2022 年度回顾

区块链安全与反洗钱分析

SLOWMIST

目录

一、背景 3
1.1 区块链安全 3
1.2 区块链反洗钱 5
二、区块链安全现状 12
2.1 区块链生态安全概览 12
2.1.1 公链 12
2.1.2 DeFi / 跨链桥 12
2.1.3 NFT 14
2.1.4 钱包 / 交易平台 15
2.1.5 其他 18
2.2 攻击手法 19
2.3 钓鱼/骗局手法 20
2.3.1 浏览器恶意书签盗取 Discord Token 20
2.3.2 “零元购” NFT 钓鱼 22
2.3.3 Redline Stealer 木马盗币 23
2.3.4 空白支票 eth_sign 钓鱼 24
2.3.5 尾号相同 + TransferFrom 零转账骗局 25
2.4 损失 Top10 安全事件 27
2.4.1 Ronin Network 损失超 6.1 亿美元 27
2.4.2 BNBChain 遭到漏洞利用 27
2.4.3 Wormhole 损失超 3 亿美元 27
2.4.4 Beanstalk Farms 遭闪电贷和提案攻击 28
2.4.5 Wintermute 损失 1.6 亿美元 28
2.4.6 Nomad 桥遭受黑客攻击 28
2.4.7 Elrond 出现安全漏洞 28

2.4.8 Mango 因价格操纵被提取 1 亿 美元 28
2.4.9 Harmony 损失超 1 亿美元 29
2.4.10 Qubit 遭攻击损失 8000 万美元 29
三、Top10 安全事件反洗钱分析 29
3.1 工具及方法 29
3.1.1 基础工具 - MistTrack 29
3.1.2 拓展方法 - 数据分析 32
3.2 反洗钱分析详述 33
3.2.1 Ronin Network 33
3.2.2 Wormhole 39
3.2.3 Beanstalk Farms 40
3.2.4 Harmony 43
四、展望 45
五、总结 47
六、免责声明 47
七、关于我们 48

本报告聚焦于 2022 年区块链行业所发生的重大事件，主要介绍区块链行业各赛道的安全状况，延伸并提炼出常见攻击手法，并披露其中几种钓鱼手法。接着对部分安全事件的被盗资金流向进行分析，并通过归纳总结，公布一种针对混币器资金追踪的高级分析方法。

一、背景

2022 年初始，全球加密货币总市值达到近 3 万亿美元，似乎一切都会越来越好，会有越来越多对区块链充满希望的人入场。然而，重大震荡不但冲击市场，也击碎部分参与者的信仰。由于加密货币价格暴跌、交易所暴雷的市场冲击，包括 Terra 崩溃、Celsius Network 和 Voyager Digital 申请破产、Three Arrows Capital 倒闭以及 FTX 暴雷，这些冲击就像多米诺骨牌，一环接一环波及整个市场，导致整个加密市场总市值蒸发约 2 万亿美元。尽管区块链市场在 2022 年经历了令人难以置信的动荡，但苦难的过程中，我们也看到了一些令人兴奋的希望：7 月 4 日，欧盟制定首套加密货币监管规则；9 月 15 日，以太坊合并成功，迈出了解决区块链"扩展性困境"的第一步；9 月 27 日，Cosmos 白皮书 2.0 在 Cosmoverse 正式发布，标志着 Cosmos 正式进入 2.0 时代；许多新兴趋势和主题正在形成，加密货币用户和 Web3 开发人员的数量正在上升，元宇宙的形态正在渐渐显现；区块链迎来加密监管新纪元的开端，加密市场正在步向合规化…… 这些趋势也将推动区块链行业在 2023 年及更长远的发展。

总而言之，2022 年对区块链行业来说是崩塌与希望交织的一年。本文将回顾 2022 年区块链行业发生的安全大事件以及反洗钱分析，同时展望 2023 年区块链的新趋势，让我们一起回味这一年来的惊心动魄和跌宕起伏，并期待着曙光。

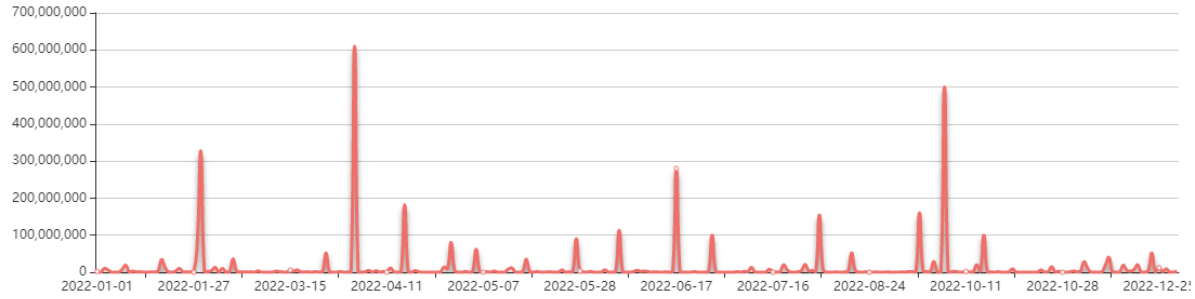
1.1 区块链安全

根据慢雾区块链被黑事件档案库 (SlowMist Hacked) 统计，2022 年安全事件共 303件，损失高达 37.77 亿美元（按事发价格计算）。

[SlowMist Hacked Statistical]:

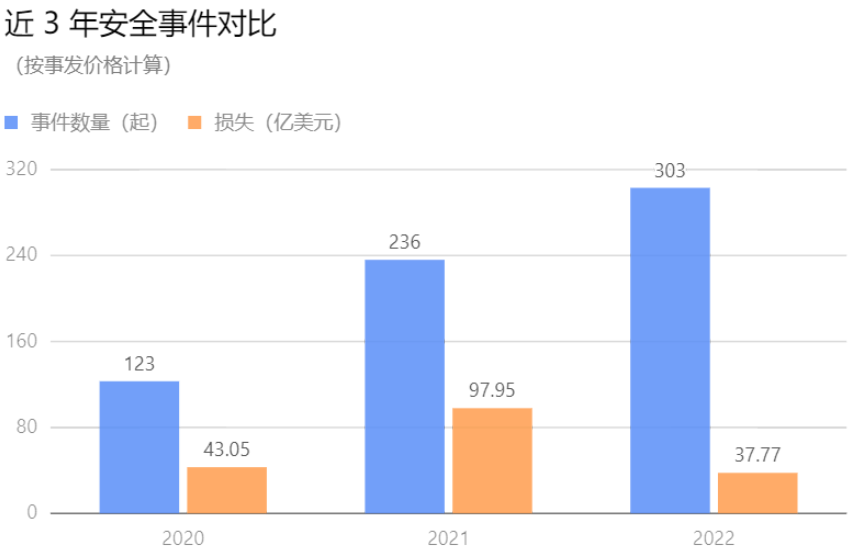
Total 2022 hack event(s) 303 ;

The total amount of money lost by blockchain hackers is about $ 3,777,968,014.78 ;



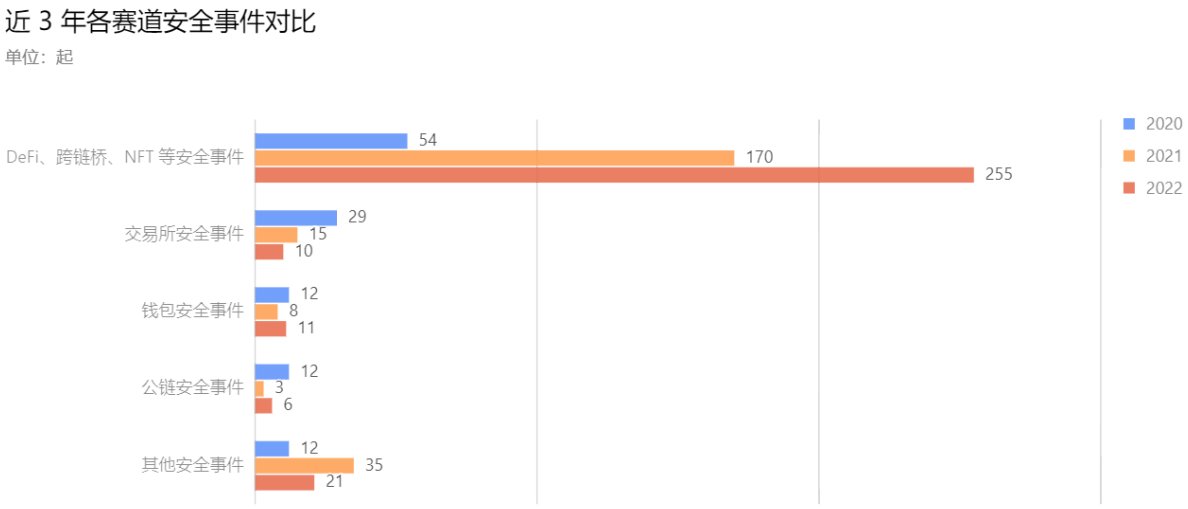
（2022 年安全事件统计）

相比 2021 年的 97.95 亿美元（按事发价格计算）下降约 61%，但这并不包括因市场动荡而损失的资产。



（近 3 年区块链损失对比图）

其中 DeFi、跨链桥、NFT 等安全事件 255 起，交易所安全事件 10 起，公链安全事件 11 起，钱包安全事件 6 起，其他类型安全事件 21 起。



（近 3 年各赛道安全事件对比图）

1.2 区块链反洗钱

匿名性与不可逆是加密货币交易的天然属性，正是这样的原因，在加密货币犯罪频发的情况下，区块链反洗钱处于一个至关重要的位置，也是阻止黑客成功变现的最后防线。面对黑客无孔不入的威胁，不同的群体也不约而同的"组建"起反洗钱同盟，其中包括交易平台/资金管理平台/项目方、监管方和区块链安全公司。

2022 年，这些群体的反洗钱动态如下：

交易平台/资金管理平台/项目方

Tether：2022 年共计 屏蔽了 250 个 ETH 地址，这些地址上拥有的 USDT-ERC20 资产被冻结不可转移。

Circle：2022 年共计 屏蔽了 126 个 ETH 地址，这些地址上拥有的 USDC-ERC20 资金被冻结不可转移。

监管方

美国联邦调查局：2 月 18 日宣布成立专门打击加密货币犯罪部门，新成立的团队名为虚拟资产行动小组。

美国财政部：4 月 14 日制裁 Ronin Network 黑客（LAZARUS GROUP）相关的地址，5 月 6 日 制裁 加密货币混币器 Blender，值得注意的是，美国财政部在此之前从未制裁过加密货币混币器，8 月 8 日 制裁 以太坊混币器 Tornado.Cash，共计制裁 Tornado.Cash 38 个地址。
美国司法部：9 月 17 日成立全国检察官网络，专注于打击加密货币犯罪。

区块链安全公司
Chainalysis：3 月 10 日，创建 SanctionsList 链上数据库合约，共计 制裁 177 个地址 。
SlowMist：4 月 27 日，MistTrack 反洗钱追踪系统 正式上线，专注于打击加密货币洗钱活动。

众所周知，造成区块链安全事件的黑客、黑色产业链、欺诈者和 Rug Pull 项目方一直是洗钱的主力，其中最臭名昭著的莫过于朝鲜 LAZARUS GROUP 黑客组织，给区块链生态安全带来巨大的威胁。

根据开源情报和链上数据分析推测 LAZARUS GROUP 2022 年部分动态如下：

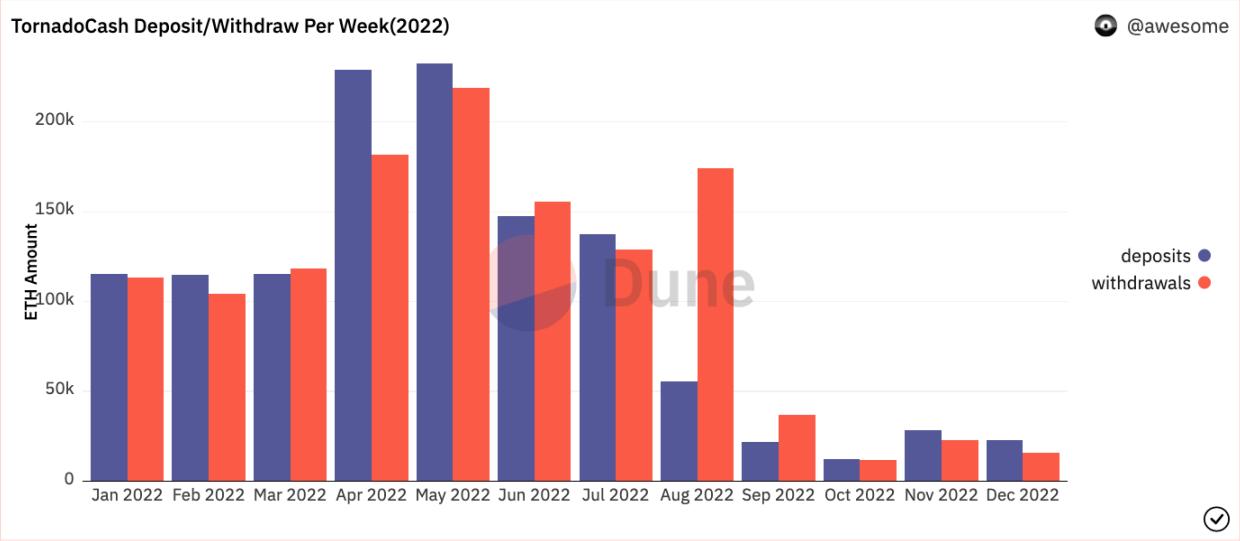
- 1 月 17 日，Crypto.com 的少数用户账户遭到未经授权提款。
- 2 月 8 日，The IRA Financial 的 Gemini 托管账户被恶意提款。
- 3 月 23 日，Ronin Network 跨链桥被盗成为加密货币领域损失最大的黑客攻击事件之一。

在这些与 LAZARUS GROUP 相关的安全事件中，我们可以通过他们成体系的洗钱手法发现他们的痕迹：

- 初期：将 ETH 链上的获利资金全部兑换为 ETH，并将所有的 ETH 分批转入 Tornado.Cash（大量）或者交易平台（少量）。
- 中期：从 Tornado.Cash 分批提款后兑换为 renBTC 代币跨链到 BTC 链。
- 后期：在 BTC 链上，从 renBTC 提款后汇总资金，并进一步转移到 Coinjoin 和混币器。

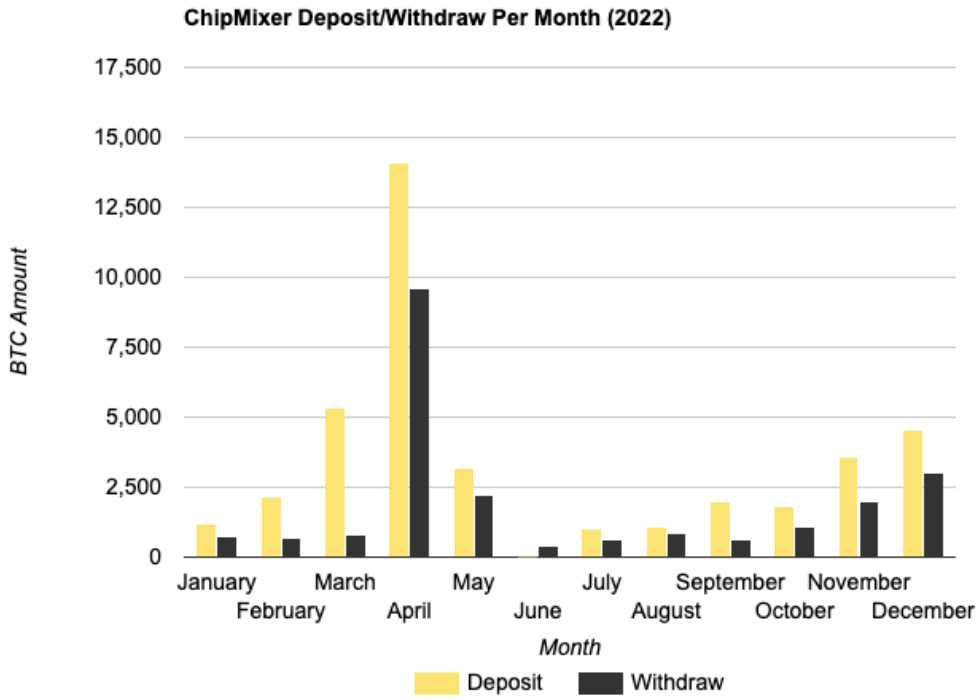
在黑客、黑色产业链、欺诈者和 Rug Pull 项目方洗钱过程中，自然少不了一些洗钱工具的帮忙，常见的洗钱工具有 ETH/BSC 链上的 Tornado.Cash，BTC 链上的 Coinjoin 工具（ChipMixer 等）、混币器（Blender、CryptoMixer 等）、隐私钱包（Wasabi、Samourai 等）、换币平台（ChangeNOW、SimpleSwap、FixedFloat 等）和一些交易平台。

一些常见洗钱工具在 2022 年的存提款数据如下：



（Tornado.Cash 2022 年存款/提款图）

Tornado.Cash：2022 年 用户共计存款 1,233,129 ETH（约 28.29亿美元）到 Tornado.Cash，共计从 Tornado.Cash 提款 1,283,186 ETH(约 28.37 亿美元）。



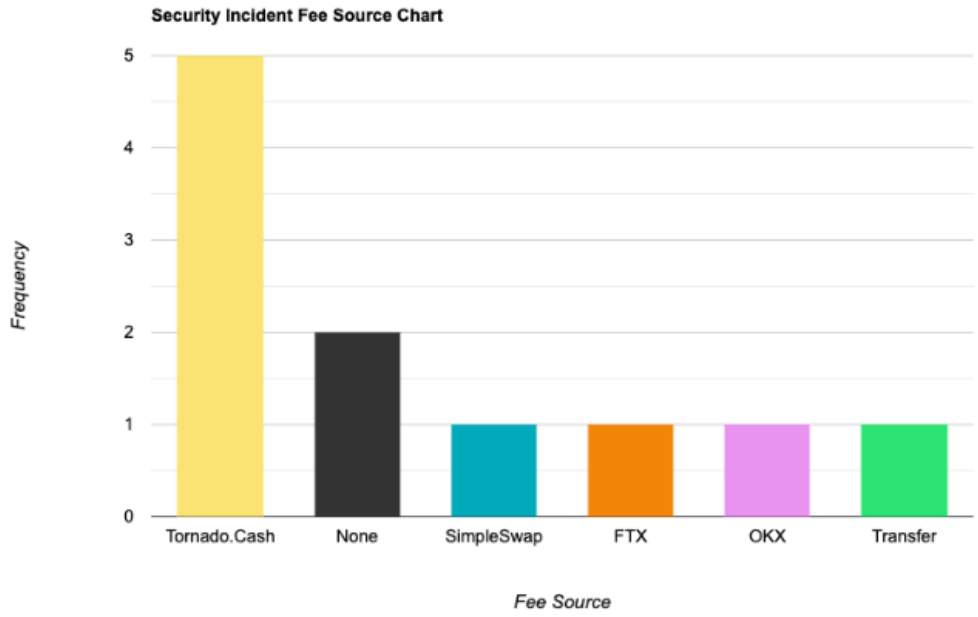
（ChipMixer 2022 年存款/提款图 ）

ChipMixer：2022 年用户共计存款 40,065.33 BTC 到 ChipMixer，共计从 ChipMixer 提款 22,582.44 BTC。

Blender：LAZARUS GROUP 使用此混币器洗 Ronin Network 跨链桥被盗的钱，于 5 月 6 日被美国财政部制裁，目前站点已不可用。

在反洗钱分析过程中，始终存在着几个核心的问题：发起攻击的手续费来自哪里？洗钱的资金去了哪里？我们将通过部分安全事件来探索这两个问题。

发起攻击的手续费来自哪里？



（部分安全事件攻击手续费来源图）

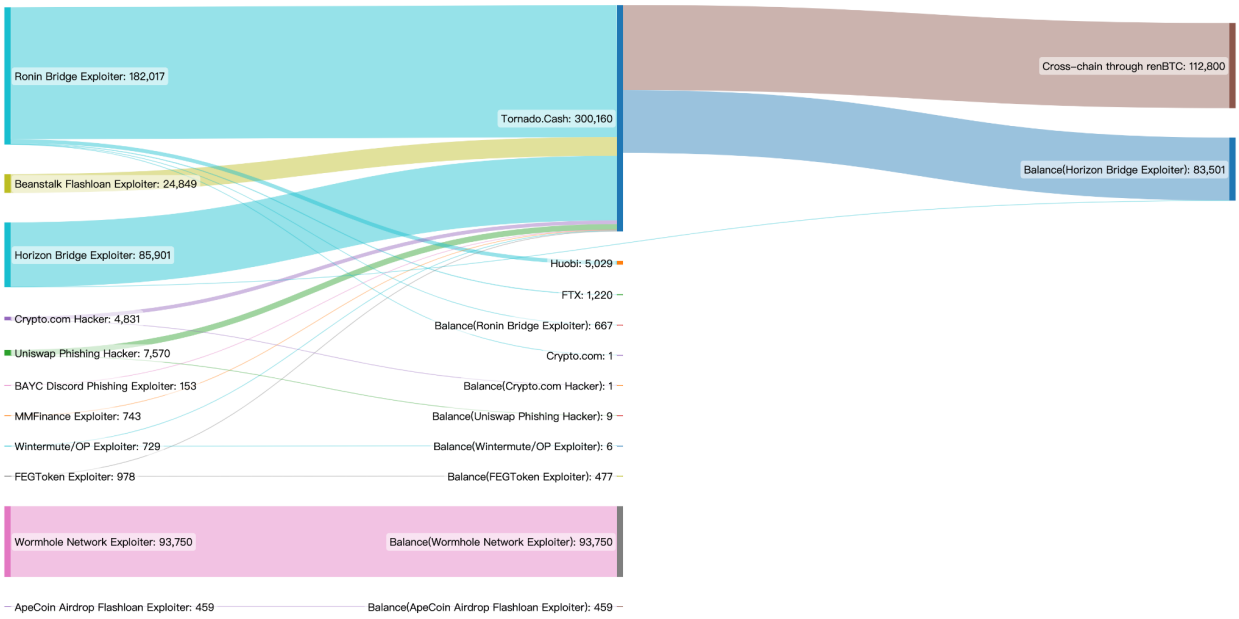
根据部分安全事件攻击手续费来源图，部分安全事件的攻击手续费大多都来自 Tornado.Cash 提款，也有从换币平台、交易平台提款或从其他个人地址转移的情况。

洗钱的资金去了哪里？

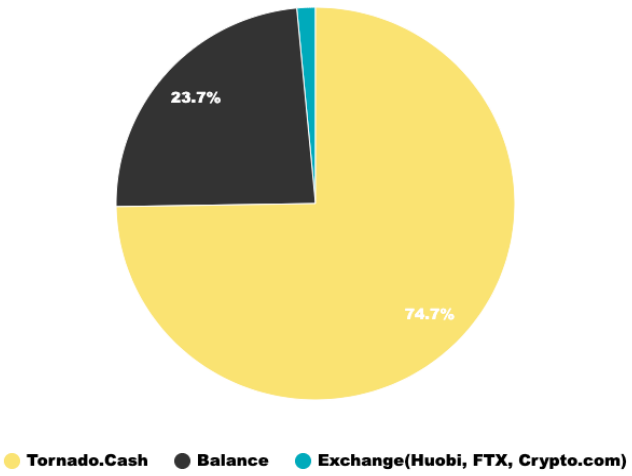
通过对部分安全事件的整体分析，洗钱的主要流程发生在 ETH 链或 BTC 链，如果资金没有在这两条链上，黑客也会考虑将资金跨链到这两条链进一步变现。

通过对部分安全事件被盗资金的 ETH 和 BTC 流向进行分析，得到 ETH/BTC 资金流向图，能够初步评估出洗钱资金的态势。

(1) ETH 资金流向图



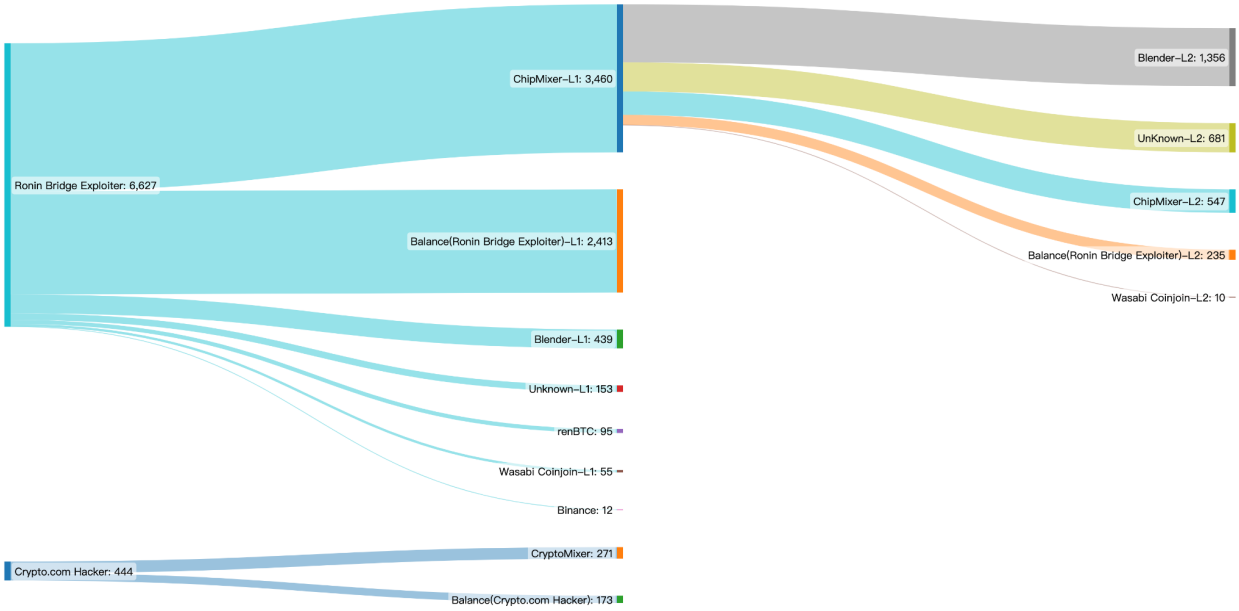
（部分安全事件 ETH 资金流向图）



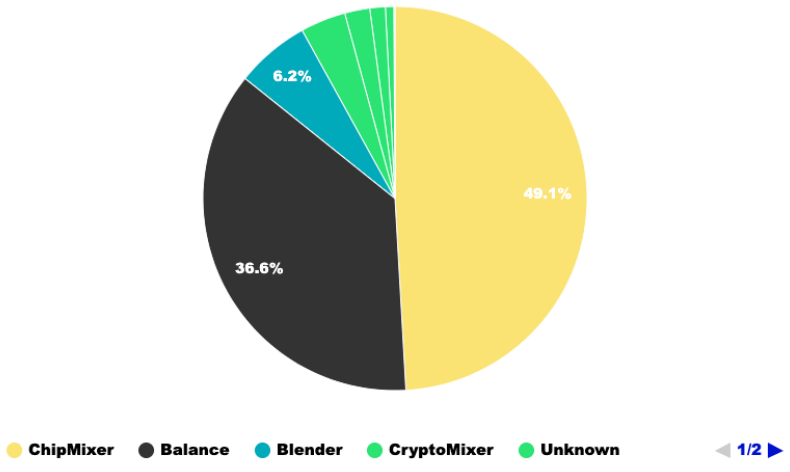
（部分安全事件 ETH 资金流向比例饼图）

根据部分安全事件 ETH 资金流向图，74.6% 洗钱资金流向 Tornado.Cash，资金量高达 300,160 ETH；23.7% 洗钱资金保留在黑客地址，暂未进一步转移，资金量为 95,570 ETH；1.5% 洗钱资金流向交易平台，资金量为 6,250 ETH。

(2) BTC 资金洗钱图



（部分安全事件 BTC 资金流向图 ）



（部分安全事件 BTC 资金流向比例饼图 ）

根据部分安全事件 BTC 资金流向图，48.9% 洗钱资金流向 ChipMixer，资金量高达 3,460 BTC；36.5% 洗钱资金保留在黑客地址，暂未进一步转移，资金量为 2,586 BTC；6.2% 洗钱资金流向 Blender，3.8% 洗钱资金流向 CryptoMixer，2.1% 洗钱资金流向未知主体，1.3% 洗钱资金流向 renBTC，0.7% 洗钱资金流向 Wasabi Coinjoin，0.1% 洗钱资金流向 Binance 交易平台。

二、区块链安全现状

2.1 区块链生态安全概览

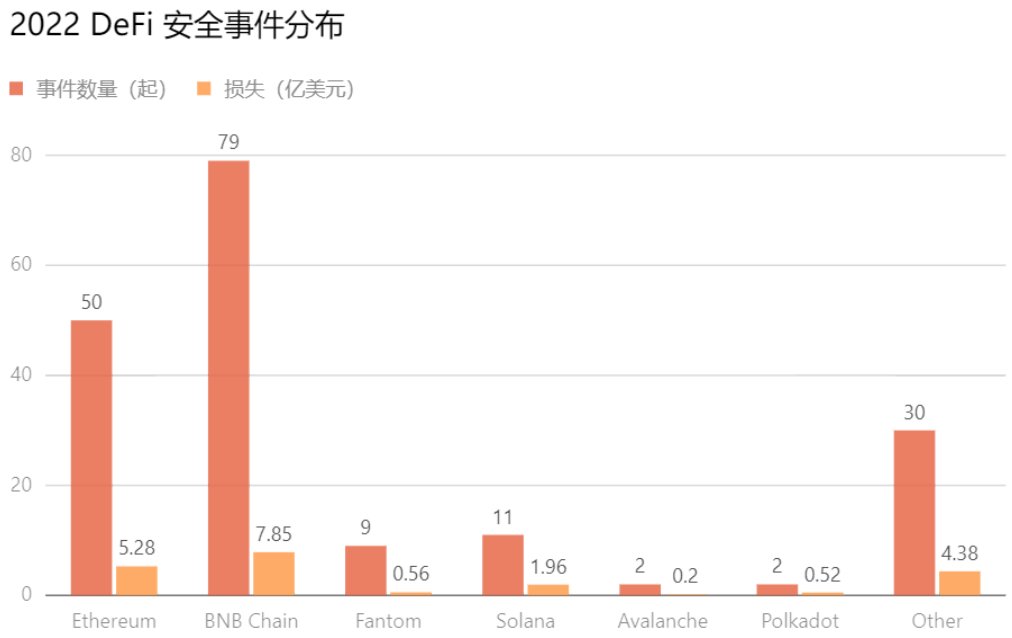
2.1.1 公链

公链是 Web3 领域最重要的基础设施，也是行业中竞争最激烈的赛道之一。而 2022 年最令人讶异的莫过于 Terra 事件了。5 月 8 日，加密货币市场上出现了史上最具破坏性的一次崩盘。Terra 网络的算法稳定币 UST 出现了 2.85 亿美元的巨额抛售，引发了一系列连锁反应。Terra 的原生代币 LUNA 的价格突然毫无征兆的连续跳崖式暴跌，一天时间，LUNA 市值蒸发了近 400 亿美元，全生态项目 TVL 也几乎归零。此次事件或许成为了开启 2022 加密寒冬的死亡按钮。

2.1.2 DeFi / 跨链桥

据 DeFi Llama 数据显示，截止 12 月底，DeFi 总锁仓价值约为 398 亿美元，同比下降 75%。其中 Ethereum 以占比整个 DeFi TVL 的 58.5%（约 233 亿美元）占据主导地位，紧随其后的是 TRON（约 43 亿美元）、BNB Chain（约 42 亿美元）。有趣的是，2022 年 5 月，Ethereum 的 TVL 在 DeFi 中的占比减少了 35%，而 TRON 的 TVL 占比增长了 47%。

根据 SlowMist Hacked 统计，2022 年 DeFi 安全事件共 183 起，损失高达20.75 亿美元，占比 2022 年总损失约 55%。其中 BNBChian 上发生安全事件约 79 起，总损失金额约 7.85 亿美元，居各链平台损失金额第一位。而 Ethereum 上发生安全事件约 50 起，总损失金额约 5.28 亿美元，其次是 Solana 上发生安全事件约 11 起，总损失金额约 1.96 亿美元。



（2022 DeFi 安全事件分布）

跨链桥允许用户将加密资产从一条链转移到另一条链，主要解决多链扩展问题。据 Dune Analytics 的 数据，以太坊跨链桥的锁定总价值（TVL）约 83.9 亿美元，对比上半年降低约 31%。目前 TVL 最高的是 Polygon Bridges（30 亿美元），排名第二的是 Arbitrum Bridges（12.8 亿美元），随后是 Optimism Bridges（8.5 亿美元）。然而，跨链桥智能合约中的大量资金加上缺少安全审计，引来了黑客的目光。

根据 SlowMist Hacked 统计，2022 年跨链桥安全事件共 16 起，损失高达 12.12亿美元，占比 2022 年总损失的 32%。2022 年损失上亿的安全事件共 10 件，跨链桥就占了 4 件，大多是由于私钥泄露导致。

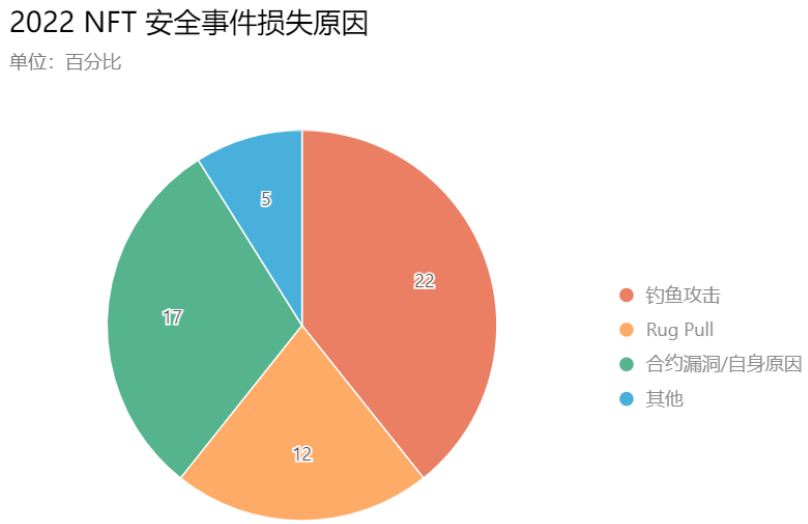
（2022 损失上亿的跨链桥）

总而言之，对项目方来说，想要尽可能的消除漏洞、降低安全风险，就必须做出有效的努力——在项目上线之前，对其进行全面深入的安全审计。同时，建议各项目方通过引入多签机制来加大资产保护的力度。另一方面，各项目在进行协议间交互或移植其他协议的代码时，需充分了解移植协议的架构以及自己项目的架构设计，做好协议之间的兼容性，防止资金损失情况的发生。对用户来说，随着区块链领域的玩法愈发多样化，用户在进行投资前认真了解项目背景，查看该项目是否有开源、是否经过审计，在参与项目时需要提高警惕，注意项目风险。

2.1.3 NFT

NFT 在 2022 年表现极为抢眼，据NFTScan 数据显示，截止 12 月底，在以太坊上的NFT 全年交易次数达 1.98 亿次，明显高于 2020 年和 2021 年。而在 BNBChain 上的 NFT 全年交易次数达 3.45 亿次，在 Polygon 上的 NFT 全年交易次数达 7.93 亿次。

另一方面，根据 SlowMist Hacked 不完全统计，2022 年 NFT 赛道安全事件约 56起，损失超 6544 万美元，其中大部分是由钓鱼攻击导致，占比约为 39%（22 起），其次是 Rug Pull 占比约为 21%（12 起），由合约漏洞或自身原因导致占比 30%（17 起）。



（2022 NFT 安全事件损失原因分布图）

2.1.4 钱包 / 交易平台

2 月 8 日，美国司法部（DOJ）发布公告称，已经查获了价值 36 亿美元的比特币，这些比特币与 2016 年加密货币交易所 Bitfinex 的黑客事件有关。34 岁的 Ilya Lichtenstein 和其 31 岁的妻子 Heather Morgan 在纽约被捕，两人被指控共谋洗钱和诈骗罪。这也是美国司法部有史以来最大规模的金融扣押。

11 月 6 日，币安创始人 CZ 发推 称决定清算账面上所有剩余的 FTT，由此引发两大交易所之间的对峙。尽管 Alameda CEO 和 FTX CEO SBF 接连发推试图稳固用户信心并辟谣此前曝光的消息，但还是引发 FTX 在流动性枯竭后迅速破产。最终，FTX 暴雷，SBF 被捕。中心化交易所的不透明再度引发人们的信任危机，缺乏审慎监管的问题越发凸显。无论是对消费者更严格的保护，还是对机构更明确的规则，监管的脚步都将愈发清晰。

在 FTX 暴雷后，硬件钱包的销量大幅增长，用户量最多的钱包 MetaMask 月活用户达 3000 万。根据 Finbold 数据显示，基于排名前 21 个加密货币存储 APP 应用，在 2022 年 1月至 2022 年 10 月期间，Android 和 iOS 设备上的加密钱包下载量已经达到约 1.0206 亿次。虽然这个数字低于 2021 年牛市期间的 1.7785 亿次下载量，但比除 2021 年之外的任何一年都高。按月细分数据显

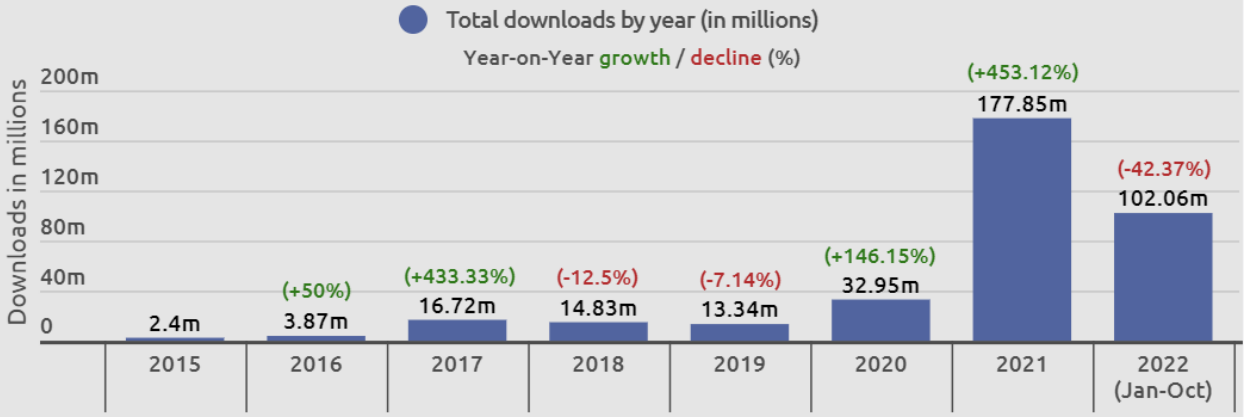
示，加密钱包下载量年初呈下降趋势，但在 Terra/Luna 崩溃以及 FTX 暴雷后均出现较大幅度增长。

Crypto Wallet App Downloads Worldwide* (2015-2022)

(from January 2015 to October 2022)

Details: Estimated number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from January 2015 to October 2022. The numbers provided are estimates based on wallets available worldwide, and may not necessarily include wallets that are popular in a specific country. The data presented include download figures for both Android and iOS devices.

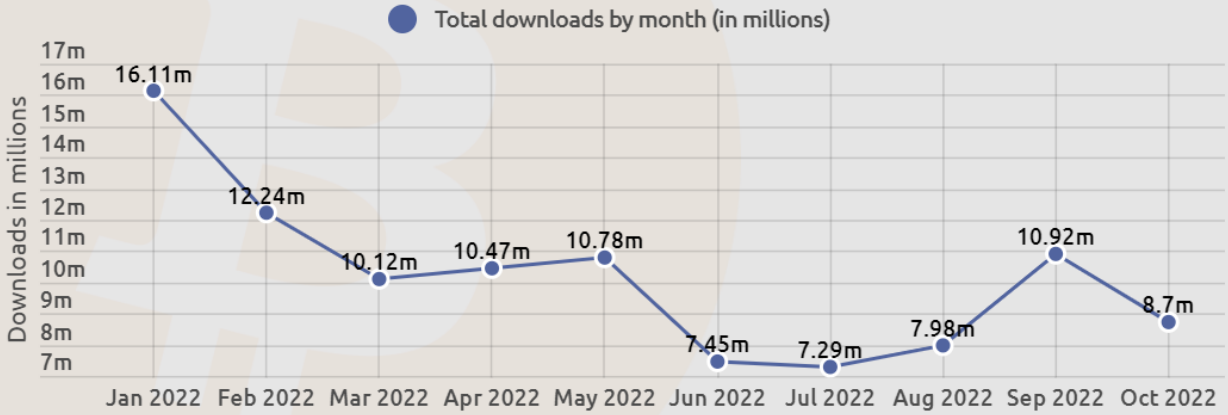
Sources: Statista, Finbold, AppMagic



*Supplementary note: The following apps include in the list: ABNB Coin Wallet; Binance; Bitcoin & Crypto DeFi Wallet; Bitcoin Wallet; Blockchain.com Wallet; BRD Bitcoin Wallet; BTC Coin Wallet; Coinbase; Coinbase Wallet; Coinomi; CoinSwitch; Crypto.com l DeFi Wallet; Dogecoin Wallet; Enjin Wallet; Exodus Wallet; MetaMask Wallet; Satoshi Wallet; Status Wallet; Sweat Wallet; Trust Wallet; Wirex Wallet.

Crypto Wallet App Downloads Worldwide in 2022 (by Month)

Details: Estimated number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from January 2022 to October 2022. The numbers provided are estimates based on wallets available worldwide, and may not necessarily include wallets that are popular in a specific country. The data presented include download figures for both Android and iOS devices.



2.1.5 其他

区块链技术不可逆、匿名性特征在有效保护隐私的同时，也为网络犯罪提供了“保护伞”。随着元宇宙、NFT 等概念受到热捧，加密货币盗窃事件、欺诈事件时有发生，很多不法分子打着区块链旗号发行所谓的虚拟资产，实施诈骗，黑灰产的先进与专业度已经远超想象。

据中国人民银行支付结算司 数据，2021 年涉诈款项的支付方式中，利用加密货币进行支付仅次于银行转账，排名第二位，高达 7.5 亿美元；而 2020 年、2019 年仅为 1.3、0.3 亿美元，逐年大幅增长的趋势明显。值得关注的是，加密货币转账在“杀猪盘”诈骗中增长迅速。2021 年“杀猪盘”诈骗资金中 1.39 亿美元使用加密货币支付，是 2020 年的 5 倍、2019 年的 25 倍。

根据美国联邦贸易委员会（FTC）发布的一份报告，在自 2021 年年初以来的一年多时间里，已有超过 4.6 万人报告自己遭遇了 加密货币骗局，损失总额超过 10 亿美元。根据 FTC Consumer Sentinel Network 的欺诈报告，最常见的加密货币骗局类型是投资相关欺诈，在总金额 10 亿美元中占 5.75 亿美元，最常向诈骗者支付的加密货币包括 BTC(70%)、USDT(10%) 和 ETH(9%)。

对于个人用户来说，遵守以下安全法则及原则，可以避免大部分风险：

两大安全法则：

- 零信任。简单来说就是保持怀疑，而且是始终保持怀疑。
- 持续验证。你要相信，你就必须有能力去验证你怀疑的点，并把这种能力养成习惯。

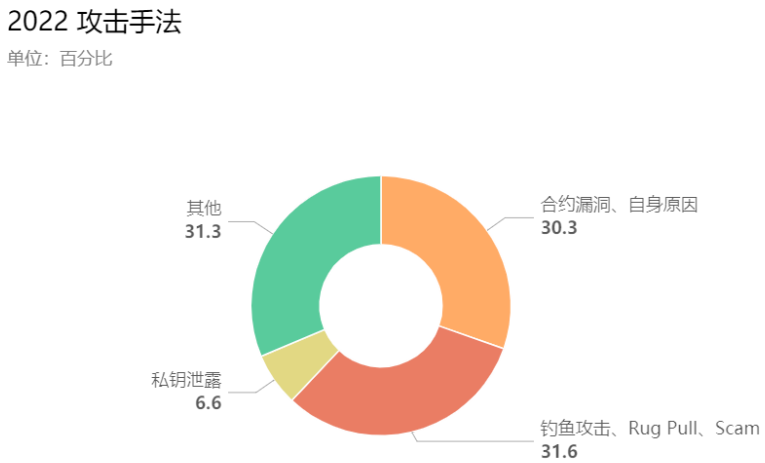
安全原则：

- 网络上的知识，凡事都参考至少两个来源的信息，彼此佐证，始终保持怀疑。
- 做好隔离，也就是鸡蛋不要放在一个篮子里。
- 对于存有重要资产的钱包，不做轻易更新，够用就好。
- 所见即所签。即你看到的内容就是你预期要签名的内容，当你签名发出去后，结果就应该是你预期的，绝不是事后拍断大腿的。
- 重视系统安全更新，有安全更新就立即行动。
- 不乱下程序。

在此，十分推荐阅读并掌握《区块链黑暗森林自救手册》。

2.2 攻击手法

303 起安全事件中，攻击手法主要分为三类：由项目自身设计缺陷和各种合约漏洞引起的攻击；包含 Rug Pull、钓鱼、Scam 类型的手法；由私钥泄露引起的资产损失。



（2022 攻击手法对比图）

2022 年最常见的攻击手法是由项目自身设计缺陷和各种合约漏洞引起，约 92 起，造成损失近 11 亿美元。其中较为主要的是利用闪电贷引起的攻击，约 33 起，造成损失 3.48 亿美元，其他包括重入问题、价格操纵、验证问题等等。

因私钥被盗引起的资产损失发生率约为 6.6%，损失金额却达到 7.62 亿美元。因私钥被盗的事件中，损失最大的来自 Ronin 事件，其次是 Harmony，都是来自跨链桥。

在 Web3 世界，用户的安全意识往往是参差不齐，这也导致了针对用户的钓鱼攻击花样多多且频繁发生。例如，攻击者利用恶意手段将各项目的官方媒体平台（如 Discord、Twitter）占为己有或者伪造官方媒体号并发布钓鱼 Mint、AirDrop 链接，还时不时转发真正的官方号内容来混肴视听。例如，利用搜索引擎上的广告宣传虚假网站或者与官方域名高度相似的域名及内容来以假乱真；例如通过伪造的邮件、吸引人的赠品活动来引你入局；又例如利用新用户信息差提供假APP下载链接。无论如何，提高安全意识才是最必要的，同时，一旦发现自己中招，第一时间转移资产，及时止损并保留证据，必要时寻求业内安全机构的帮助。

其次，最令人憎恶的则是 Rug Pull。Rug Pull 通常指项目的开发者放弃项目，带着资金逃跑，更多是项目方主动作恶。它可以以多种方式发生：比如当开发者启动初始流动性，推高价格，然后撤回流动性项目方先创建一个加密项目，通过各种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，投资该项目的用户也将蒙受巨大损失。再比如推出一个网站，在吸引了数十万存款后关闭。2022 年 RugPull 事件达到 51 起，损失约 1.88 亿美元，常发生于 BSC 生态及 NFT 领域。

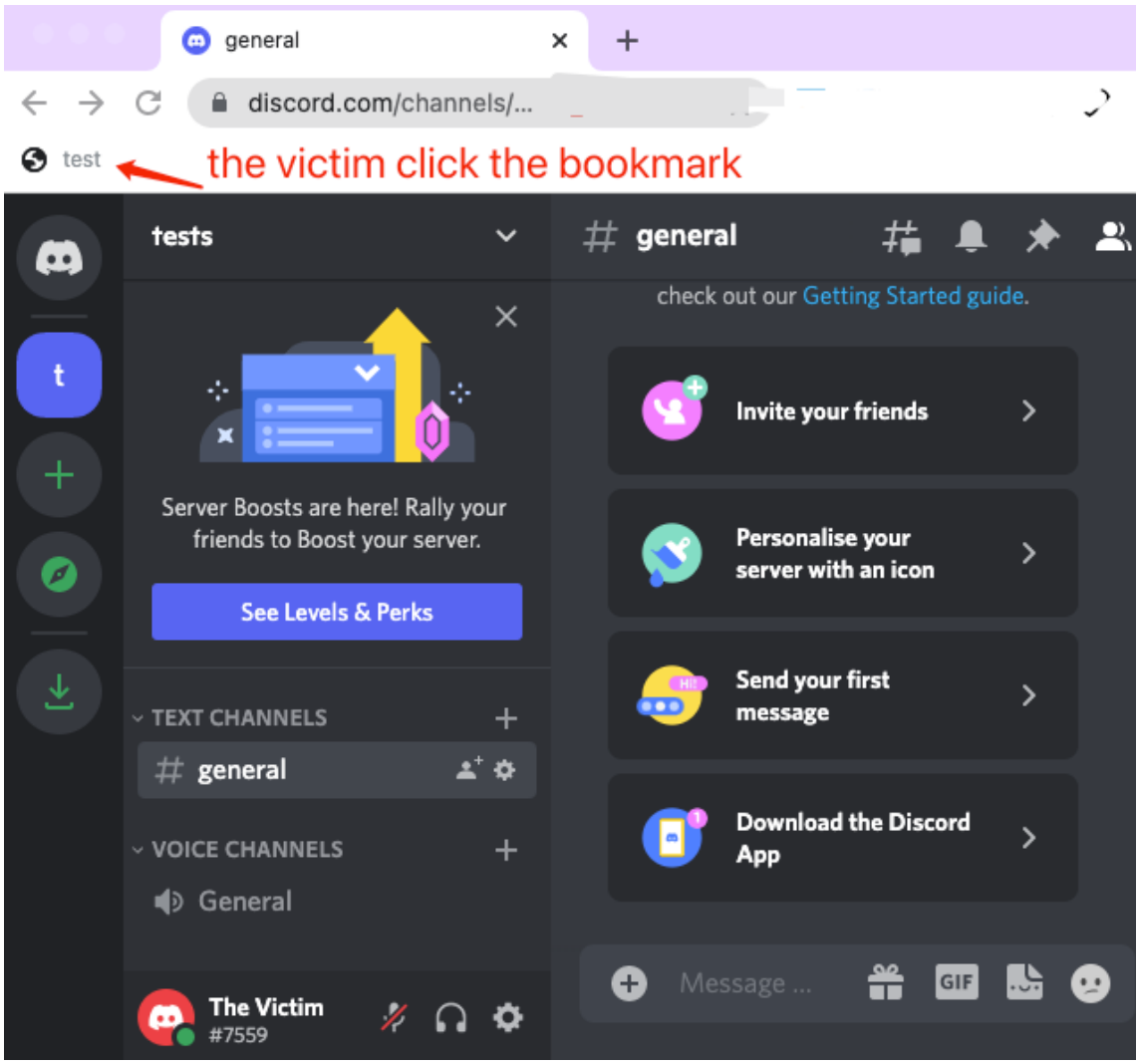
2022 年其他较为新型的手法为前端恶意攻击、DNS 攻击以及 BGP 劫持；最为奇葩的则是人为配置操作失误导致的资产损失。

2.3 钓鱼/骗局手法

此节只选取部分 SlowMist 曾披露过的钓鱼/骗局手法。

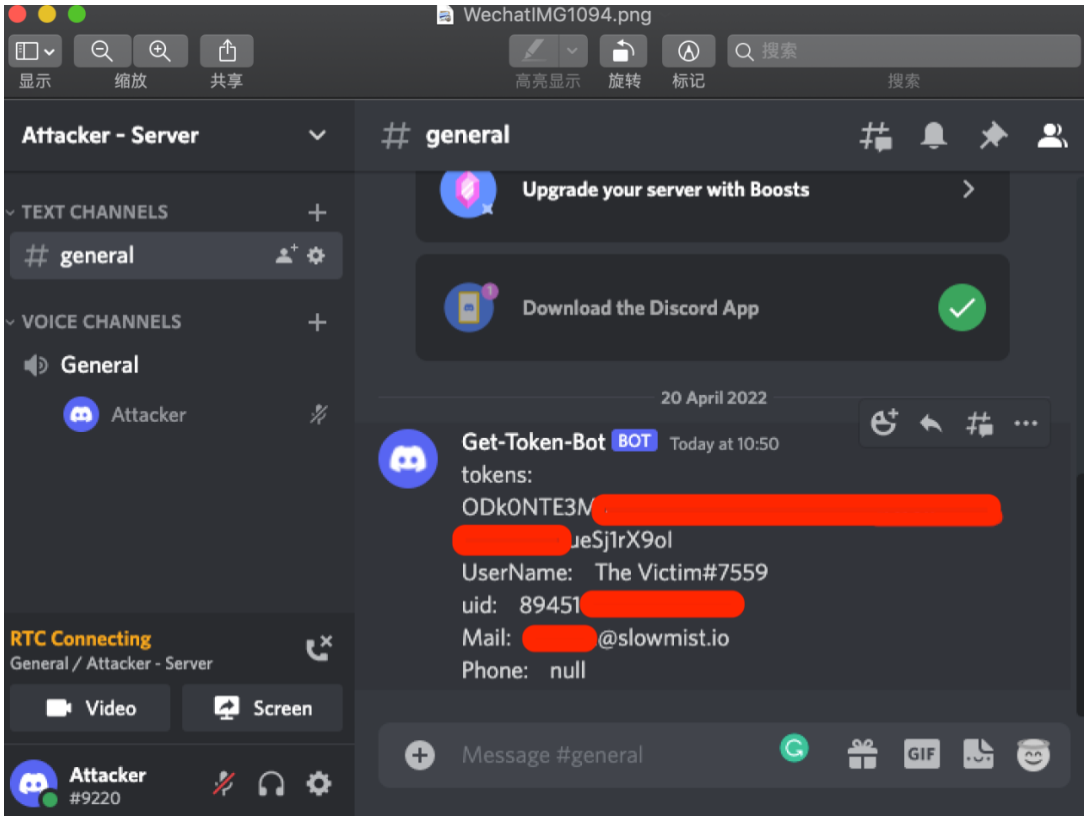
2.3.1 浏览器恶意书签盗取 Discord Token

现在的浏览器都有自带的书签管理器，在提供便利的同时也容易被攻击者利用。通过精心构造恶意的钓鱼页面可以让你收藏的书签中插入一段 JavaScript 代码，有了这个几乎可以做任何事情，包括通过 Discord 封装好的 webpackChunkdiscord_app 前端包进行信息获取。当 Discord 用户点击时，恶意 JavaScript 代码就会在用户所在的 Discord 域内执行，盗取 Discord Token，攻击者获得项目方的 Discord Token 后就可以直接自动化接管项目方的 Discord 账户相关权限。攻击者拿到了 Token 等同于登录了 Discord 账号，可以做登录 Discord 的任何同等操作，比如建立一个 Discord webhook 机器人，在频道里发布公告等虚假消息进行钓鱼。下面是演示受害者点击了钓鱼的书签：



（恶意书签钓鱼演示图）

下面是演示攻击者编写的 JavaScript 代码获取 Token 等个人信息后，通过 Discord Server 的 webhook 接收到。



（恶意书签钓鱼演示图）

可以看到，在用户登录 Web 端 Discord 的前提下，假设受害者在钓鱼页面的指引下添加了恶意书签，在 Discord Web 端登录时，点击了该书签，触发恶意代码，受害者的 Token 等个人信息便会通过攻击者设置好的 Discord webhook 发送到攻击者的频道上。

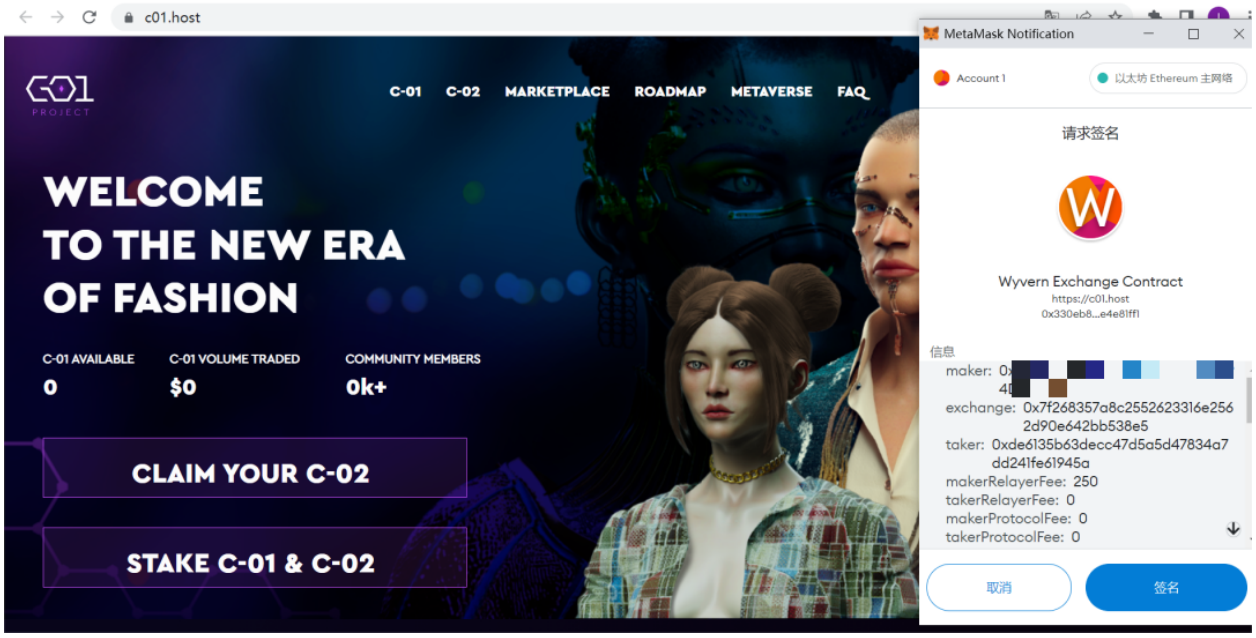
2.3.2 “零元购” NFT 钓鱼

例如下图钓鱼网站，签名内容为

Maker：用户地址

Taker：0xde6135b63decc47d5a5d47834a7dd241fe61945a

Exchange：0x7f268357A8c2552623316e2562D90e642bB538E5（OpenSea V2 合约地址）



（"零元购"钓鱼演示图）

这是一种较为常见的 NFT 钓鱼方式，骗子能够以 0 ETH（或任何代币）购买你所有授权的 NFT。也就是说，这是欺骗用户签名 NFT 的销售订单，NFT 是由用户持有的，一旦用户签名了此订单，骗子就可以直接通过 OpenSea 购买用户的 NFT，但是购买的价格由骗子决定，也就是说骗子不花费任何资金就能"买"走用户的 NFT。

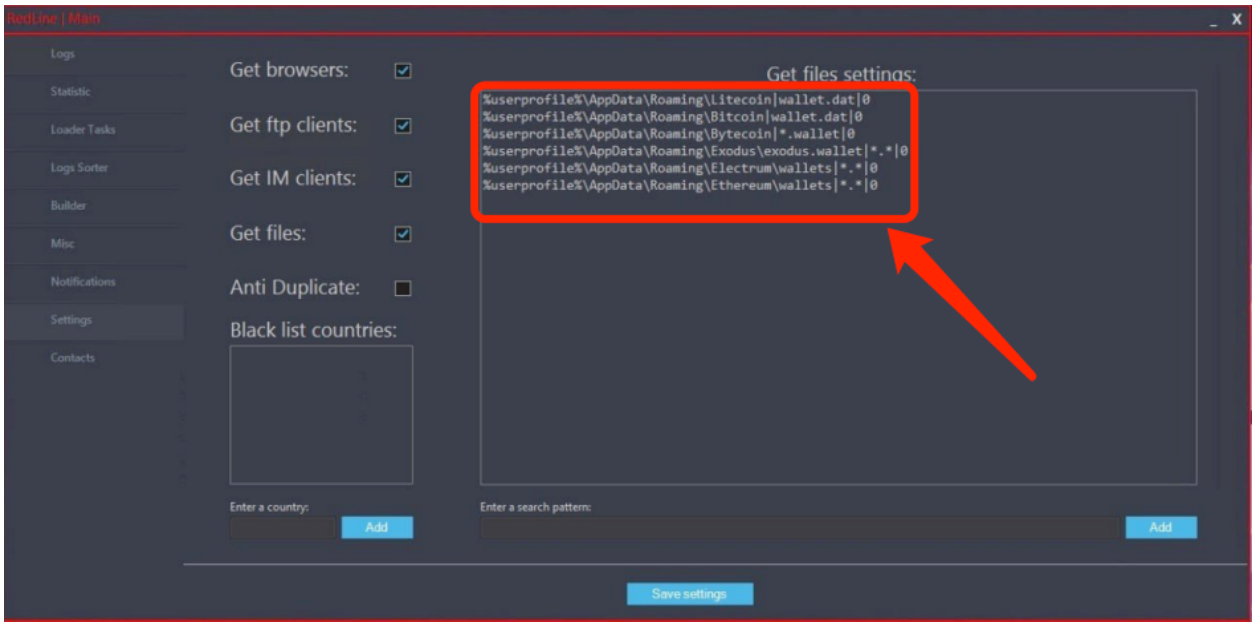
此外，签名本身是为攻击者存储的，不能通过 Revoke.Cash 或 Etherscan 等网站取消授权来废弃签名的有效性，但可以取消你之前的挂单授权，这样也能从根源上避免这种钓鱼风险。

2.3.3 Redline Stealer 木马盗币

这种攻击主要是通过 Discord 邀请用户参与新的游戏项目内测，打着"给予优惠"等幌子，或是通过群内私聊等方式发一个程序让你下载，一般是发送压缩包，解压出来是一个大概 800 M 左右的 exe 文件，一旦你在电脑上运行，它会扫描你电脑上的文件，然后过滤包含 Wallet 等关键词的文件上传到攻击者服务器，达到盗取加密货币的目的。

RedLine Stealer 是一种恶意木马软件，2020 年 3 月被发现，在地下论坛上单独出售。该恶意软件从浏览器中收集保存的凭据、自动完成数据和信用卡等信息。在目标机器上运行时，会搜集如用户名、位置数据、硬件配置和已安装的安全软件等详细信息。 新版本的 RedLine 增加了窃取加密

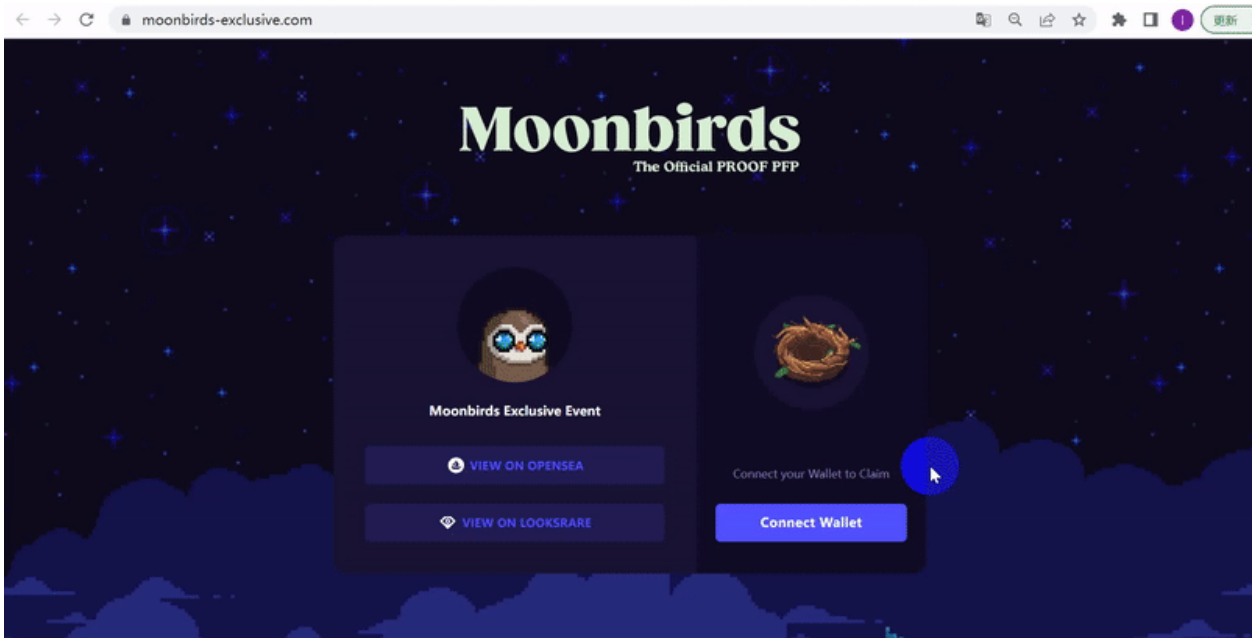
货币的能力，能够自动扫描本地计算机已安装的数字货币钱包信息，并上传到远端控制机。该恶意软件具有上传和下载文件、执行命令以及定期发回有关受感染计算机的信息的能力。常常针对加密货币钱包目录、钱包文件进行扫描：



（RedLine Stealer 木马盗币演示图）

2.3.4 空白支票 eth_sign 钓鱼

连接钱包后并点击 Claim 后，弹出一个签名申请框，同时 MetaMask 显示了一个红色提醒警告，而光从这个弹窗上无法辨别要求签名的到底是什么内容。其实这是一种非常危险的签名类型，基本上就是以太坊的"空白支票"。通过这个钓鱼，骗子可以使用您的私钥签署任何交易。这种 eth_sign 方法可以对任意哈希进行签名，那么自然可以对我们签名后的 bytes32 数据进行签名。因此攻击者只需要在我们连接 DApp 后获取我们的地址对我们账户进行分析查询，即可构造出任意数据（如：native 代币转账，合约调用）让我们通过 eth_sign 进行签名。

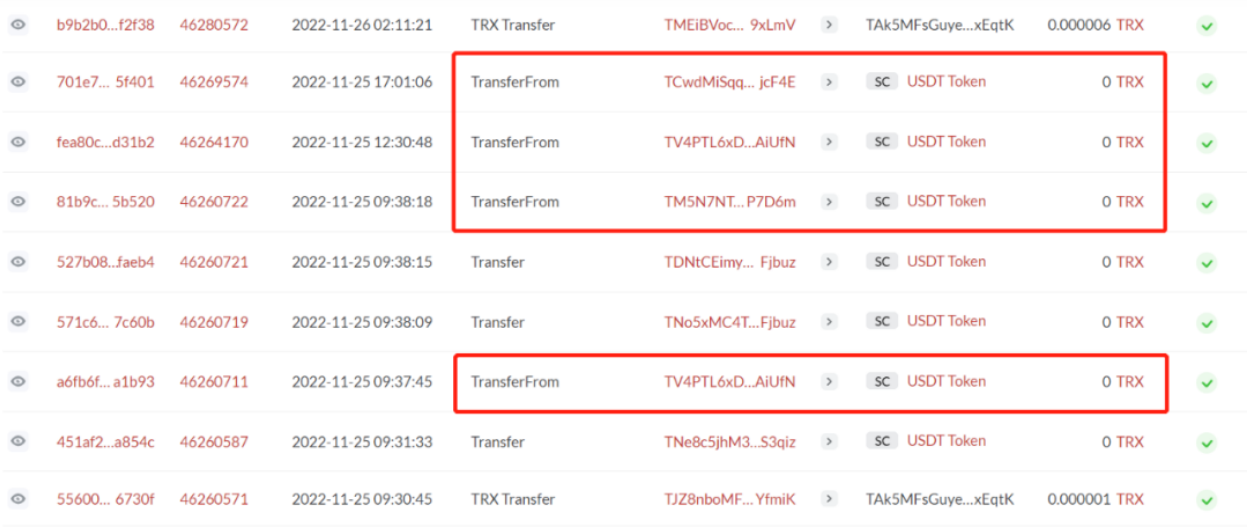


（eth_sign 钓鱼演示图）

这种钓鱼方式对用户会有很强的迷惑性，以往我们碰到的授权类钓鱼在 MetaMask 会给我直观的展示出攻击者所要我们签名的数据。而当攻击者使用 eth_sign 方法让用户签名时，MetaMask 展示的只是一串 bytes32 的哈希。

2.3.5 尾号相同 + TransferFrom 零转账骗局

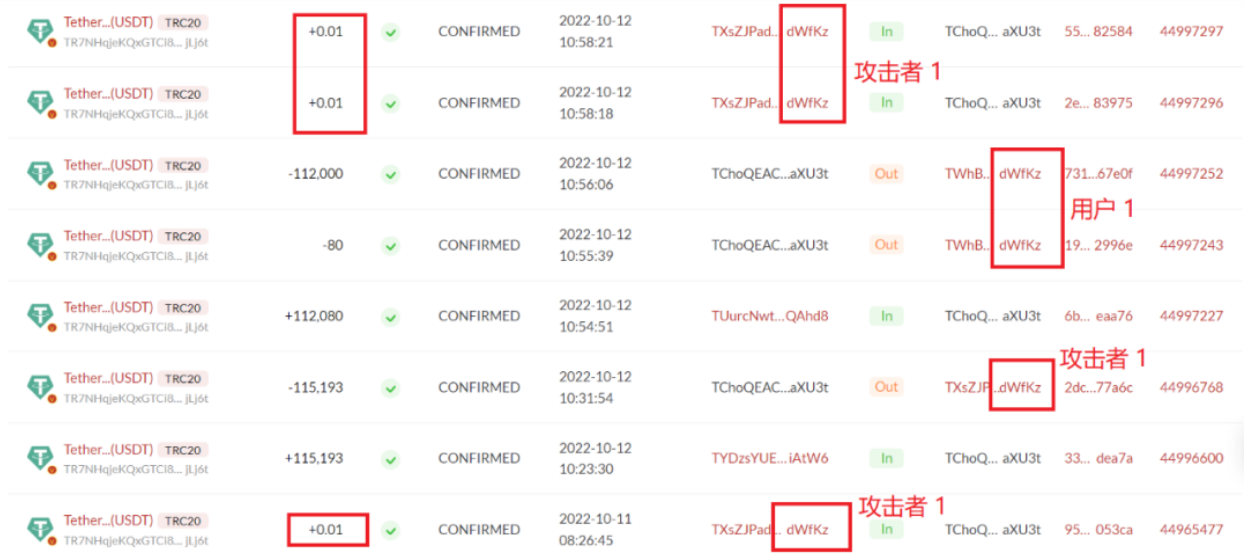
用户的钱包地址转账记录中不断出现陌生地址转账 0 USDT，而这笔交易均是通过调用 TransferFrom 函数完成的。究其原因主要是代币合约的 TransferFrom 函数未强制要求授权转账数额必须大于 0，因此可以从任意用户账户向未授权的账户发起转账 0 的交易而不会失败。恶意攻击者利用此条件不断地对链上活跃用户发起 TransferFrom 操作，以触发转账事件。



b9b2b0...f2f38	46280572	2022-11-26 02:11:21	TRX Transfer	TMEiBVoc... 9xLmV	TAk5MFsGuye...xEqtK	0.000006 TRX	
701e7... 5f401	46269574	2022-11-25 17:01:06	TransferFrom	TCwdMiSqq... jcF4E	SC USDT Token	0 TRX	
fea80c...d31b2	46264170	2022-11-25 12:30:48	TransferFrom	TV4PTL6xD...AiUfN	SC USDT Token	0 TRX	
81b9c... 5b520	46260722	2022-11-25 09:38:18	TransferFrom	TM5N7NT... P7D6m	SC USDT Token	0 TRX	
527b08...faeb4	46260721	2022-11-25 09:38:15	Transfer	TDNtCEimy... Fjbuz	SC USDT Token	0 TRX	
571c6... 7c60b	46260719	2022-11-25 09:38:09	Transfer	TNo5xMC4T...Fjbuz	SC USDT Token	0 TRX	
a6fb6f... a1b93	46260711	2022-11-25 09:37:45	TransferFrom	TV4PTL6xD...AiUfN	SC USDT Token	0 TRX	
451af2...a854c	46260587	2022-11-25 09:31:33	Transfer	TNe8c5jhM3...S3qiz	SC USDT Token	0 TRX	
55600... 6730f	46260571	2022-11-25 09:30:45	TRX Transfer	TJZ8nboMF... YfmiK	TAk5MFsGuye...xEqtK	0.000001 TRX	

（TransferFrom 交易演示图）

除了 0 USDT 转账骚扰，还伴随着攻击者针对交易规模较大频率较高的用户不断空投小额数量的 Token（例如 0.01 USDT 或 0.001 USDT 等），攻击者地址尾数和用户地址尾数几乎一样，通常为后几位，用户去复制历史转账记录中的地址时一不小心就复制错，导致资产损失。



Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	+0.01	CONFIRMED	2022-10-12 10:58:21	TXsZJPad...dWfKz	In	TChoQ... aXU3t	55... 82584	44997297
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	+0.01	CONFIRMED	2022-10-12 10:58:18	TXsZJPad...dWfKz	In	TChoQ... aXU3t	2e... 83975	44997296
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	-112,000	CONFIRMED	2022-10-12 10:56:06	TChoQEAC...aXU3t	Out	TWhB...dWfKz	731...67e0f	44997252
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	-80	CONFIRMED	2022-10-12 10:55:39	TChoQEAC...aXU3t	Out	TWhB...dWfKz	19... 2996e	44997243
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	+112,080	CONFIRMED	2022-10-12 10:54:51	TUurcNwt...QAhd8	In	TChoQ... aXU3t	6b... eaa76	44997227
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	-115,193	CONFIRMED	2022-10-12 10:31:54	TChoQEAC...aXU3t	Out	TXsZJP...dWfKz	2dc...77a6c	44996768
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	+115,193	CONFIRMED	2022-10-12 10:23:30	TYDzsYUE...iAtW6	In	TChoQ... aXU3t	33... dea7a	44996600
Tether...(USDT) TRC20 TR7NHqjeKQxGTCi8... jtJ6t	+0.01	CONFIRMED	2022-10-11 08:26:45	TXsZJPad...dWfKz	In	TChoQ... aXU3t	95... 053ca	44965477

（尾号相同钓鱼演示图）

小节 2.2 与 2.3 只是举例了一些常见的攻击手法和场景，实际上道高一尺魔高一丈，黑客的攻击手法永远都在推陈出新，我们能做的就是不断提高自己的见识。

2.4 损失 Top10 安全事件

此节选取了 2022 年损失 Top10 的安全事件。

2.4.1 Ronin Network 损失超 6.1 亿美元

3 月 29 日，Axie Infinity 侧链 Ronin Network 发布 社区预警，Ronin Network 出现安全漏洞，共 17.36 万枚 ETH 和 2550 万枚 USDC 被盗，损失超 6.1 亿美元。据官方发布的信息，攻击者使用被黑的私钥来伪造提款，仅通过两次交易就从 Ronin bridge 中抽走了资金。值得注意的是，黑客事件早在 3 月 23 日就发生了，但官方据称是在用户报告无法从 bridge 中提取 5k ETH 后才发现这次攻击。本次事件的损失甚至高于去年的 PolyNetwork 被黑事件，后者也窃取了超过 6 亿美元。事情背景可追溯到去年 11 月，当时 Sky Mavis 请求 Axie DAO 帮助分发免费交易。由于用户负载巨大，Axie DAO 将 Sky Mavis 列入白名单，允许 Sky Mavis 代表其签署各种交易，该过程于 12 月停止。但是，对白名单的访问权限并未被撤销，这就导致一旦攻击者获得了 Sky Mavis 系统的访问权限，就能够通过 gas-free RPC 从 Axie DAO 验证器进行签名。Sky Mavis 的 Ronin 链由九个验证节点组成，其中至少需要五个签名来识别存款或提款事件。攻击者通过 gas-free RPC 节点发现了一个后门，最终攻击者设法控制了五个私钥，其中包括 Sky Mavis 的四个 Ronin 验证器和一个由 Axie DAO 运行的第三方验证器。美国调查机构认为朝鲜黑客组织 LAZARUS GROUP 是此事件的幕后黑手。

2.4.2 BNBChain 遭到漏洞利用

10 月 7 日，BNB Chian 跨链桥 BSC Token Hub 遭 攻击。黑客利用跨链桥漏洞分两次共获取 200 万枚 BNB，超 5.7 亿美元。根据安全研究员Samczsun的 推文，攻击根本原因是攻击者找到了 为特定区块伪造证明的方法。

2.4.3 Wormhole 损失超 3 亿美元

2 月 3 日，攻击者利用 Wormhole 网络中的签名验证漏洞在 Solana 上铸造了 12 万 WETH，价值超 3.26 亿美元。Wormhole 发布针对该事件的报告 中指出，此次事件中 Wormhole 的漏洞具体是 Solana 端核心 Wormhole 合约的签名验证代码存在错误，允许攻击者伪造来自“监护人”的消息来铸造 Wormhole 的 WETH。本次事件是目前针对 Solana 的黑客攻击中造成的最大损失规模事件。

2.4.4 Beanstalk Farms 遭闪电贷和提案攻击

4 月 17 日，基于以太坊的算法稳定币项目 Beanstalk Farms 遭 攻击，损失约为 1.82 亿美元。本次攻击的主要原因在于提案的投票与执行两阶段间无时间间隔，导致攻击者在完成投票后未经社区审核可以直接执行恶意提案。有趣的是，攻击者将其中 25 万美元捐赠给了一个用于为乌克兰政府筹集捐款的地址。

2.4.5 Wintermute 损失 1.6 亿美元

9 月 20 日，加密做市商 Wintermute 创始人兼首席执行官 EvgenyGaevoy 发推，称 Wintermute 在 DeFi 黑客攻击中损失 1.6 亿美元，Wintermute 为了优化手续费使用了 Profanity 来创建钱包，在得知 Profanity 存在漏洞后，他们开始转移旧地址的资金，但由于内部（人为）错误，调用了错误的函数，致使遭受攻击。

2.4.6 Nomad 桥遭受黑客攻击

8 月 2 日，跨链互操作协议 Nomad 桥遭受黑客 攻击，本次攻击是由于 Nomad 桥 Replica 合约在初始化时可信根被设置为 0x0，且在进行可信根修改时并未将旧根失效，导致了攻击可以构造任意消息对桥进行资金窃取，攻击者能够从攻击中榨取超过 1.9 亿美元的价值。到目前为止，已有 40 多个地址向 Nomad 返还了超过 3600 万美元。

2.4.7 Elrond 出现安全漏洞

6 月 5 日，区块链网络 Elrond 疑似出现安全 漏洞，黑客“凭空获得”了近 165 万 $EGLD，并且通过去中心化交易所 Maiar 抛售。6 月 8 日，Elrond 创始人兼首席执行官 Beniamin Mincu 发推表示，此前的 Bug 已经解决，所有的资金和用户都是安全的，几乎所有被盗取的资金都已被追回。

2.4.8 Mango 因价格操纵被提取 1 亿 美元

10 月 12 日，Solana 生态去中心化金融平台 Mango 发推 称：“目前正在调查一起黑客通过预言机价格操纵从 Mango 中提取资金的事件。”根据详细报告，该协议大约于北京时间 10 月 12 日 6:00 遭遇攻击，2 个由 USDC 提供资金的账户在 MNGO-ERP 中持有过高的头寸，各个交易所（FTX、Ascendex）的 MNGO/USD 底层价格在几分钟内出现了 5-10 倍的价格上涨，导致 Switchboard 和 Pyth 预言机将其 MNGO 基准价格更新为 0.15 美元以上，进一步导致未实现的利润使做多 MNGO-ERP 的账户价值按市价计算增加，允许账户从 Mango 协议中借入和提取 BTC (sollet)、USDT、SOL、mSOL、USDC，使得平台上 1.9 亿美元等值存款的借贷额度达到了最大值，当时该账户提取的净值约为 1 亿美元。

2.4.9 Harmony 损失超 1 亿美元

6 月 24 日，Harmony Horizon bridge 遭到黑客 攻击 。经慢雾 MistTrack 分析，攻击者获利超 1 亿美元，包括 11 种 ERC20 代币、13,100 ETH、5,000 BNB 以及 640,000 BUSD。26 日 Harmony 创始人 Stephen Tse 在 Twitter 上表示，Horizon 被攻击并非因为智能合约漏洞，而是由私钥泄露导致。虽然 Harmony 对私钥进行了加密存储，但攻击者还是解密了其中部分私钥并签名了一些未经授权的交易。

2.4.10 Qubit 遭攻击损失 8000 万美元

BSC 生态去中心化借贷项目 QBridge 旗下借贷产品 Qubit 遭到黑客攻击，黑客铸造大量 xETH 抵押品并消耗了资金池中约 8000 万美元资产。据慢雾分析，本次攻击的主要原因在于在充值普通代币与 native 代币分开实现的情况下，在对白名单内的代币进行转账操作时未对其是否是 0 地址再次进行检查，导致本该通过 native 充值函数进行充值的操作却能顺利走通普通代币充值逻辑。

三、Top10 安全事件反洗钱分析

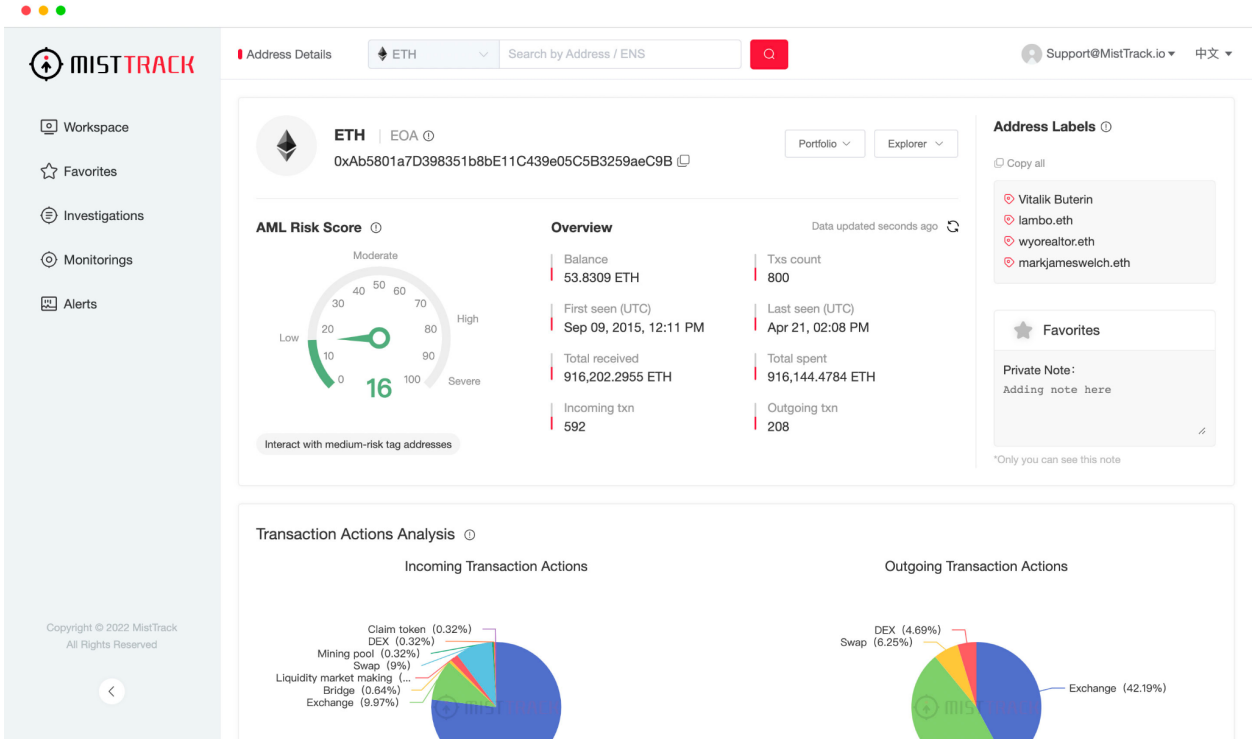
关于安全事件反洗钱分析，我们将主要讨论以下的内容：

- 提出一种针对混币器（Tornado.Cash 和 ChipMixer）资金转出的分析方法
- 应用反洗钱分析方法对部分安全事件进行分析

3.1 工具及方法

在正式开始反洗钱分析之前，我们首先要有一个高效的工具和一套有效应对复杂洗钱情况的分析方法。

3.1.1 基础工具 - MistTrack



（MistTrack 反洗钱追踪系统示例图）

MistTrack 反洗钱追踪系统 是一套由慢雾科技创建的专注于打击加密货币洗钱活动的 SaaS 系统，具有资金风险评分模块、交易行为分析模块、资金溯源追踪模块、资金监控模块等核心功能。

- **AML Risk Score**

MistTrack 反洗钱追踪系统主要从地址所属实体、地址历史交易活动、慢雾恶意钱包地址库三方面为其计算 AML 风险评分。当地址所属实体为高风险主体（如混币平台）或地址与已知的风险主体存在资金来往时，系统会将该地址标记为风险地址。同时，结合慢雾恶意钱包地址库中的恶意地址数据集，对已核实的勒索、盗币、钓鱼欺诈等非法行为的涉案地址进行风险标记。

- **Address Labels**

MistTrack 反洗钱追踪系统积累了超 2 亿个钱包地址标签，地址标签主要包含 3 个分类：

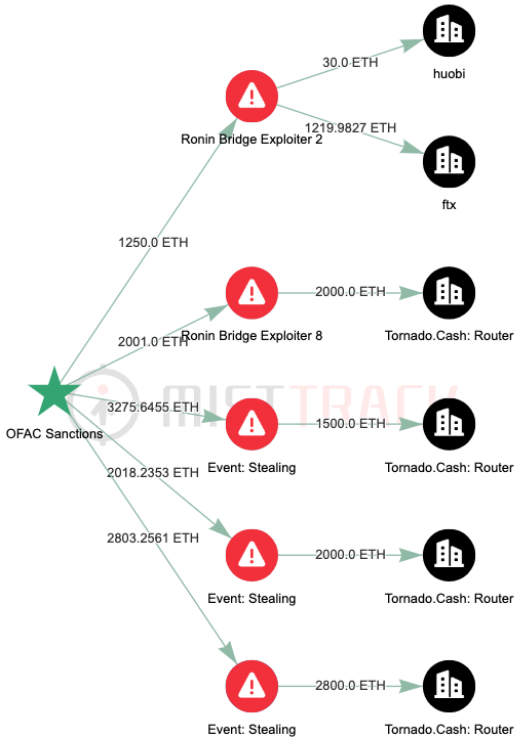
(1) 它归属于什么实体，如 Coinbase、Binance

(2) 它的链上行为特征，如 DeFi 鲸鱼、MEV Bot 以及 ENS

(3) 一些链下情报数据，如曾使用过 imToken/MetaMask 钱包

- **Investigations**

追踪和识别钱包地址上的加密资产流向，实时监控资金转移，将链上和链下信息整合到一个面板中，为司法取证提供强有力的技术支持。



（MistTrack 追踪分析示例图）

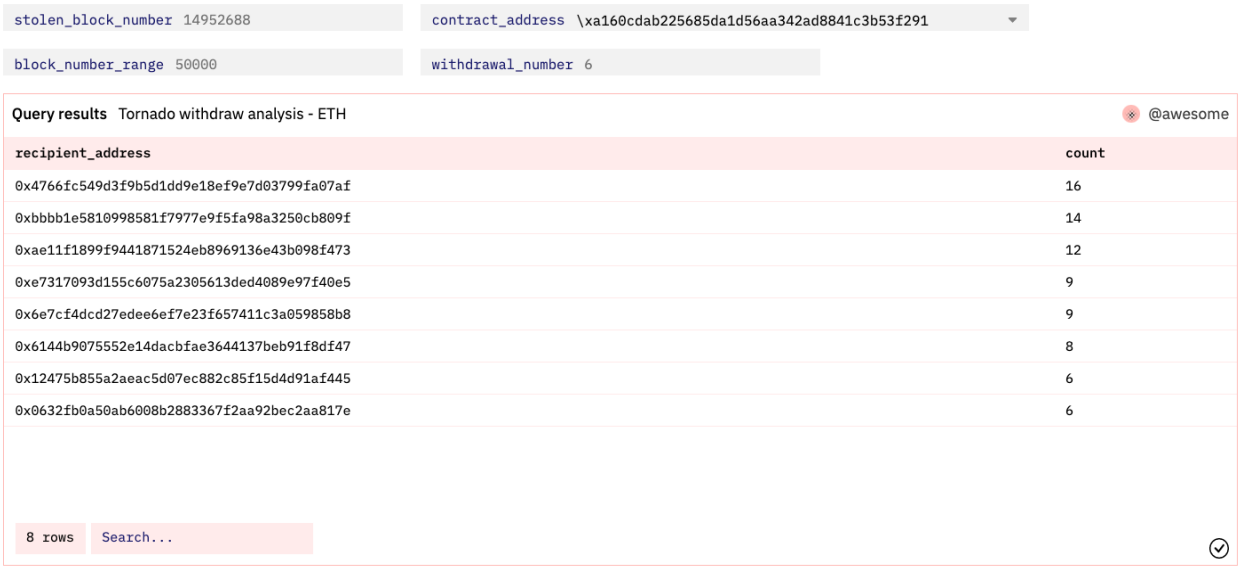
通过标记 1 千多个地址实体、2 亿多个地址标签，10 万多个威胁情报地址，以及超过 9000 万个与恶意活动相关的地址，MistTrack 为反洗钱分析和研究提供了全面的情报数据帮助。通过对任意钱包地址进行交易特征分析、行为画像以及追踪调查，MistTrack 在反洗钱分析评估工作中起到至关重要的作用。

3.1.2 拓展方法 - 数据分析

MistTrack 可以满足常见的反洗钱分析场景，而遇到复杂特殊的情况就需要其他的方法辅助分析。从区块链反洗钱资金态势中我们可以看到很多被黑事件发生后，在 ETH/BSC 链上的资金都不约而同的流向了一片灰暗之地——Tornado.Cash，Tornado.Cash 已成为 ETH/BSC 链上反洗钱的主战场。

新的洗钱手法需要新的分析方法，对 Tornado.Cash 转出分析的需求变得越来越普遍，此处我们将提出一个针对 Tornado.Cash 资金转出的分析方法。

- 记录目前已知的信息，已知信息包括转入 Tornado.Cash 总数，第一笔 Tornado.Cash 存款时间，第一笔 Tornado.Cash 存款的区块高度。
- 将参数填入我们准备的 分析面板 。
- 得到初步的 Tornado.Cash 提款数据结果，再使用特征分类的方式对数据结果做进一步筛选。
- 筛选后的结果是一批疑似黑客转出的结果集，取概率最高的结果集并对它进行验证。
- Tornado.Cash 转出分析结论。



（Dune Dashboard - Tornado.Cash 转出分析）

通过这个 Tornado.Cash 资金转出的分析方法，我们已成功分析出 Ronin Network 等多个安全事件从 Tornado.Cash 转出后的资金详情。

显而易见，这个 Tornado.Cash 资金转出的分析方法同样存在局限性：
转入 Tornado.Cash 的数量分类也是一个匿名集，资金量越大相应的匿名集数量越少，资金量越小则相反。所以对于资金量小的分析难度更大。

而在 BTC 链上，通过区块链反洗钱资金态势我们可以看到 ChipMixer 和 Blender 是黑客的常用洗钱平台。Blender 目前已被美国财政部制裁，站点已不可用，这里不再做进一步的探讨。

ChipMixer 流入洗钱资金量巨大，我们同样需要提出一个针对 ChipMixer 资金转出的分析方法。

- 识别 ChipMixer 的提款特征。

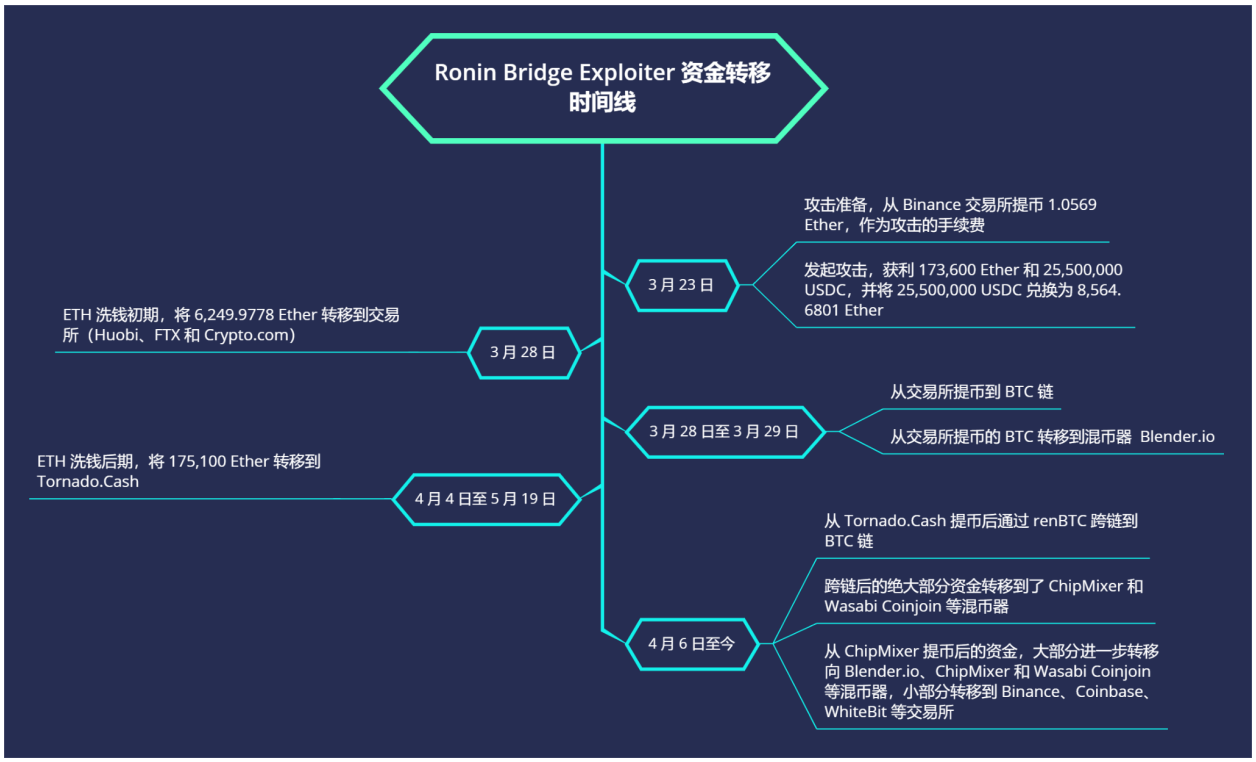
输入地址类型	输出地址类型	输入数额特征	版本	锁定时间
bech32(bc1q...)	bech32(bc1q...)	所有的输入数额都满足 Chips(即 0.001 * 2 的 n 次方，n < 14)的要求	2	区块高度 - 1/ 区块高度 - 2/ 区块高度 - 3

- 根据上述提款特征对相应时间段的结构化区块数据进行扫描和筛选，得到这个时间段内 ChipMixer 的提款记录。
- 对提款记录数据归类结果集，取概率最高的结果集并对它进行验证。
- ChipMixer 转出分析结论。

3.2 反洗钱分析详述

3.2.1 Ronin Network

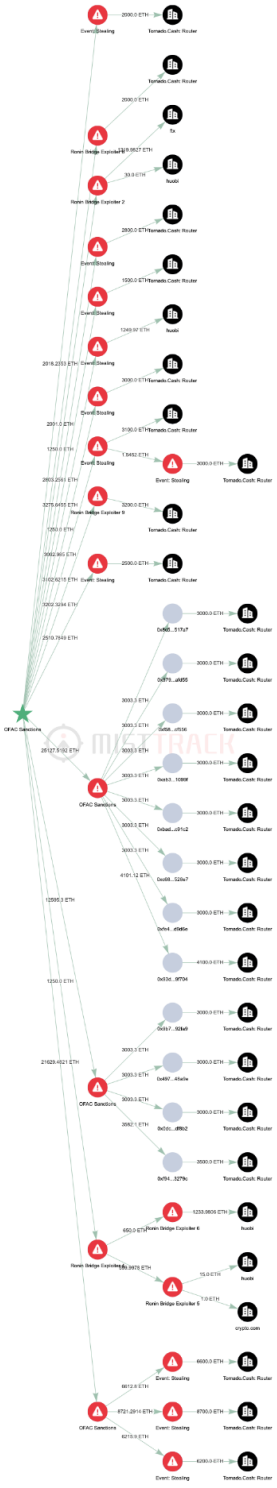
黑客地址：0x098B716B8Aaf21512996dC57EB0615e2383E2f96（ETH 链）
被盗时间：3 月 23 日
损失统计：173,600 ETH、25,500,000 USDC
攻击手续费来源：SimpleSwap
资金转移：



（Ronin Bridge Exploiter 资金转移时间线）

ETH 资金转移

黑客将攻击获利的 25,500,000 USDC **兑换为了** 8,562.6801 ETH，**所以黑客需要洗币的总额为** 182,163.737 ETH（Binance **提款** 1.0569 ETH + **攻击所得** 173,600 ETH + **攻击兑换** USDC **所得** 8,562.6801 ETH）。


Event: Stealing
Tornado.Cash: Router
Ronin Bridge Exploiter 2
Ronin Bridge Exploiter 9
Ronin Bridge Exploiter 6
Ronin Bridge Exploiter 5
OFAC Sanctions
MistTrack

（Ronin Bridge Exploiter 资金转移图）

黑客获利资金流向主体详情如下表：

主体	流向资金
Tornado.Cash	175,100 ETH
Huobi	5,028.9951 ETH
FTX	1,219.9827 ETH
Crypto.com	1 ETH
Balance	667.3916 ETH

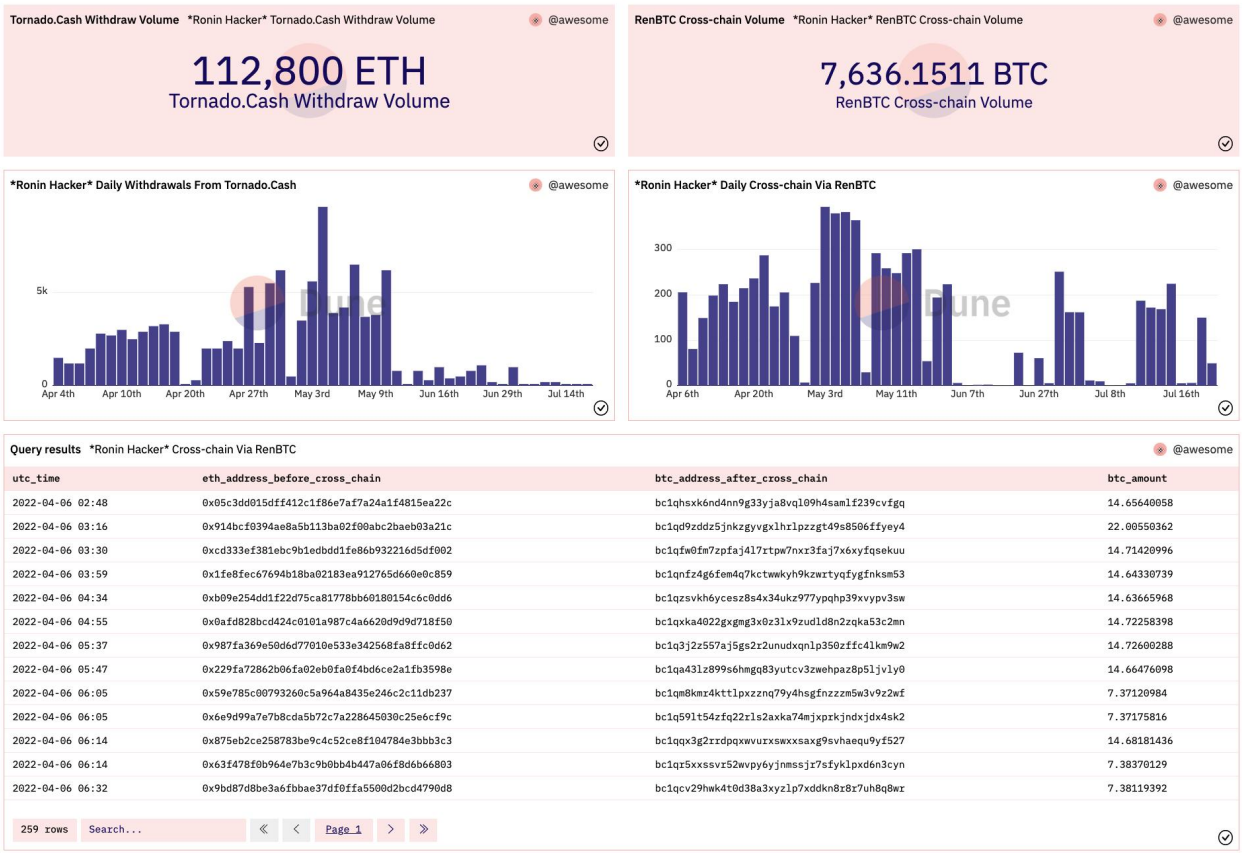
注：其他未做统计的流向资金为洗币过程损失。

Tornado.Cash 资金转移

黑客总计转入 Tornado.Cash 175,100 ETH，经过分析，我们得出 Ronin 黑客从 Tornado.Cash 提款符合下列特征：

从 Tornado.Cash 转出后直接或转移一层后使用 1inch 或 Uniswap 兑换为 renBTC，通过 renBTC 跨链到 BTC 链。

通过 Dune Analytics，我们将符合上述特征的 Tornado.Cash 提款和跨链到 BTC 链的数据筛选出来，并进行有效的 可视化展示，如下图：



（Ronin 黑客从 Tornado.Cash 转出后通过 renBTC 跨链数据）

根据上面的分析图，得到 Tornado.Cash 转出资金情况如下表：

流向	流向资金
通过 renBTC 跨链到 BTC 链	112,800 ETH
在 Tornado.Cash 中的余额	62,300 ETH

注：数据有效时间截止于 7 月 20 日。

BTC 资金转移

根据对 Tornado.Cash 资金转移的分析，我们得到符合特征的共计 8,075.9329 BTC 的资金跨链到 BTC 链。其中的 6,191.2542 BTC 经过分析确认与 Ronin 黑客相关，再加上从 Huobi 和 FTX 提款的 439.7818 BTC，确认共计 6,631.036 BTC 为 Ronin 黑客所属资金。此部分资金的进一步转移情况如下表：

主体	流向资金
ChipMixer	3460.6845 BTC
Blender	439.7818 BTC
Wasabi Coinjoin	55.1448 BTC
renBTC	95.6871 BTC
Coinbase	0.5632 BTC
ChangeHero	0.488 BTC
Binance	12.0973 BTC
Wirex	0.0399 BTC
Kuna	0.0384 BTC
Any.Cash	0.0676 BTC
Unknown	153.0143 BTC
Balance	2413.4292 BTC
合计	6631.036 BTC

注:0.1 BTC 以下转移额不做统计。

ChipMixer 资金转移

根据 BTC 资金转移可以看到 3460.6845 BTC 转移到了 ChipMixer，通过对 BTC 链上数据监控以及对 ChipMixer 的提款数据进行分析，识别出 Ronin 黑客从 ChipMixer 共计提款 2,871.03 BTC。此部分资金的进一步转移情况如下表：

主体	流向资金

Blender	1356.0 BTC
Wasabi Coinjoin	9.8365 BTC
ChipMixer	547.7938 BTC
UnKnown	681.4247 BTC
Balance	235.4739 BTC

注：0.1 BTC 以下转移额不做统计。

3.2.2 Wormhole

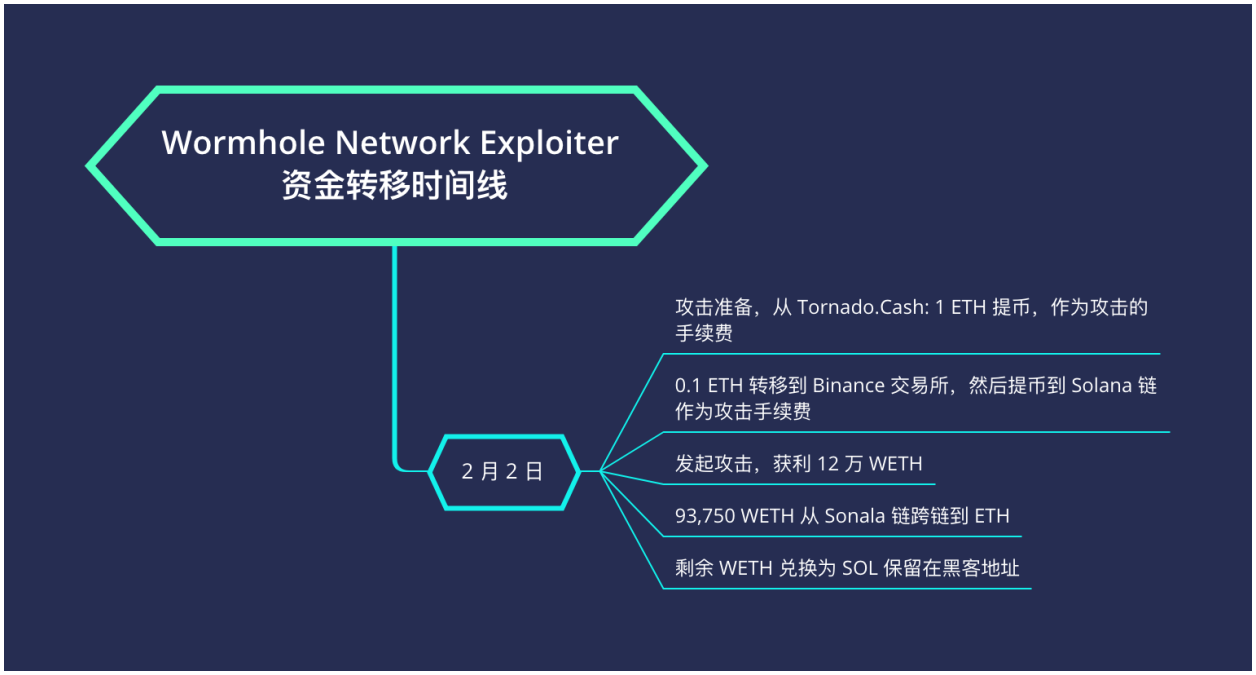
黑客地址：CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka (Solana)

被盗时间：2 月 2 日

损失统计：120,000 WETH

攻击手续费来源：Tornado.Cash

资金转移：



（Wormhole Network Exploiter 资金转移时间线）

WETH 资金转移

流向	流向资金
跨链到 ETH 链	93,750 WETH
兑换为 SOL	26,250 WETH

黑客地址余额

地址	余额
CxegPrfn2ge5dNiQberUrQJkHCcimeR4VXkeawcFBBka	432,661.15 SOL
0x629e7da20197a5429d30da36e77d06cdf796b71a	93,750.623 ETH

3.2.3 Beanstalk Farms

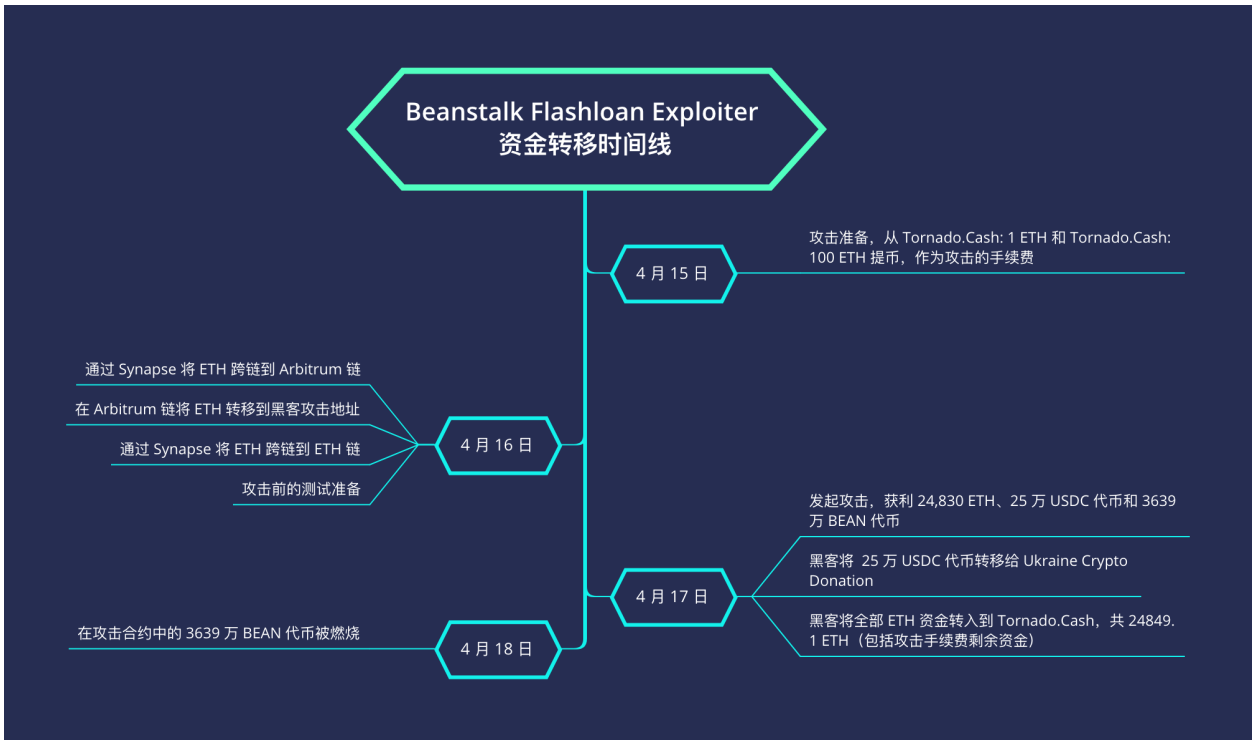
黑客地址:0x1c5dCdd006EA78a7E4783f9e6021C32935a10fb4(ETH 链)

被盗时间：4 月 17 日

损失统计：24,830 ETH、250,000 USDC 代币和 36,390,000 BEAN 代币

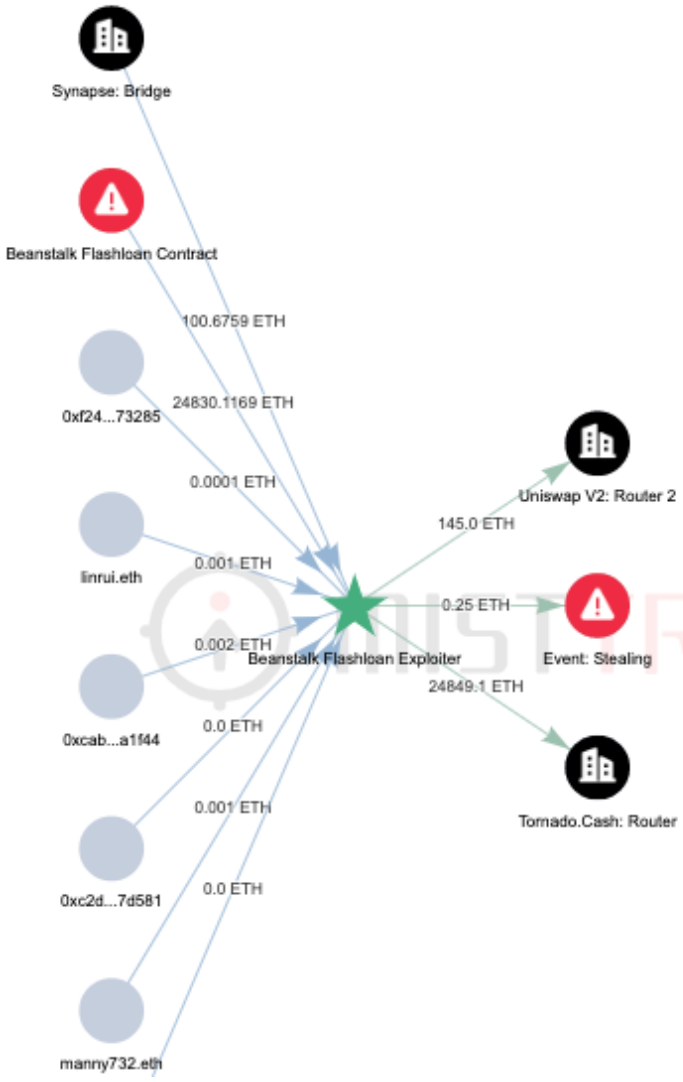
攻击手续费来源：Tornado.Cash

资金转移：



（Beanstalk Flashloan Exploiter 资金转移时间线）

ETH 资金转移



（Beanstalk Flashloan Exploiter ETH 资金转移图 ）

ETH 的资金转移如下表：

流向	流向资金
Tornado.Cash	24849.1 ETH

注：转移资金中包括攻击手续费剩余资金。

3.2.4 Harmony

黑客地址:

0x0d043128146654C7683Fbf30ac98D7B2285DeD00（ETH **链**）

0x0d043128146654C7683Fbf30ac98D7B2285DeD00（BSC **链**）

被盗时间：6 **月** 23 **日**

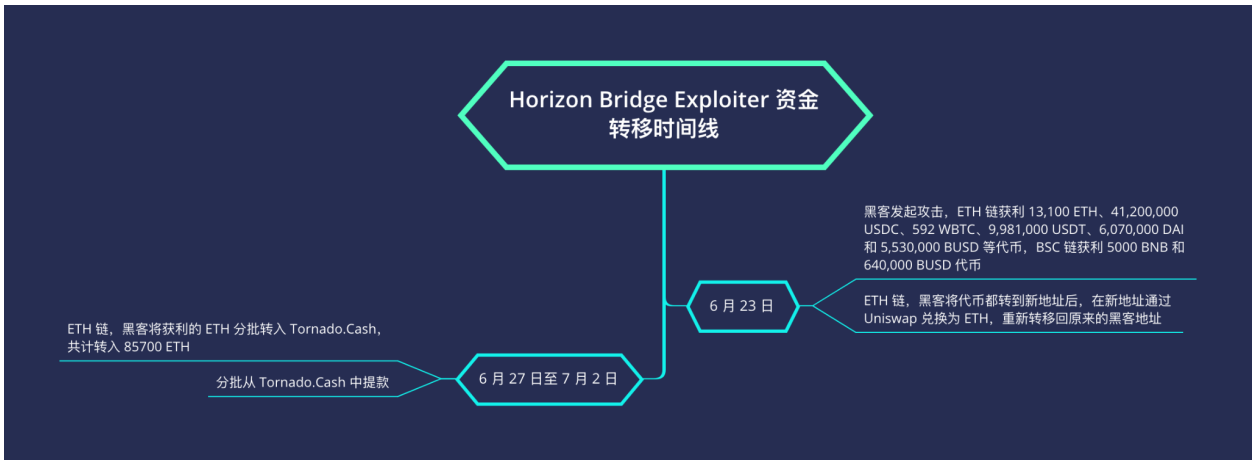
损失统计：

（ETH **链**）13,100 ETH、41,200,000 USDC、592 WBTC、9,981,000 USDT、6,070,000 DAI、5,530,000 BUSD、84,620,000 AAG、110,000 FXS、415,000 SUSHI、990 AAVE、43 WETH **和** 5,620,000 FRAX

（BSC **链**）5,000 BNB **和** 640,000 BUSD

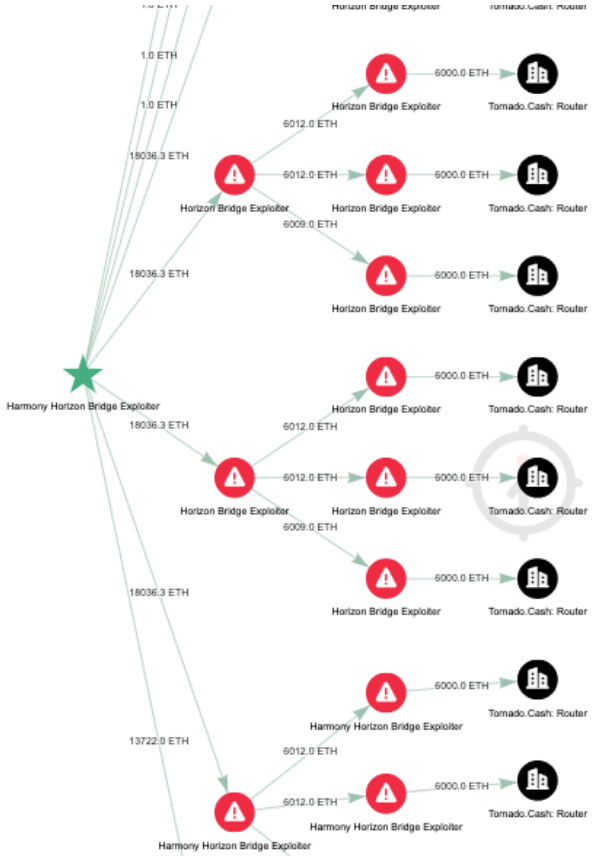
攻击手续费来源：**无**

资金转移：



（Horizon Bridge Exploiter 资金转移时间线）

ETH 资金转移



（Horizon Bridge Exploiter ETH 资金转移图）

ETH 资金转移表：

流向	流向资金
Tornado.Cash	85,700 ETH
Balance	201.2094 ETH

Tornado.Cash 资金转移

黑客总计转入 85,700 ETH 到 Tornado.Cash，经过分析，我们得出 Harmony 黑客的 Tornado.Cash 提款符合下列特征：

- 从 Tornado.Cash 的分批提款，每个提款地址的提款次数相对固定，主要提款次数是 5 和 6，即提款 5 * 100 ETH 或 6 * 100 ETH 到提款地址。
- 从 Tornado.Cash 提款后，长达一个月未发生进一步转移。

根据上述的 Tornado.Cash 提款特征，共计发现了黑客 83,300 ETH 的提款，从 Tornado.Cash 转出资金情况如下表：

流向	流向资金
Balance	83,300 ETH

四、展望

2023 年在加密货币世界中我们还需要关注什么？

1、监管合规化

由 FTX 暴雷等事件引发的监管问题已成为核心难题。加密货币项目方虽然像银行一样运营，但却没有银行应遵守的规则和监管。如何更有效地监管这个市场，让消费者既能得到保护，又能在项目遭受损失时获得补救，让市场变得更稳定是当下最需要去解决的问题。当然，我们从好的方面去考虑，这也意味着监管机构及大众对加密货币和区块链技术的了解程度越来越高，各国对加密货币领域的政策和态度越发清晰，加密货币市场将逐步迈向合规化。

2、加强对安全审计的关注

2022 年安全事件频频发生，尤其从 10 月 1 日到 10 月 15 日半个月时间内，Web3 领域相关项目和交易平台就受到近 20 次攻击，大部分还是因为项目代码存在安全漏洞而被黑客攻击利用，这也说明了在区块链生态繁荣发展的同时，项目开发的代码安全规范仍然是重中之重。比如很多跨链桥匆匆上线，以零手续费、快速吸引用户和项目方，却往往忽略了最重要的安全性，一是因为跨链桥流动资金量很大且去中心化程度较低，权限几乎都掌握在多签钱包中，只要掌握了签名就可以掌控一切，二是因为跨链桥很少会找安全审计机构对它们的产品进行安全审计，社区对它的监控也很少，导致跨链桥频频成为黑客的攻击目标。随着安全事件愈来愈多，相信未来会有更多的项目方意识到审计的重要性。因为 SlowMist 在区块链安全方面有很深的积累和经验，我们始终认为，对项目方来说在项目上线之前进行全面深入的前后端及合约的安全审计是非常有必要的。同时也可以发布 Bug Bounty 来规避项目在持续运行和发展过程中的安全问题，提升项目的安全等级。

3、扩容继续升温，多链和谐共存

2021 年各大公链崛起，Solana、Avalanche 等公链获得了大量投资者的关注，2022 年，一批新兴公链也获得了高额的投资和极大的关注，如 Aptos、Sui 等。尽管以太坊在合并之后，从工作量证明机制（PoW）转为能耗更低的权益证明机制（PoS），但在手续费和交易速度等方面没有变化，扩容战争将继续升温，其他公链通过不同方法扩大吞吐量，降低交易成本，吸引优秀的开发人员加入，争夺市场份额。近年来，为了降低一层网络的负担，提高业务处理效率，实现扩容，不少以太坊项目都是基于 Layer2 搭建的。例如 Rollup、Arbitrum，作为解决 Ethereum 网络堵塞问题的中长期方案，将继续受到关注。同时，由于区块链天生存在不可能三角，而区块链上的赛道逐渐增多，一条区块链很难满足多种用户需求，所以未来会是多链共存的局面。首先我们希望未来会解决多条链的互操作性兼容问题，将兼容 EVM 和 非 EVM 的链更好的连接起来，其次弱化互操作性不可能三角问题，达到跨链桥的速度够快、流动性足够高、用户的交互体验更流畅安全的最佳平衡。

4、反洗钱与链上追踪分析

随着黑客攻击事件越来越多，链上追踪分析的重要性渐渐显现出来。目前的主流区块链浏览器都是以查询链上信息为主，但查询只是浏览器的最基本功能，在这基础之上，链上数据还可以用来做一些数据追赃和反洗钱的工作。随之而来的是各种链上追踪分析工具和平台，用户除了检查自己的资产是否与脏钱相关联，还可以通过这些追踪工具的数据聚合找到自己想要的信息，例如资金去向等等。相信在未来，追踪工具不断演变，会为反洗钱增添更多力量。

5、加强对备份的关注

加密资产的所有权备份，即对私钥或助记词的备份，因为它们承载着对加密货币的完整所有权，一旦被盗或丢失则会损失所有资产。对于加密资产领域来说，私钥/助记词的备份反而是很大的短板，资产使用上的场景都可以有大量对应的产品来解决，无论是热钱包还是冷钱包，使用上可以保证安全，但很容易忽略其备份的重要性。目前大多数的盗币或者丢币的情况，反而是因为私钥/助记词的备份泄漏或丢失而导致的。备份的重要性等同于加密资产本身，必须要重视起来。比如最近几个月，一种叫作 多方计算（MPC, multi-party computation）的新技术频繁被提及。MPC 是一种较为优秀解决单点备份问题的机制，可以在最初的私钥生成时即可分为多个分片，将不同的分片分发给一群人，需要恢复时使用特定的程序来还原出原始私钥即可，MPC 在与多签技术配合使用是我们觉得很有前景且应该尽快普及的，希望在不久的将来能发展出满足业内公认标准且开源的方案。

6、零知识证明：扩容与隐私

零知识证明指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个推断是正确的。零知识技术是密码学的一个分支，可以为许多 Layer1 区块链项目解决扩容和隐私问题。虽然它不是一个新的技术名词，但直到最近几个月才成为热门话题，或许零知识证明会是未来几年 Web3 和区块链最重要的解决方案之一。

五、总结

纵览整个 2022，“动荡”一词贯穿全年。尽管仍有暴雷的余震回荡，尽管我们正在经历寒冬，但任何事物都无法改变区块链发展的方向，只有如履薄冰，认真做有利于行业发展的事情才能稳固长久。无论如何，我们仍期待着区块链行业在 2023 年的发展。

六、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。

七、关于我们

慢雾科技 (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。慢雾科技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。

慢雾科技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。慢雾科技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。

慢雾科技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，慢雾科技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。慢雾科技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科技努力的方向。

慢雾科技安全解决方案

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