT 的税务上的一般处理文件，指南除了列举争对 NFT 征收所得税的案例外，也发布了征收消费税等情况的案例。另外，日本央行表示，将在 2026 年之前就发行 CBDC 做出最终决定。

- 韩国

韩国对加密货币有着明确的规定，包括注册要求、合规性审核和金融消费者保护。同时，韩国也在推动各类与区块链相关的创新项目。2023 年，韩国央行 (BOK) 公布了其零售央行数字货币 (CBDC) 试点计划的详细信息，表示将有 10 万名选定的韩国公民于 24 年第四季度加入试点。此外，韩国金融服务委员会 (Financial Services Commission, FSC) 于 12 月公布了关于《虚拟资产用户保护法》(Virtual Asset User Protection Act) 等法律的实施令和监管规定的立法预告。该法律旨在保护虚拟资产使用者和建立健全的虚拟资产市场交易秩序，规定了虚拟资产的定义、从虚拟资产中排除的对象，以及规定虚拟资产经营者必须安全保管和管理用户的存款和虚拟资产。鉴于此背景，韩国金融监督院宣布将新设"虚拟资产监管局"和"虚拟资产调查局"，为 24 年 7 月即将实施的《虚拟资产用户保护法》做准备。

- 新加坡

新加坡在加密货币方面的立法一直都比较前瞻，新加坡金融管理局(MAS)于 2023 年发布了一份关于加密消费者保护手册的咨询文件，之后将制定最终指导方针。新加坡一直支持并参与国际金融合作，例如新加坡金融管理局 (MAS) 成立了由日本金融厅 (FSA)、英国金融行为监管局 (FCA) 和瑞士金融市场监管局 (FINMA) 组成的政策制定者小组 Project Guardian，以推动跨境金融发展资产代币化方面的合作。同时，新加坡金融管理局(MAS)还于 2023 年上线了数字资产和去中心化金融（DeFi）服务试点。

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。

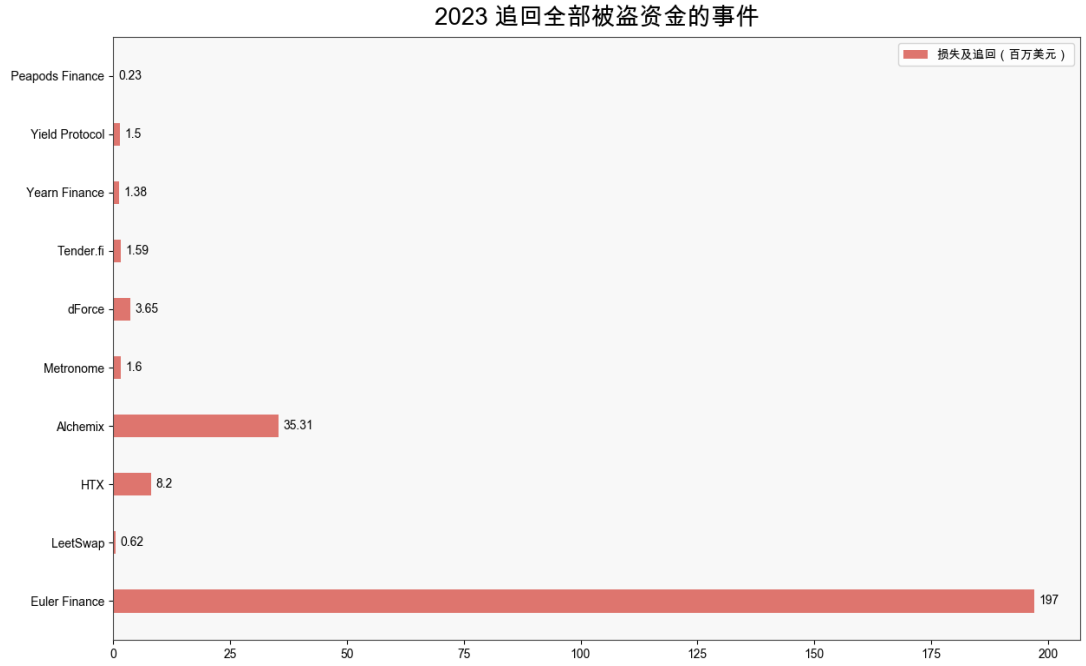
3.2 安全事件反洗钱

3.2.1 资金冻结数据

在 InMist 情报网络合作伙伴的大力支持下，2023 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 1250 万美元。

3.2.2 资金归还数据

2023 年遭受攻击后仍能全部或部分收回损失资金的事件共有 31 起。在这 31 起事件中，被盗资金总计约 3.84 亿美元，其中的 2.97 亿美元被返还，占被盗资金的 77%。在这 31 起事件中，有 10 个协议的资金被全部退回。



(2023 追回全部被盗资金的事件)

无论是给予赏金还是以合理谈判的方式拿回被盗资金，主要有两种传递消息的方式：一个是在项目方媒体平台发声，另一个则是攻击者与项目方通过链上留言进行沟通。讲到链上留言，就不得不提到本年度最“荒谬”且前所未有的一个链上谈判案例 —— KyberSwap Exploiter。

11 月 23 日攻击发生后，KyberSwap 团队与黑客通过链上消息进行谈判。KyberSwap 团队表示愿意支付 10% 白帽赏金，而 KyberSwap Exploiter 则就潜在的协商条款发表声明如下：

```
To ALL relevant and/or interested parties,

I thank you for your attention and patience during this uncertain time for Kyber (the protocol/DAO) as well as Kyber
(the company). Below I have delineated a treaty for us to agree to.


My demands are as follows:

* Complete executive control over Kyber (the company)

* Temporary full authority and ownership over the governance mechanism (KyberDAO) in order to enact legislative
changes. My current wallet address is fine for this.

* All documents and information related to company / protocol formation, structure, operation, revenues, profits,
expenses, assets, liabilities, investors, salaries, etc.

* Surrender of all Kyber (the company) assets. This is both On-chain and Off-chain assets. It includes but is not
limited to: shares, equity, tokens (KNC and non-KNC), partnerships, blogs, websites, servers, passwords, code, social
channels, any and all creative and intellectual property of Kyber.


Once my demands have been met, I will provide the following:

* Executives, you will be bought out of the company at a fair valuation. You will be wished well in your future
endeavors. You haven't done anything wrong. A small error was made, rounding in the wrong direction, it could have been
made by anyone. Simply bad luck.

* Employees, under the new regime your salary will be doubled. It is understandable that many current employees will
want to leave regardless. The employees who don't want to stay will be given a 12-month severance with full benefits
and assistance in finding a new career, no questions asked.

* Token Holders and Investors, under this treaty, your tokens will no longer be worthless. Is this not sweet enough?
I'll go further still. Under my management, Kyber will undergo a complete makeover. It will no longer be the 7th most
popular DEX, but rather, an entirely new cryptographic project.

* LPs, you will be gifted a rebate on your recent market-making activity. The rebate will be for 50% of the losses you
have incurred. I know this is probably less than what you wanted. However, it is also more than you deserve.


This is my best offer. This is my only offer.
I require my demands to be met by December 10, otherwise, the treaty falls through.

Additionally, should I be contacted by agents from any of the 206 sovereignties, concerning the trades I placed on
Kyber, the treaty falls through. In this case, rebates will total to exactly 0.

Kyber is one of the original and longest-running DeFi protocols. No one wants to see it go under.

To assist with this transition of leadership, I may be contacted on telegram: @Kyber_Director

Thank you.

- Kyber Director
```

在这份链上声明中，KyberSwap Exploiter 提出了一系列和解条件，包括对 Kyber 公司的完全执行控制权，临时全面掌握 KyberDAO 的治理机制以实施立法变更，以及要求交出所有与公司/协议有关的文件和资讯。此外，攻击者也要求 Kyber 公司交出所有链上和链下资产。KyberSwap Exploiter 承诺，一旦要求得到满足，将对公司高层、员工、代币持有者和投资者进行一系列补偿措施。包括为高阶主管提供公平估值的买断、将员工薪水翻倍、为不愿留下来的员工提供 12 个月的遣散费和全面福利，以及保证投资者代币的价值。攻击者强调，如果其要求在 12 月 10 日前未满足，或受到任何主权国家代理人的联系，和解协议将宣告破裂。在这份声明中，KyberSwap Exploiter 还自称为 Kyber Director。

据 KyberSwap 团队最新的消息，已与抢跑机器人的主控者取得联系，协商退还其获取的用户资金的 90%，到目前为止，KyberSwap 团队已收到抢跑机器人的主控者退回的价值总计约 517 万美元的资金。

想了解如何进行链上留言，可参考 https://mp.weixin.qq.com/s/76u8R1c1411eQRd1aj85SA。

3.3 黑客团伙画像及动态

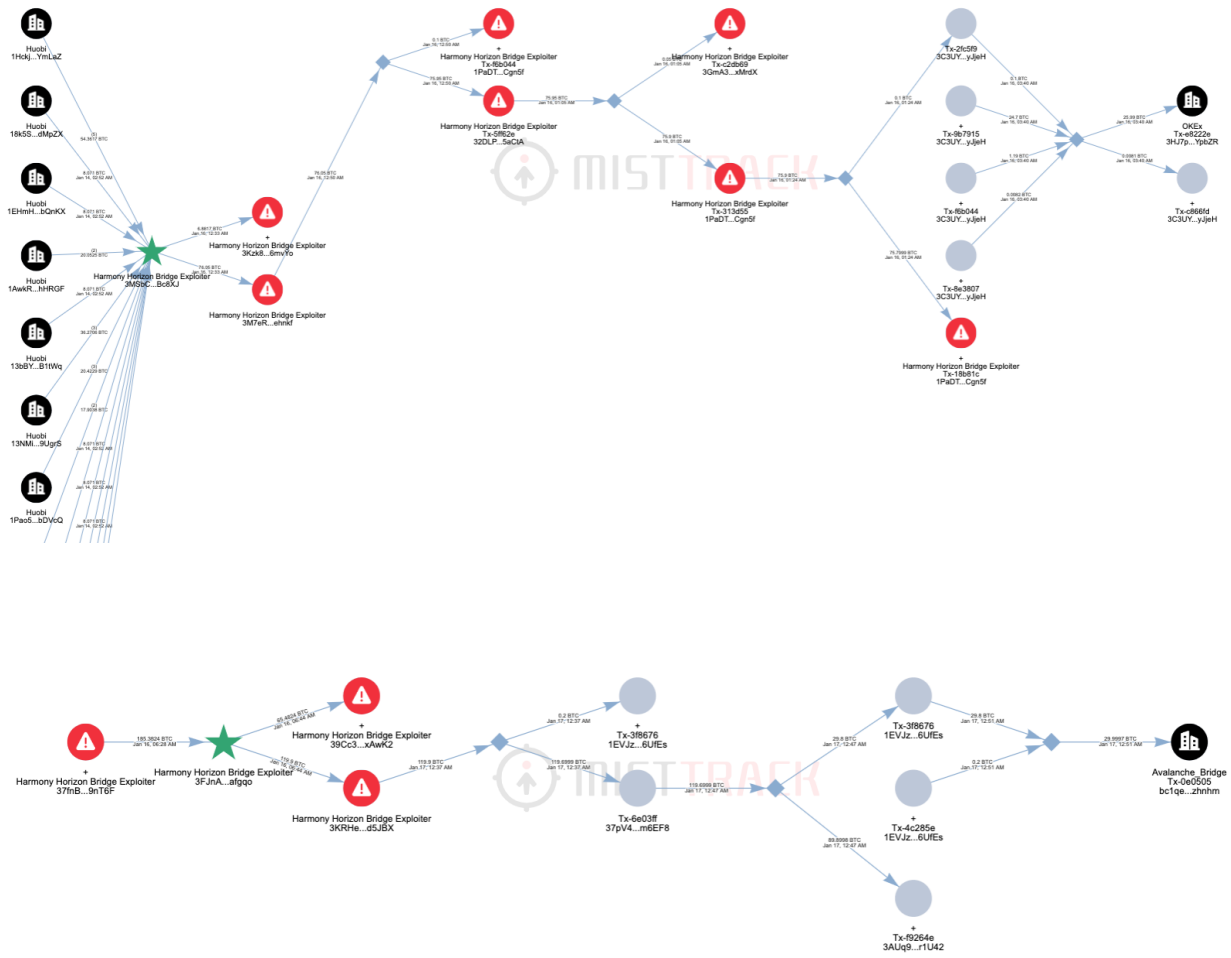
3.3.1 黑客团伙 Lazarus Group

根据 2023 年的公开信息，截止到 6 月份，仍然没有任何重大加密货币盗窃案被归因为朝鲜黑客 Lazarus Group。从链上活动来看，朝鲜黑客 Lazarus Group 主要在清洗 2022 年盗窃的加密货币资金，其中包括 2022 年 6 月 23 日 Harmony 跨链桥遭受攻击损失的约 1 亿美元的资金。

2022 年 6 月 23 日 Harmony 跨链桥遭受攻击后，被盗资金被直接存款到 Tornado Cash 隐私混币协议后随即提款到一批新地址作为余额，后未进一步转移。

朝鲜黑客 Lazarus Group 清洗 2022 年盗窃 Harmony 跨链桥相关加密货币资金的活动如下：

- 在沉寂了近半年后，2023 年 1 月 13 日至 1 月 16 日，黑客开始转移从 Tornado Cash 提取的资金，并在隐私网络 Railgun 中进行充提款，随后部分资金被转移到交易平台并提款到 BTC 网络。



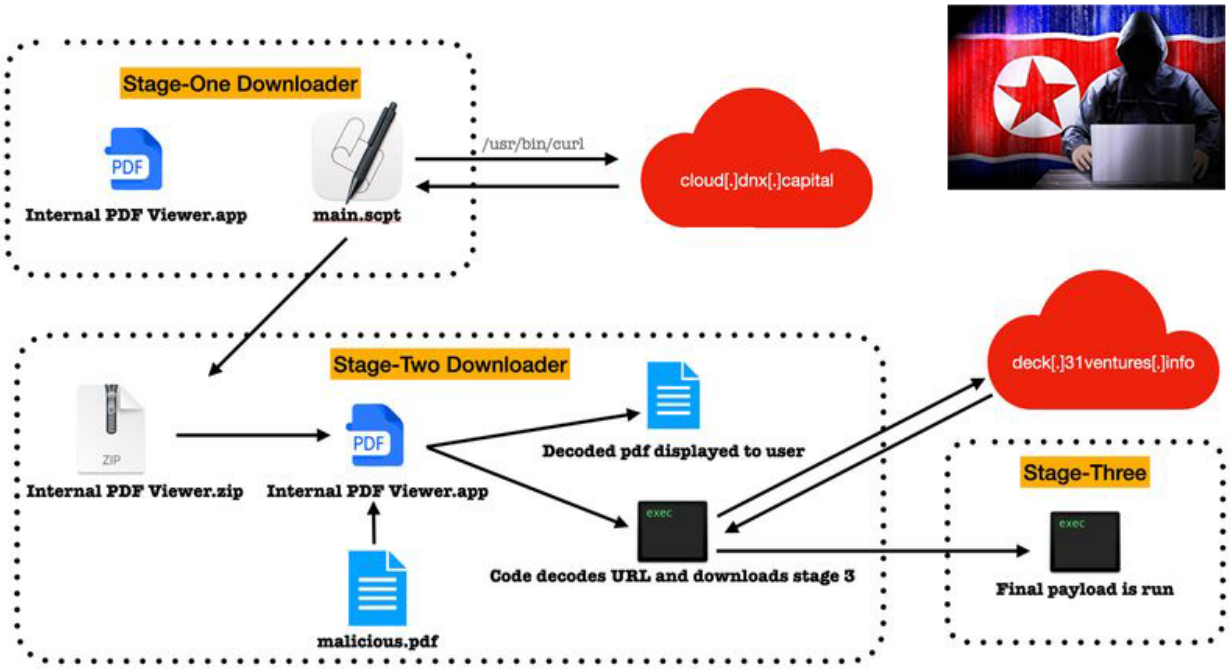
- 1 月 16 日后几天，黑客将提款到 BTC 网络的资金进行进一步的多层转移。一部分资金再次转移到一些交易平台，而另一部分资金则通过 Avalanche Bridge 跨链到 Avalanche 链，最终兑换成 USDT/USDD，并转移到 ETH / TRON 链中的混币网络。

后续的事实却表明，朝鲜黑客 Lazarus Group 除了在清洗 2022 年盗窃的加密货币资金以外，其他的时间也没有闲着，这个黑客团伙在黑暗中蛰伏着，暗中地进行 APT 相关的攻击活动。这些活动直接导致了从 6 月 3 日开始的加密货币行业的“黑暗 101 日”。

在“黑暗 101 日”期间，共计有 5 个平台被盗，被盗金额超 3 亿美元，其中被盗对象多为中心化服务平台。

时间	事件	被盗资金	参考
6 月 3 日	多名 Atomic Wallet 用户的资产被盗	超 100M 美元	链接
7 月 22 日	Coinspaid 热钱包恶意授权提款	37.3M 美元	链接
7 月 23 日	Alphapo 热钱包被盗	60M 美元	链接
9 月 4 日	Stake.com 加密货币赌博平台被盗	41M 美元	链接
9 月 12 日	CoinEx 热钱包私钥泄露	70M 美元	链接
	合计	308.3M 美元	

9 月 12 日左右，慢雾联合合作伙伴发现黑客团伙 Lazarus Group 定向对加密货币行业进行的大规模APT攻击活动。攻击手法如下：首先是进行身份伪装，通过实人认证骗过审核人员并成为真实客户，而后真实入金存款。在此客户身份掩护下，在之后多个官方人员和客户(攻击者)沟通时间点上针对性地对官方人员精准投放 Mac 或 Windows 定制木马，获得权限后进行内网横向移动，长久潜伏从而达到盗取资金的目的。



美国 FBI 同样关注着加密货币生态的重大盗窃案，并在新闻稿中公开说明由朝鲜黑客 Lazarus Group 操纵的事件。以下是 FBI 于 2023 年发布的关于朝鲜黑客 Lazarus Group 的相关新闻稿。

- 1 月 23 日，FBI 确认 朝鲜黑客 Lazarus Group 应该对 Harmony Hack 事件负责。
- 8 月 22 日，美国联邦调查局 (FBI) 发布 通告 称，朝鲜黑客组织涉及 Atomic Wallet、Alphapo 和 CoinsPaid 的黑客攻击，共窃取 1.97 亿美元的加密货币。
- 9 月 6 日，美国联邦调查局 (FBI) 发布 新闻稿，确认朝鲜黑客 Lazarus Group 应对 Stake.com 加密货币赌博平台被盗 41M 美元事件负责。

根据我们的分析，朝鲜黑客 Lazarus Group 的洗钱方式也随着时间在不断进化，隔一段时间就会有新型的洗钱方式出现，洗钱方式变化的时间表如下表：

时间	事件	新型洗钱方式
1 月	资金洗钱 - Harmony 跨链桥被攻击事件	ETH 链：被盗资金 -> Tornado Cash -> Railgun -> 一些交易所（例如 Binance, OKX, Huobi 等）-> BTC 链：从交易所提款 -> Avalanche Bridge -> Avalanche 链：跨链后资金 -> 1inch 交易聚合器 limit order 功能兑换为 ETH Token -> Bridge -> ETH 链： 1.跨链后资金 -> 1inch 交易聚合器 limit order 功能兑换为 USDT Token -> ETH 洗钱网络 2.跨链后资金 -> 1inch 交易聚合器 limit order 功能兑换为 USDD Token -> BitTorrent Bridge -> TRON 链：跨链后资金 -> 多层转移 -> TRON 洗钱网络
6 月	多名 Atomic Wallet 用户的资产被盗	ETH 链：被盗 Token 资金 -> MetaMask Swap ->

		ETH -> WETH -> 恶意合约 -> ETH -> WETH -> Avalanche Bridge
7 月	Coinspaid 热钱包恶意授权提款	ETH 链：被盗 Token 资金 -> Uniswap -> ETH -> WETH -> Avalanche Bridge -> Avalanche 链：从 Avalanche Bridge 提款 -> 1inch -> BTC Token -> Bridge BTC 链：从 Bridge 提款 -> Sinbad 混币器
7 月	Alphapo 热钱包被盗	TRON 链：被盗 Token 资金 -> Sunswap -> TRX 资金 -> TransitSwap -> ETH 链：与 (1) Stake.com 加密货币赌博平台被盗 和 (2) CoinEx 热钱包私钥泄露 事件的资金在不同链上有重合
9 月	Stake.com 加密货币赌博平台被盗	BSC 链：被盗 Token 资金 -> 1inch / Biswap / Pancakeswap -> BNB -> Swft 跨链 -> TRON 链：Swft 跨链后资金 -> USDT-TRC20 -> Swft 跨链 -> BSC 链：Swft 跨链后资金 -> BNB -> BSC: Token Hub -> BNB Chain -> Thorchain -> BTC Network
9 月	CoinEx 热钱包私钥泄露	TRON 链：被盗 Token 资金 -> Sunswap -> TRX -> Sunswap -> USDT -> Hieswap / BitTorrent -> BSC 链：从 Hieswap / BitTorrent 提款 -> USDT-BEP20 -> Stargate -> USDT-ERC20 ->

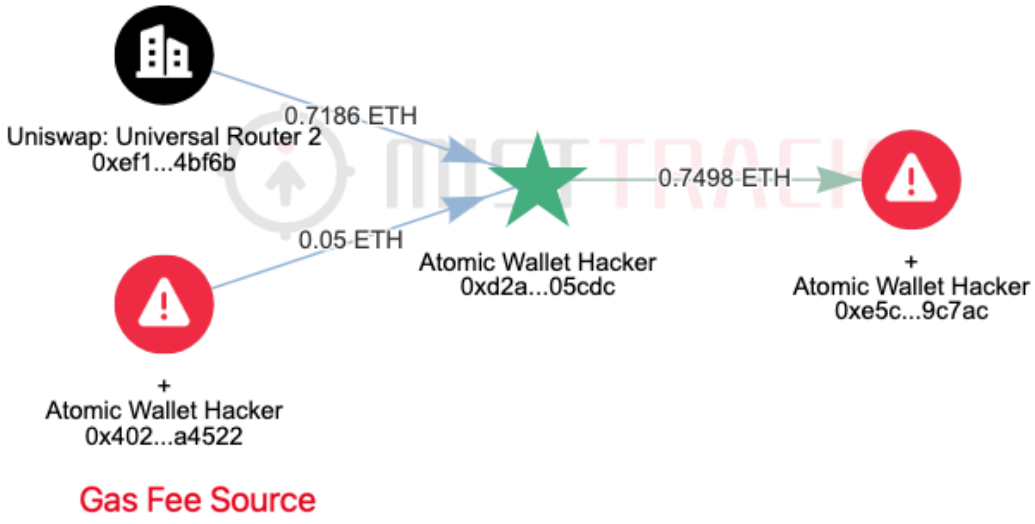
		Thorchain -> BTC 链：Thorchain 跨链后资金 -> BTC -> Swft 等跨链桥 TRON 链：Swft 跨链后资金 -> USDT-TRC20 -> TRON 链 OTC 地址s
9 月	资金洗钱 - Harmony 跨链桥被攻击事件	转移到某俄罗斯交易所进行洗钱

基于 InMist 情报网络合作伙伴的大力情报相关支持，慢雾 AML 团队对这些被盗事件与黑客团伙 Lazarus Group 相关的数据进行跟进分析，进而得出黑客团伙 Lazarus Group 的部分画像：

- 常使用欧洲人、土耳其人的身份作为伪装。
- 已经掌握到的数十个 IP 信息、十数个邮箱信息及部分脱敏后身份信息。
    - 111.*.*.49
    - 103.*.*.162
    - 103.*.*.205
    - 210.*.*.9
    - 103.*.*.29
    - 103.*.*.163
    - 154.*.*.10
    - 185.*.*.217

关于与黑客团伙 Lazarus Group 有关的事件细节分析分享如下：

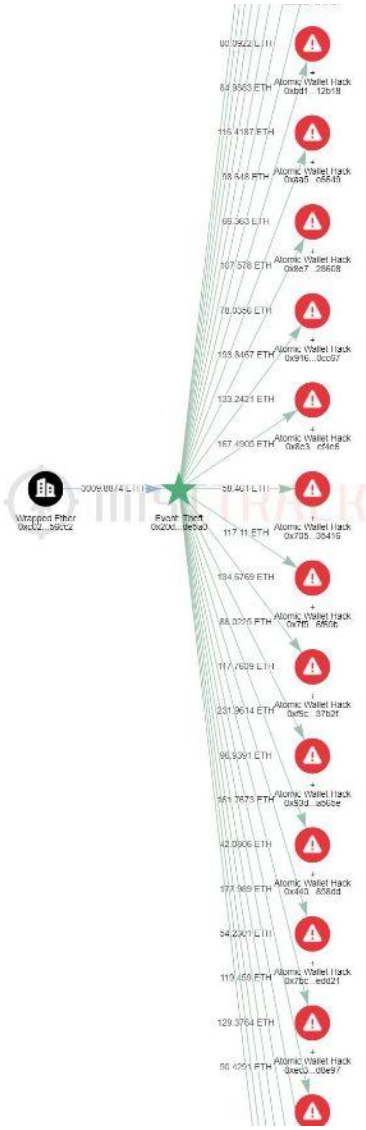
- Atomic Wallet 用户被盗事件



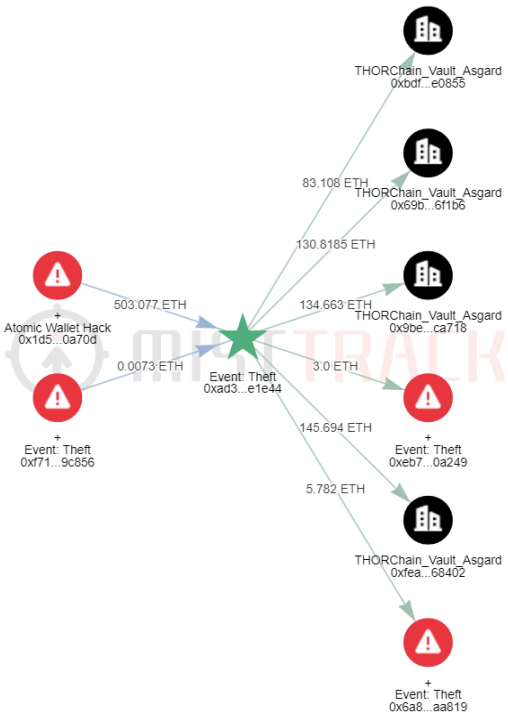
6 月 3 日，一些 Atomic Wallet 用户在社交媒体上报告，称他们的钱包资产被盗。据统计，目前被盗金额已达到 1 亿美金，调查工作发现 142 个与黑客有关的新的可疑地址。到 6 月 9 日，调查发现了 Atomic Wallet 黑客的资金转移模式类似于 Lazarus Group 以前使用的策略（Token 类资金被黑客从被盗用户地址转移到新地址后，通过 Uniswap、MetaMask Swap 及 Sunswap 等方式将所有 Token 类资金兑换为链基础资产，Ethereum 链为 ETH 币种，TRON 链为 TRX 币种）。

据 MistTrack 分析，目前已出现以下三种洗钱方式：

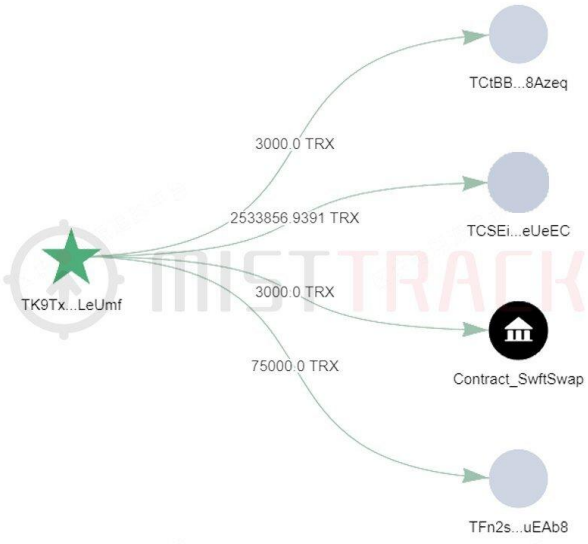
1）黑客分别部署两个兑换合约，其一先将 ETH 兑换为 WETH，其二再将 WETH 兑换为 ETH。接着将兑换后的 ETH 分散转移到多个地址，并再次兑换为 WETH 后跨链到 Avalanche，最后将 WETH 换为 BTC，并从 Avalanche 跨链到 BTC 网络。



2) 将 ETH 转移到 THORChain，接着将 ETH 兑换为 BTC，再跨链到 BTC 地址。此外，黑客还使用 SwftSwap 进行跨链。

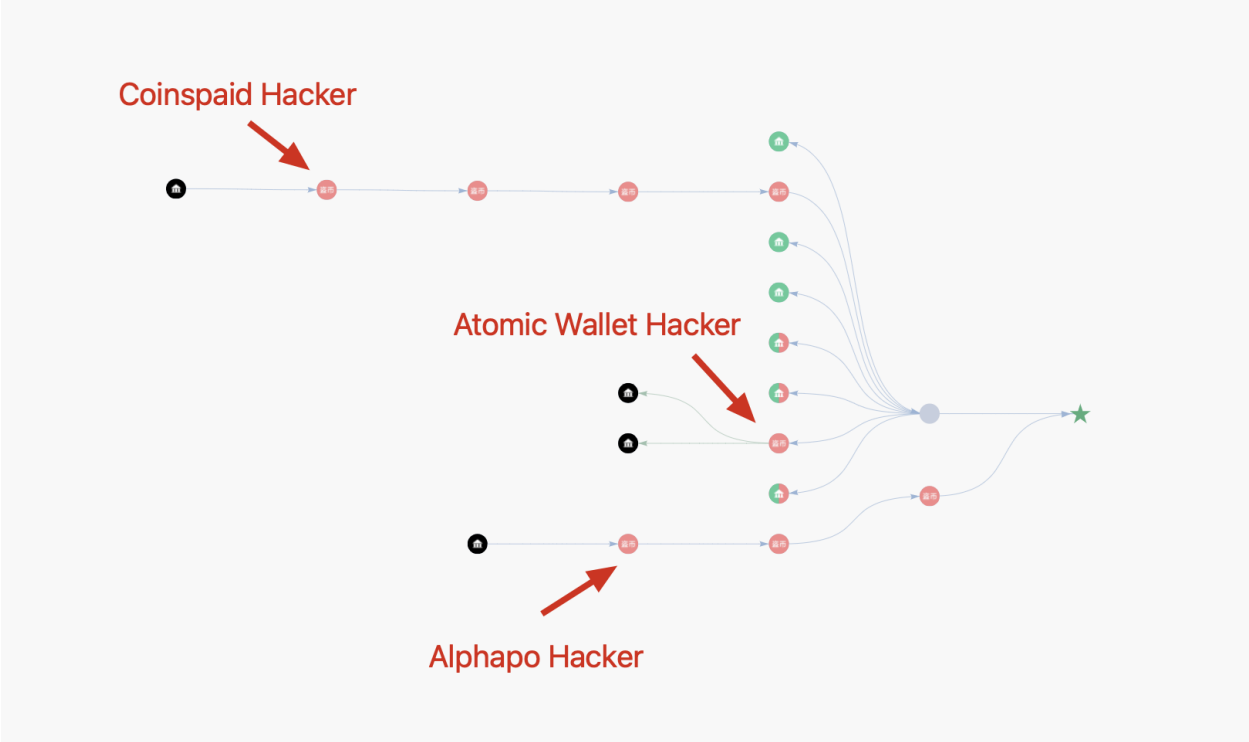


3) 黑客将大部分 USDT 通过 SunSwap 兑换为 TRX 并汇集到某个 TRON 地址。该 TRON 地址再将 TRX 分散转移到多个地址，最后大部分转入交易平台充币地址，一部分使用 SuntSwap 将 TRX 换为 USDT，大部分 USDT 被分散转入交易平台，一部分使用 SwftSwap 跨链。



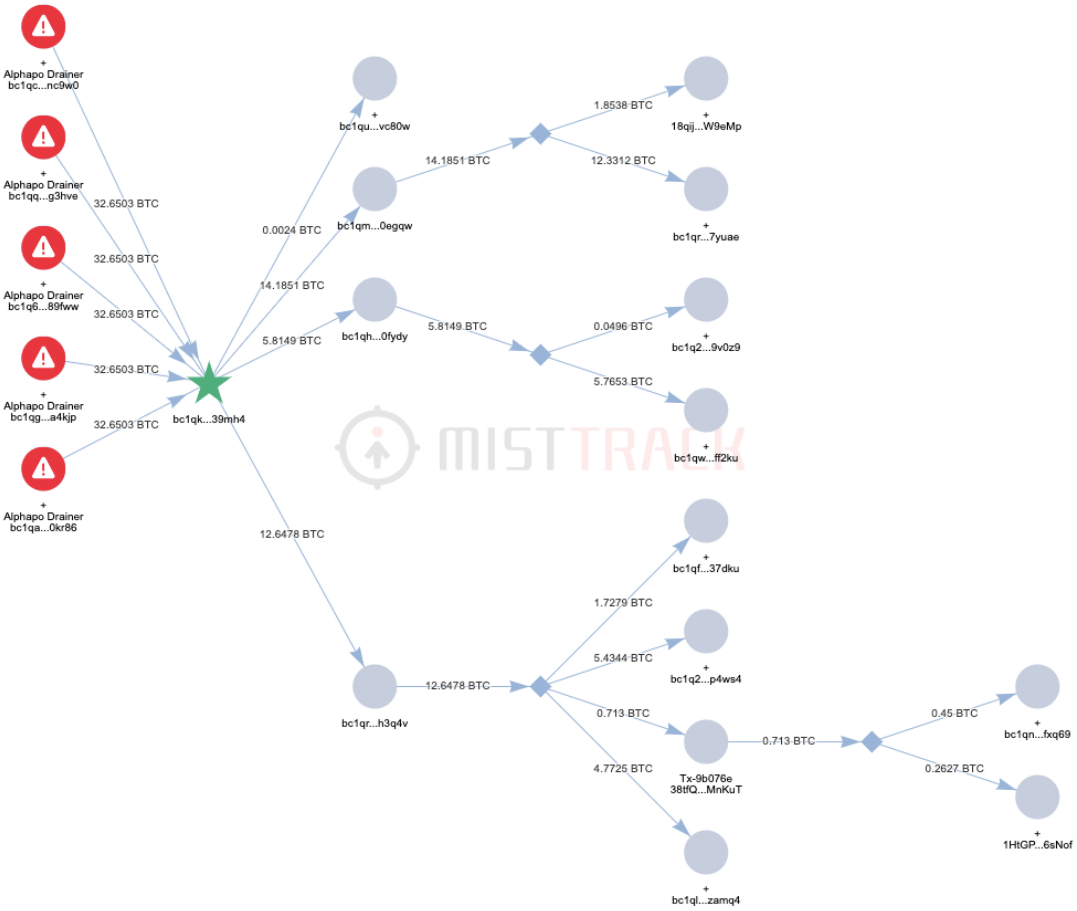
- Coinspaid 热钱包恶意授权提款

在 2023 年 7 月 22 日的 CoinsPaid 攻击中，疑似黑客团伙 Lazarus Group 冒充招聘者，专门针对 CoinsPaid 的员工发送了招聘电子邮件和 LinkedIn 消息。其中 CoinsPaid 表示，疑似黑客团伙 Lazarus Group 花了 6 个月的时间试图获得对其网络的访问权限。Coinspaid 后续的被盗资金转移与多名 Atomic Wallet 用户的资产被盗和 Alphapo 热钱包被盗事件资金有重合。



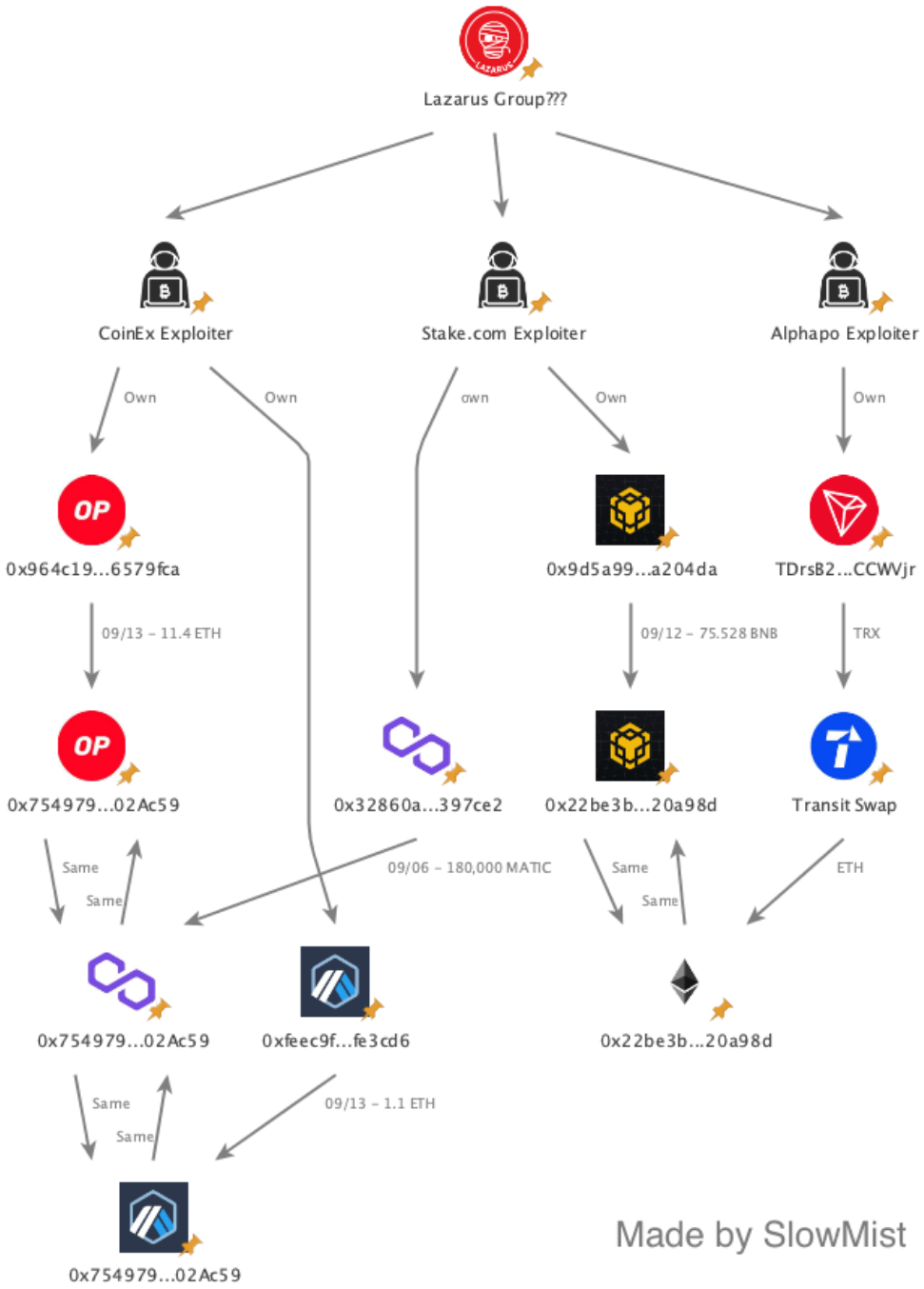
- Alphapo 热钱包被盗

7 月 23 日，Alphapo 热钱包被盗后，黑客将被盗资金进行多层跨链后提款到 BTC 网络，后再次通过跨链桥将 BTC 兑换为 USDT-TRC20 提款到 TRON 网络。例如在 ETH 链上被盗资金的兑换路径为：Ethereum Chain -[Avalanche Bridge]-> Avalanche Chain -[Avalanche Bridge]> Bitcoin Network.



- Stake.com 加密货币赌博平台被盗

根据 AML 反洗钱团队分析，Stake.com 被盗资金的后续转移与 Alphapo 热钱包被盗和 CoinEx 热钱包私钥泄露事件资金有重合。其中在 BSC 链，Stake.com 加密货币赌博平台的被盗 BNB 资金转移到多个 ChangeNOW 充币地址，后部分被盗资金通过 TransitSwap 和 Swft 跨链平台兑换后转移到 Mexc 等交易所。



- CoinEx 热钱包私钥泄露

CoinEx 交易所在 9 月 13 日发生热钱包私钥泄露事件。根据链上关联，被盗资金在转移过程中与 Alphapo 热钱包被盗 和 Stake.com 加密货币赌博平台被盗事件资金有重合，此前美国 FBI 于 8 月

22 日和 9 月 6 日分别确认 Alphapo 与 Stake.com 被盗事件由黑客团伙 Lazarus Group 负责。

CoinEx 热钱包私钥泄露事件被盗资金的洗钱转移分为多个阶段，且在不同的链存在不同的洗钱行为：

1）第一阶段：转移资金到 BTC 网络

Tron 链被盗资金：Tron 链被盗 Token 资产 -> Sunswap -> TRX -> SunSwap -> USDT-TRC20 -> HieSwap / BitTorrent 跨链桥 -> BSC 链 -> USDT-BEP20 -> Stargate 跨链桥 -> ETH 链 -> USDT-ERC20 -> ThorChain 跨链桥 -> Bitcoin -> Sinbad 混币器。

BSC 链被盗资金：BSC 链被盗 Token 资产 -> Pancakeswap -> BNB -> BSC: Token Hub -> BNB Chain -> Thorchain -> Bitcoin

Solana 链被盗资金：SOL -> Wormhole Bridge 跨链桥 -> ETH 链 -> ETH -> Kucoin 等交易所。

其他链币种通过 ChangeNOW, FixedFloat, Simpleswap, letsexchange 等交易所进行跨链兑换。

2）第二阶段：从 BTC 网络转移资金到 Tron 链 OTC

BTC -> Swft / 其他跨链桥平台 -> Tron 链 -> USDT-TRC20 -> 疑似 OTC

3）第三阶段：从 Sinbad 混币器提款 -> BTC -> Thorchain -> ETH 链

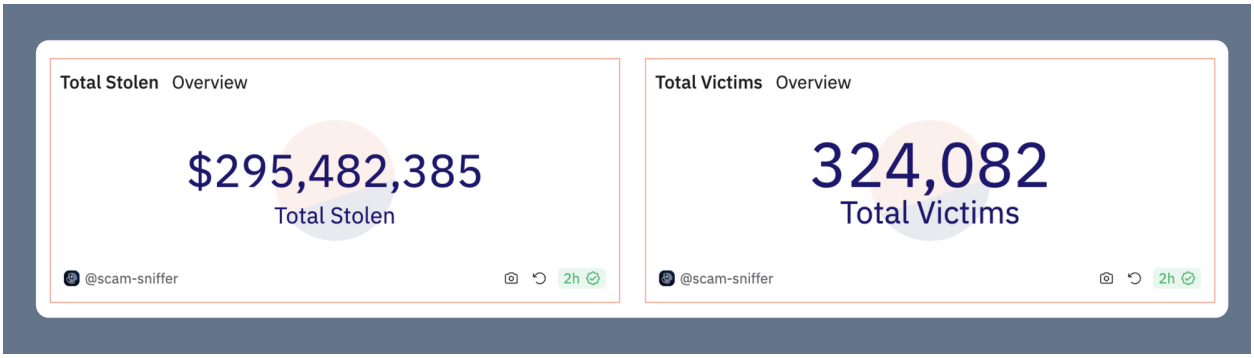
3.3.2 钓鱼团伙 Wallet Drainers

注：本小节由 Scam Sniffer 倾情撰写，在此表示感谢。

- 概览

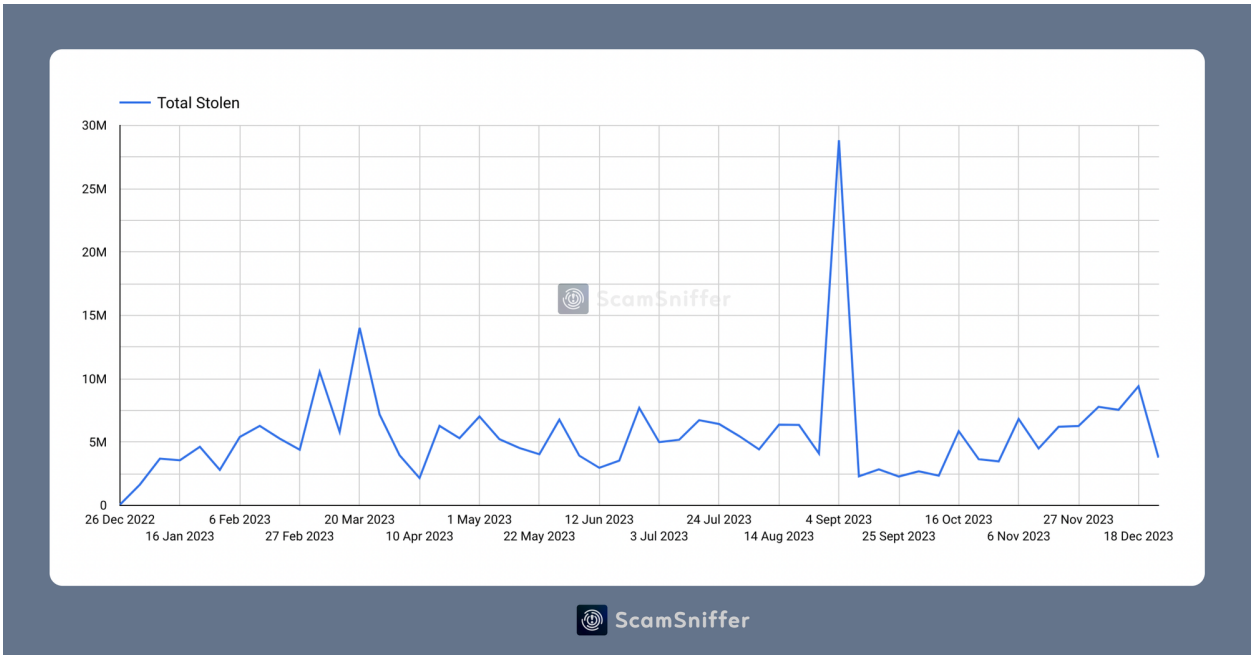
Wallet Drainer 作为一种加密货币相关的恶意软件，在过去的一年里取得了显著的"成功"。这些软件被部署在钓鱼网站上，骗取用户签署恶意交易，进而盗取其加密货币钱包中的资产。这些钓鱼活动以多种形式不断地攻击普通用户，导致许多人在无意识地签署恶意交易后遭受了重大财产损失。

- 被盗统计



在过去一年，Scam Sniffer 监控到这些 Wallet Drainers 已经从大约 32 万受害者中盗取了将近 2.95 亿美金的资产。

- 被盗趋势



值得一提的是，3 月 11 号这一天有接近 700 万美金被盗。大部分是因为 USDC 汇率波动，遭遇了假冒 Circle 的钓鱼网站。也有大量的被盗临近 3 月 24 号 Arbitrum 的 Discord 被黑以及后续的空投。

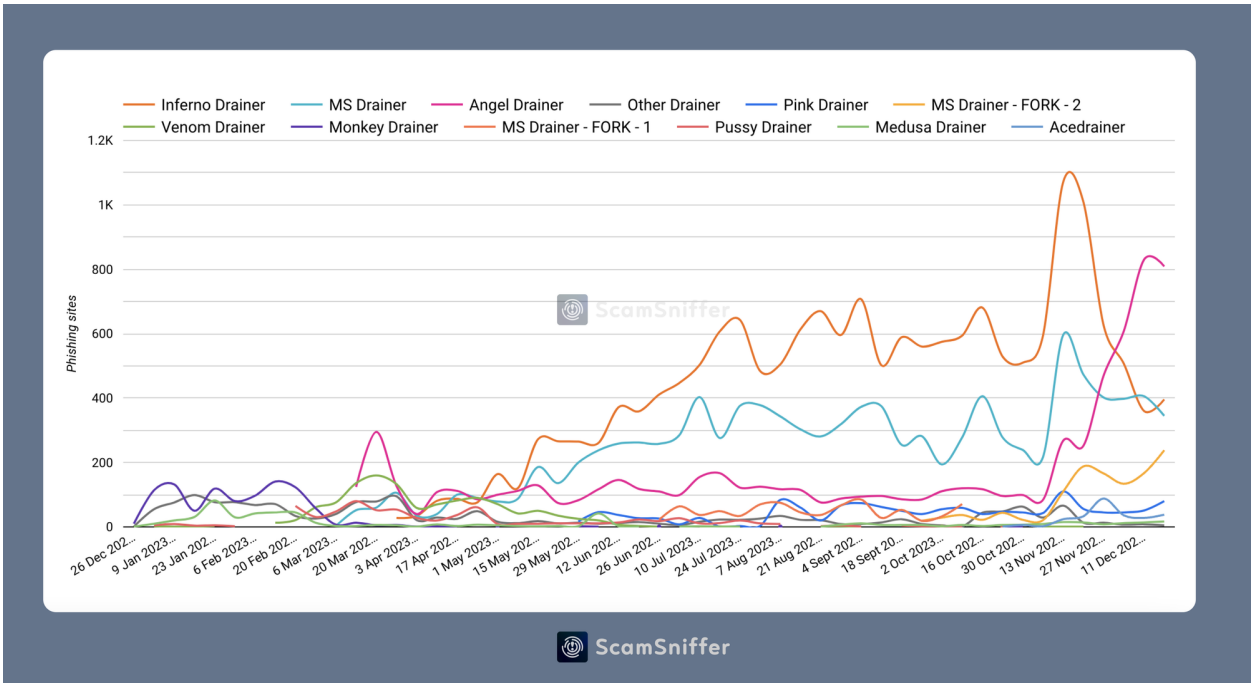
每次波峰都伴随着关联群体性事件。可能是空投，也可能是黑客事件。

- 值得注意的 **Wallet Drainers**

Drainer	Total Stolen	Victims	Source	Appeared time
Inferno Drainer	$81 million	134k	View	March, 2023
MS Drainer	$59 million	63k	View	March, 2023
Angel Drainer	$20 million	30k	View	March, 2023
Monkey Drainer	$16 million	18K	View	August, 2022
Venom Drainer	$27 million	15k	View	January, 2023
Pink Drainer	$18 million	9k	View	March, 2023
Pussy Drainer	$15 million	4k	View	January, 2023

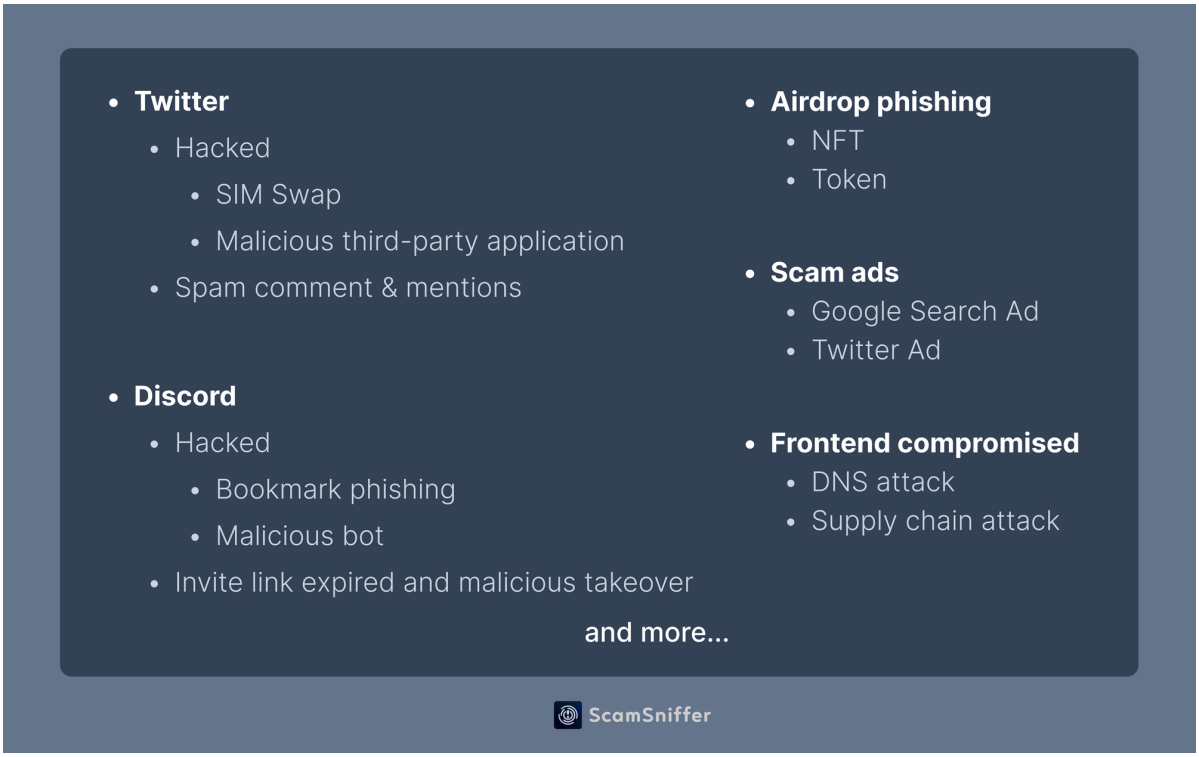
随着 ZachXBT 揭露 Monkey Drainer 后，他们在活跃了 6 个月后宣布退出，然后 Venom 接替了他们的大部分客户。随后 MS, Inferno, Angel, Pink 也都在 3 月份左右出现。随着 Venom 在 4 月份左右停止服务，大部分的钓鱼团伙转向了使用其他的服务。按照 20% 的 Drainer 费用，他们通过出售服务获利至少 4700 万美金。

- **Wallet Drainers 趋势**



通过分析趋势可以发现，钓鱼活动相对来讲一直在持续增长。而且在每一个 Drainer 退出后都会有新的 Drainer 替代他们，比如近期在 Inferno 宣布退出后，Angel 似乎成为了新的替代品。

- 他们都是如何发起钓鱼活动的？



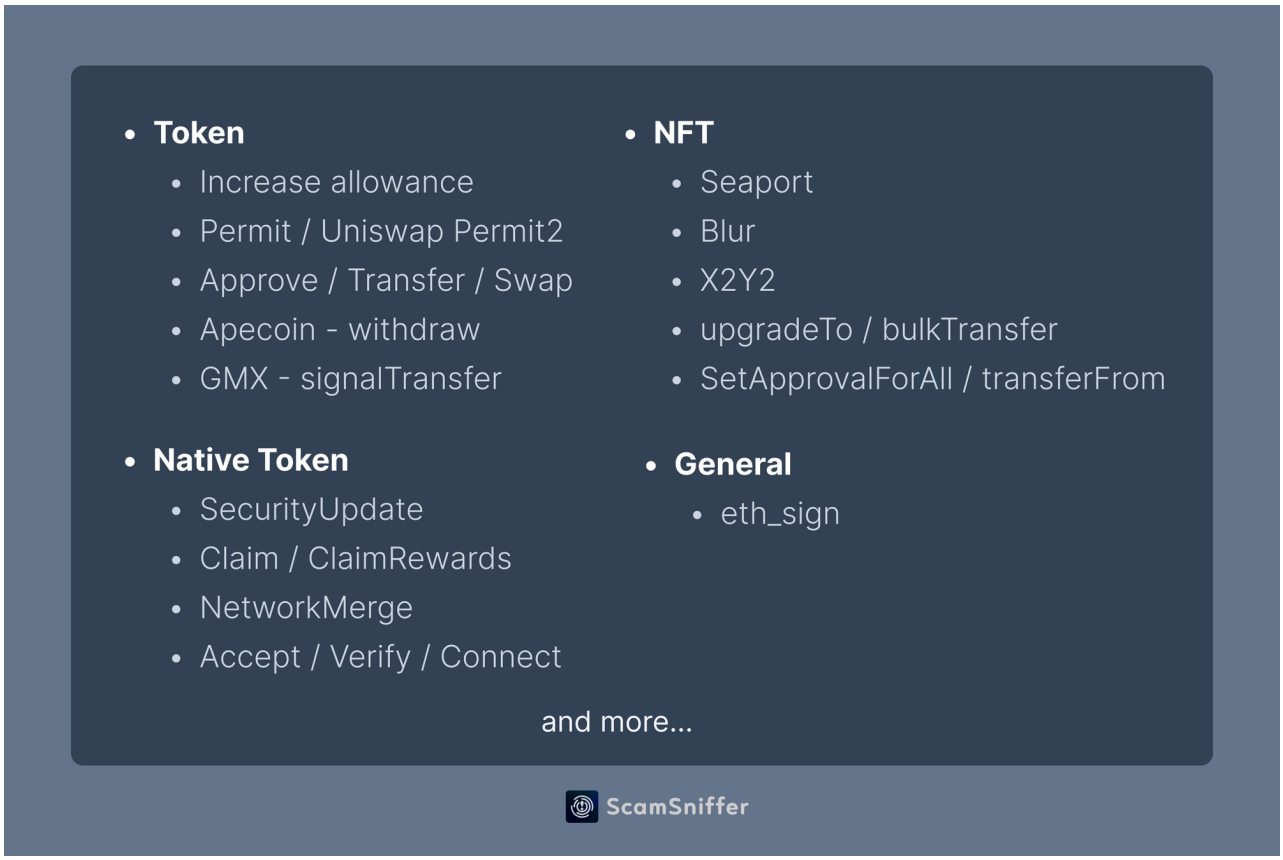
这些钓鱼网站其主要获取流量的方式可以大致主要分为几类：

- 黑客攻击
    - 官方项目 Discord 和 Twitter 被黑
    - 官方项目前端或使用的库被攻击
- 自然流量
    - 空投 NFT 或 Token
    - Discord 链接失效被占用
    - Twitter 垃圾提醒和评论
- 付费流量
    - Google 搜索广告
    - Twitter 广告

黑客攻击虽然影响面大，但往往反应足够及时，一般 10-50 分钟整个社区都有所行动。而空投、自然流量、付费广告、以及 Discord 链接失效被占用，这些则更加的不容易察觉。

除此之外，还有更加针对性的对个人的私信钓鱼等。

- 常见的钓鱼签名

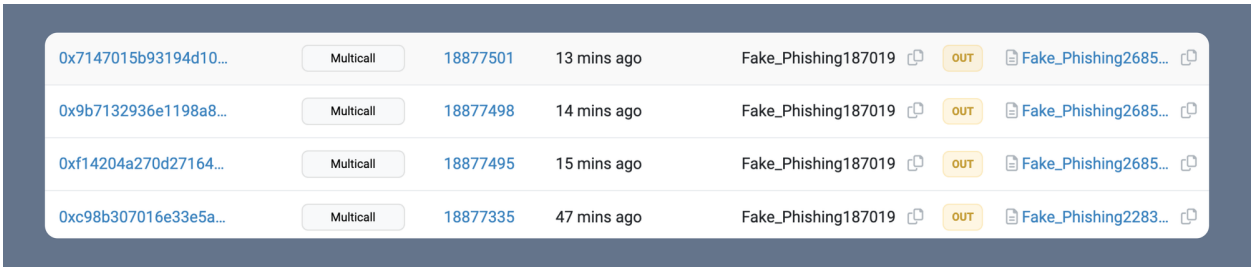


针对不同的资产类型也有着不同的方式来发起恶意钓鱼签名，以上是一些不同类资产所常见的钓鱼签名方式。受害者钱包所拥有的资产类型会决定发起什么样的恶意钓鱼签名。

从利用 GMX 的 signalTransfer 盗取 Reward LP token 的案例中，我们可以发现他们对特定资产的钓鱼利用方式已经到了很精细化的研究。

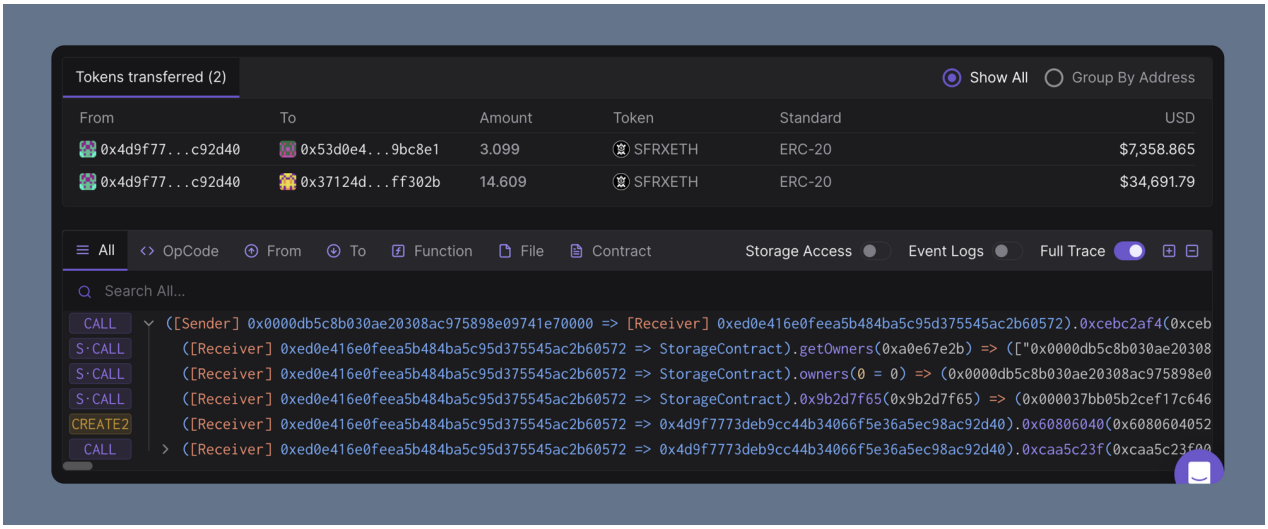
- 更多的使用智能合约

1）Multicall



从 Inferno 开始，他们也开始更多的资源在使用合约技术上。比如在 Split 手续费需要分两笔交易进行。而这有可能速度不够快导致在第二笔转账的时候被受害者提前撤销授权，为了提高效率他们便使用 multilcall 来进行更高效的资产转移。

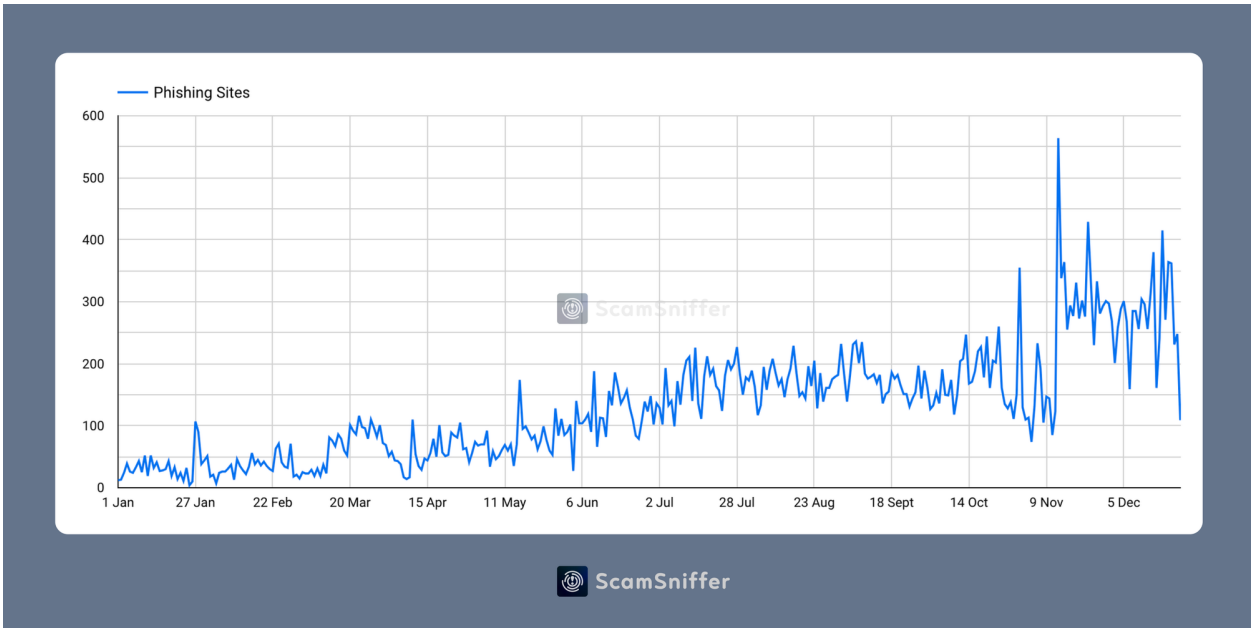
2) CREATE2 & CREATE



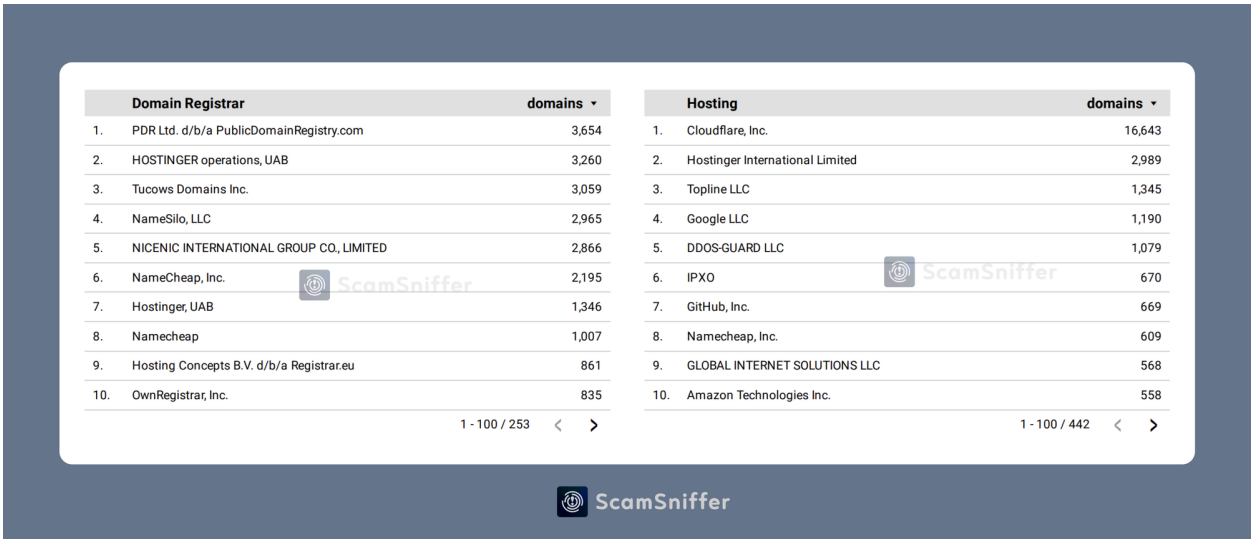
同样为了绕过一些钱包的安全验证，他们也开始尝试使用 create2 或 create 动态生成临时地址。这将导致钱包端的黑名单失去作用，同样对钓鱼研究也产生更大的麻烦。因为你不签名就不知道资产会被转移到什么地址，而临时地址不具备分析意义。

这比起去年来说有着很大的变化。

- 钓鱼网站

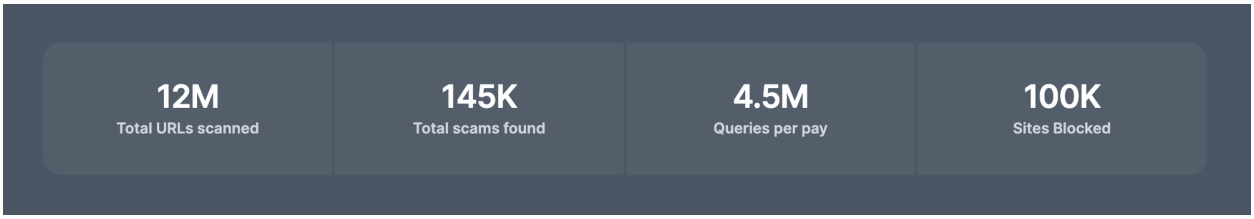


通过分析钓鱼网站的数量趋势，可以明显看到钓鱼活动每个月都在逐步增长，这跟稳定的 wallet drainer 服务有很大关系。

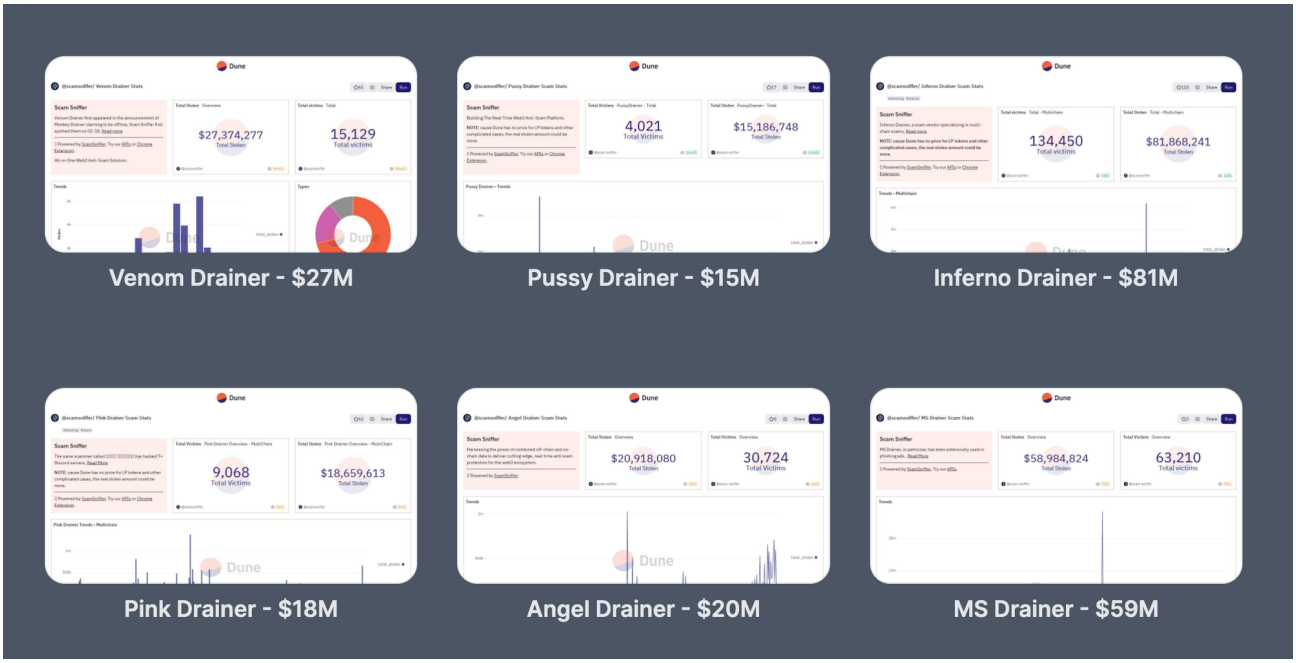


以上是这些钓鱼网站的主要使用的域名注册商。通过分析服务器地址可以发现，他们大都使用了 Cloudflare 来隐藏真实的服务器地址。

在过去的一年中，Scam Sniffer 扫描了近 1200 万条 URL，发现了将近 145,000 个恶意 URL，每天服务了 400 百万的查询。Scam Sniffer 的开源黑名单目前包含了近 100,000 个恶意域名，并持续向 Chainabuse 等平台推送这些恶意网站域名。



作为一家 Web3 反诈骗平台，Scam Sniffer 致力于为下一个十亿用户提供安全的 Web3 环境。他们已连续报道了多个知名的 Wallet Drainers，并在社交平台持续分享有关大额盗窃案例，以提醒和增强大众对钓鱼的认知。目前 Scam Sniffer 已经协助了一些知名平台保护其用户，有需要可以通过邮箱 b2b@ScamSniffer.io 与他们联系。

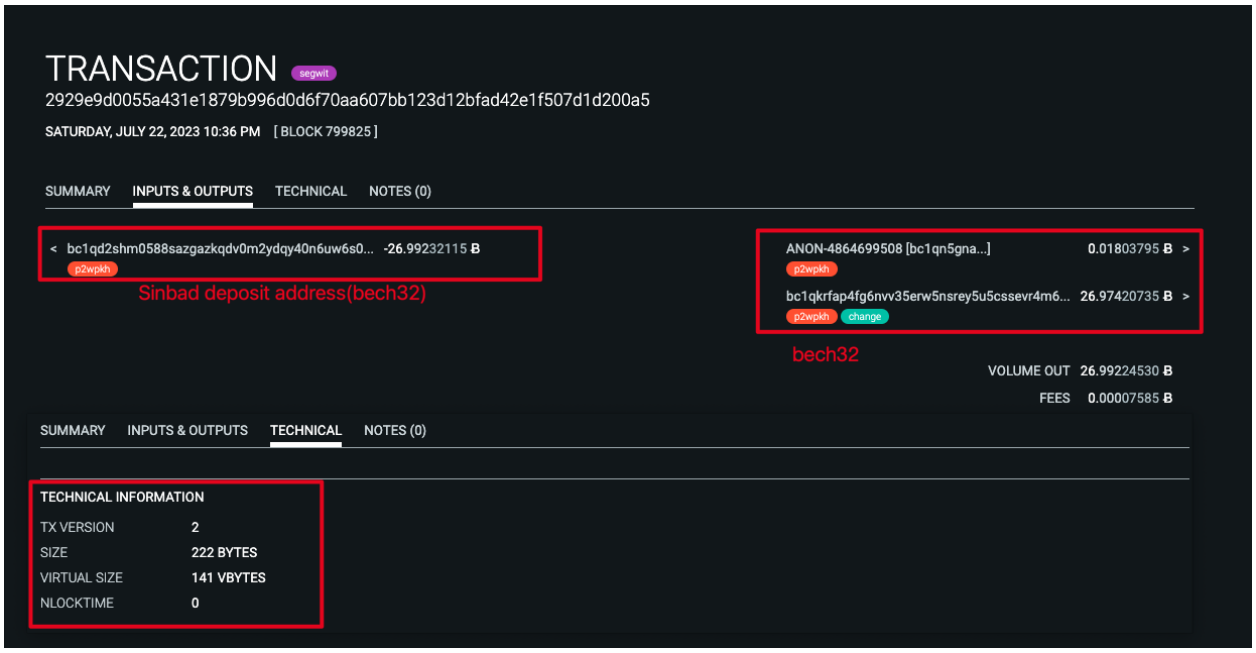


3.4 洗钱工具

3.4.1 Sinbad 混币器

Sinbad 是一个成立于 2022 年 10 月 5 日的比特币混合器。

Alphapo 黑客（Lazarus Group）曾在洗钱过程中使用 Sinbad，如交易：



(https://oxt.me/transaction/2929e9d0055a431e1879b996d0d6f70aa607bb123d12bfad42e1f507d1d200a5)

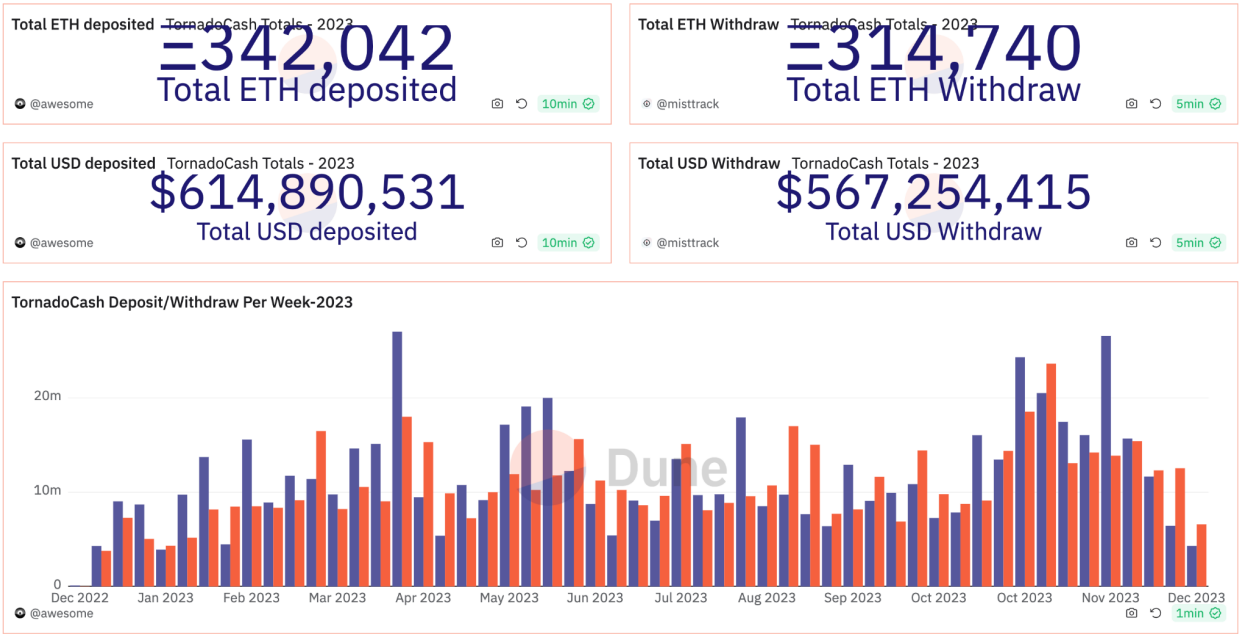
Sinbad 在这笔交易的钱包指纹如下：

Input Address Type	Output Address Type	Version	Locktime
bech32(bc1q...)	bech32(bc1q...)	2	0

11 月 29 日，美国财政部已从全球美元金融体系中屏蔽了加密货币混合服务 Sinbad，原因是该服务支持与朝鲜黑客组织有关的交易。Sinbad 的网站也被美国联邦调查局、荷兰金融情报调查局、荷兰检察官办公室和芬兰国家调查局查封。

美国财政部将 Sinbad 描述为“虚拟货币混合器，是 OFAC 指定的朝鲜黑客组织 Lazarus 集团的主要洗钱工具”。Sinbad 处理了来自 Horizon Bridge 和 Axie Infinity 黑客攻击的资金，还转移了与“逃避制裁、贩毒、购买儿童性虐待材料以及在暗网市场上进行其他非法销售”相关的资金。

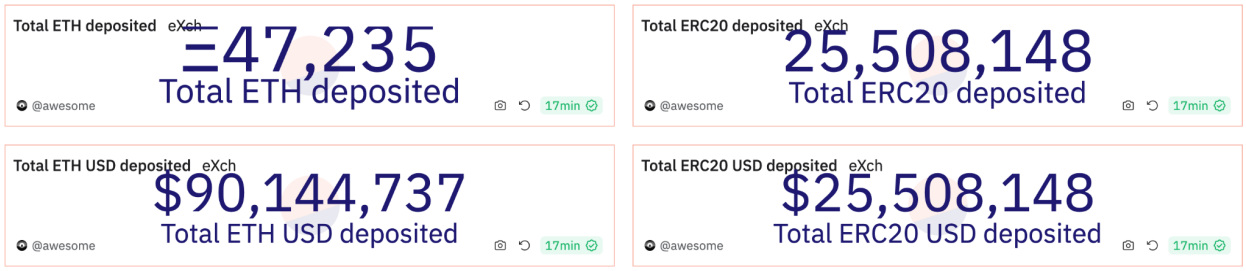
3.4.2 Tornado Cash



(https://dune.com/misttrack/mixer-2023)

2023 年用户共计存入 342,042 ETH（约 6.14 亿美元）到 Tornado.Cash，共计从 Tornado.Cash 提款 314,740 ETH（约 5.67 亿美元）。

3.4.3 eXch



(https://dune.com/misttrack/mixer-2023)

2023 年用户共计存入 47,235 ETH（约 9014 万美元）到 eXch，共计存入 25,508,148 ERC20 稳定币（约 2550 万美元）到 eXch。

3.4.4 Railgun

在 2023 年初，美国联邦调查局表示，朝鲜黑客团伙 Lazarus Group 运用隐私混合器 —— Railgun 来清洗从 Harmony 的 Horizon Bridge 窃取的超过 6000 万美元的资金，使得资金的追溯变得困难。

为了应对制裁，加强反洗钱合规性，并保护用户隐私，Railgun 与 Chainway 于 5 月 8 日达成了合作。他们共同引入了一项"无罪证明"的新功能，这一功能使得用户能在保护其个人身份的同时证明其进行的交易来源合法，未涉及任何黑名单地址。

四、总结

2023 年对于区块链行业来说无疑是极具变化和挑战的一年。它既充满了创新和突破，也伴随着风险和波动。在这样的背景下，我们制作了这份报告，为读者提供一个关于区块链行业安全现状的全面剖析和深度解读。

本报告总结了 2023 年区块链行业的关键监管合规政策及动态，包括但不限于全球范围内对于加密货币的监管态度以及一系列关键的政策变化。同时，我们还总结了 2023 年的区块链安全事件和反洗钱动态，对部分洗钱工具进行了分析，对那些典型的安全事件和钓鱼骗局进行了说明，并提出了相应的防范和应对措施。希望通过我们的努力，提高区块链行业从业者和用户的安全意识。

我们还很荣幸邀请了 Web3 反诈骗平台 Scam Sniffer 贡献了关于钓鱼团伙 Wallet Drainers 的披露。我们相信这部分内容对于了解其工作方式和获利情况具有重要的参考意义。同时，我们对黑客团伙 Lazarus Group 的洗钱手法进行了分析和统计，揭示了他们如何进行洗钱活动，以期提供防范此类威胁的参考。

总的来说，我们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，使每一位与行业参与者都能从中受益，为推动区块链生态安全的发展贡献出一份力量。

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、关于我们

慢雾(SlowMist) 作为一家行业领先的区块链安全公司，在威胁情报方面深耕多年，主要通过安全审计及反洗钱追踪溯源等服务广大客户，并构建了扎实的威胁情报合作网络。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、漏洞监测(Vulpush)、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、FireEye、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

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

Twitter

https://twitter.com/SlowMist_Team

Github

https://github.com/slowmist

Medium

https://slowmist.medium.com

Email

team@slowmist.com

微信公众号

SLOWMIST

Focusing on Blockchain Ecosystem Security