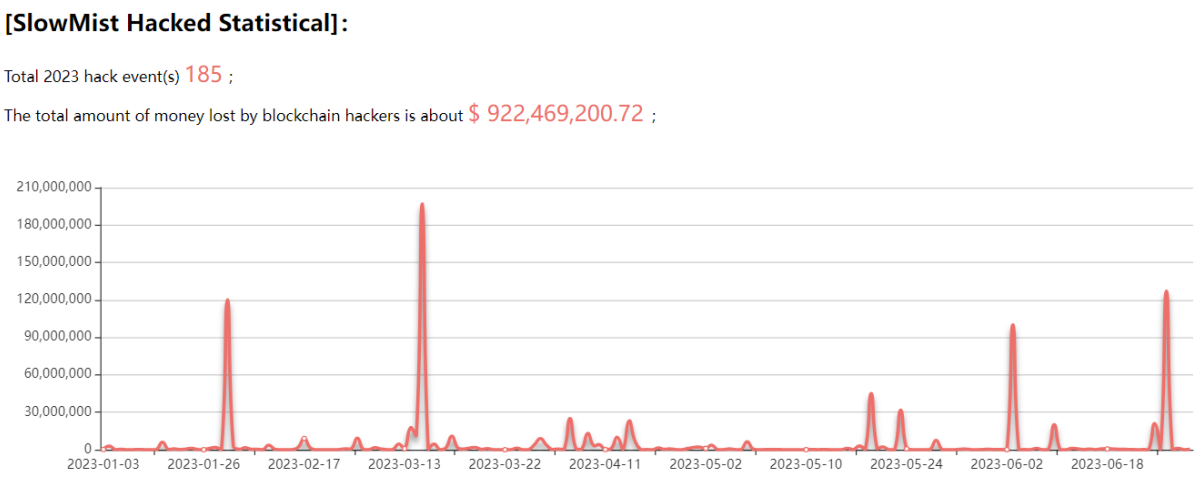

SLOWMIST 2023 上半年
区块链安全与反洗钱报告

目录

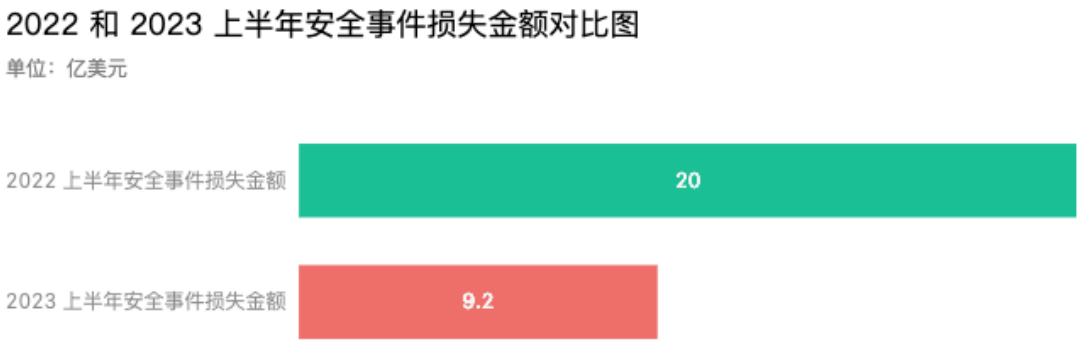
一、前言

在过去的半年里，全球范围内的区块链技术持续演进，为数字经济带来了新的可能性和机遇。然而，随其发展势头而来的是区块链安全面临着日益严峻的挑战。随着区块链应用的扩大和深入，攻击者也变得更加精明和复杂，不断攻破和利用区块链系统的漏洞进行攻击，导致巨额的损失。在上半年我们见证了一系列涉及智能合约的攻击、钓鱼攻击、交易平台被盗和网络欺诈等安全事件。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年安全事件共 185 件，损失高达 9.2 亿美元。



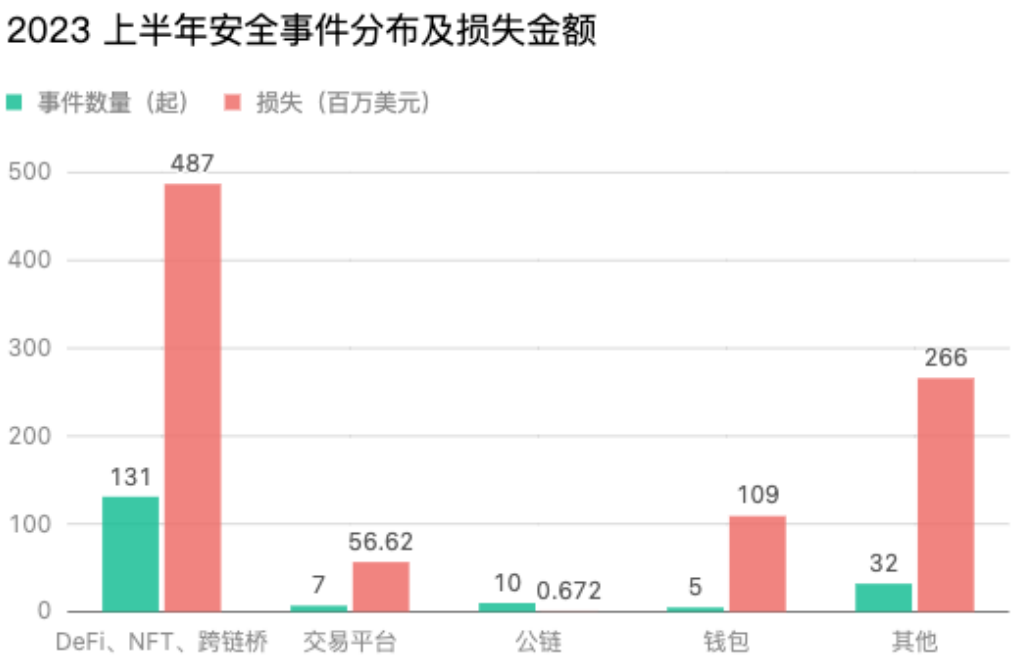
(https://hacked.slowmist.io/)

对比 2022 年上半年（共 187 件，损失约 20 亿美元），损失同比降低 54%。



（2022 和 2023 上半年安全事件损失对比图 ）

其中 DeFi、NFT、跨链桥事件共 131 起，损失约 4.87 亿美元；交易平台安全事件 7 起，损失约 5662 万美元；公链安全事件 10 起，损失约 67.2 万美元；钱包安全事件 5 起，损失约 1.09 亿美元；其他安全事件 32 起，损失约 2.66 亿美元。



（2023 上半年安全事件分布及损失金额 ）

在这样的背景下，本报告着眼于区块链生态安全，梳理了 2023 上半年区块链主要的安全事件以及资金追回情况，让大家对当前和未来区块链的安全风险有一个全面认识。此外，由于区块链的匿名性和去中心化特性，区块链技术也常常被恶意分子滥用于资金洗钱活动，洗钱活动不仅会威胁金融系统的稳定性，大规模的洗钱活动还可能导致市场价格波动、市场操纵和金融市场的不公平竞争。因此，本报告还将通过某些事件辅助识别可疑交易模式和行为，探讨区块链生态的反洗钱情况。

二、安全事件

1、公链

作为区块链的基础设施，公链承载了人们对于区块链作为 Web3 底层网络的期望，其通过分散存储数据和交易记录，实现无需中心化控制的操作，并提供可追溯、安全和高效的交易环境。由于公链上通常存在大量的数字资产，攻击者可能利用漏洞、恶意代码或其他手段攻击公链，窃取用户的资金。

根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年公链安全事件共 10 件，损失约 67.2 万美元。上半年公链安全事件中，大部分是由分叉引起，这往往是因为公链中存在大量的验证器，其同步和相互协议出现了分歧导致。此外，近些年供应链安全也逐渐成为 Web3 行业乃至全球关注的焦点。恶意的软件和代码可以在软件供应链的不同环节中植入，包括开发工具、第三方库、云服务和更新过程。一旦这些恶意元素被成功植入，攻击者可以利用它们来窃取加密货币资产和用户敏感信息、破坏系统功能、勒索企业或大规模传播恶意软件。

虽然公链安全漏洞造成的损失一般较小，但对整个链生态的影响巨大。所以公链在上线前一定要经过专业的安全审计。建议公链项目方与可信且职业的安全团队进行深入合作，部署因地制宜的安全建议，将引起安全问题的可能性降到最低，从而保障整个公链生态系统的稳定和可持续发展。

2、交易平台

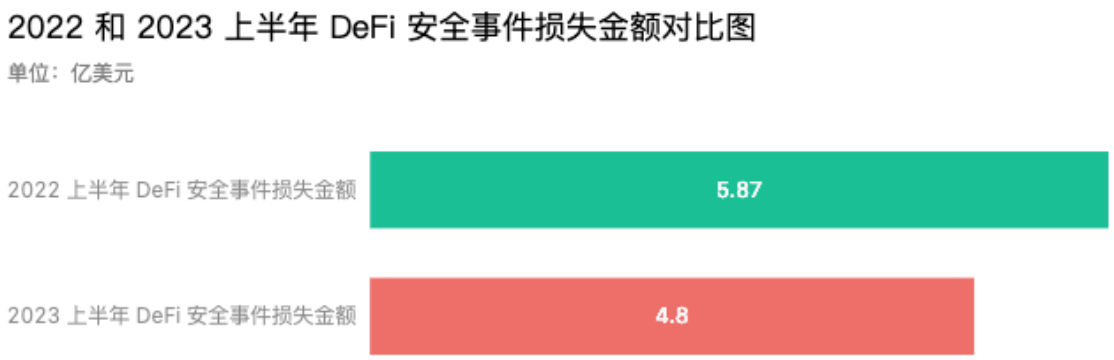
在区块链领域，交易平台扮演着至关重要的角色。作为数字资产交易的主要场所，交易平台为用户提供存储和管理数字资产的服务。如果交易平台存在安全漏洞或遭黑客攻击，用户的资产可能受到损失或盗窃。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年交易平台安全事件共 7 件，损失高达 5662 万美元。

一方面，去年区块链行业经历了一系列的爆雷事件，这些事件凸显出了交易平台营运透明度的重要性。当然，无论用户是选择将资产存放至交易平台，还是采用托管的方式，都必须知道每一种方法都有相应的风险，关键是要清楚自己承担风险的能力，以及如何做风险管理。

另一方面，交易平台的安全性对于保护用户资产、确保交易的顺利进行、建立用户信任以及推动加密货币市场的稳定发展至关重要。建议各大交易平台通过加强安全意识培训，提高员工和用户识别应对潜在的安全威胁和社会工程攻击；定期进行安全审计，发现和修复交易平台可能存在的漏洞和安全问题，确保交易平台的软件和系统保持最新的安全补丁和更新等方式加强对数字资产的安全保障。

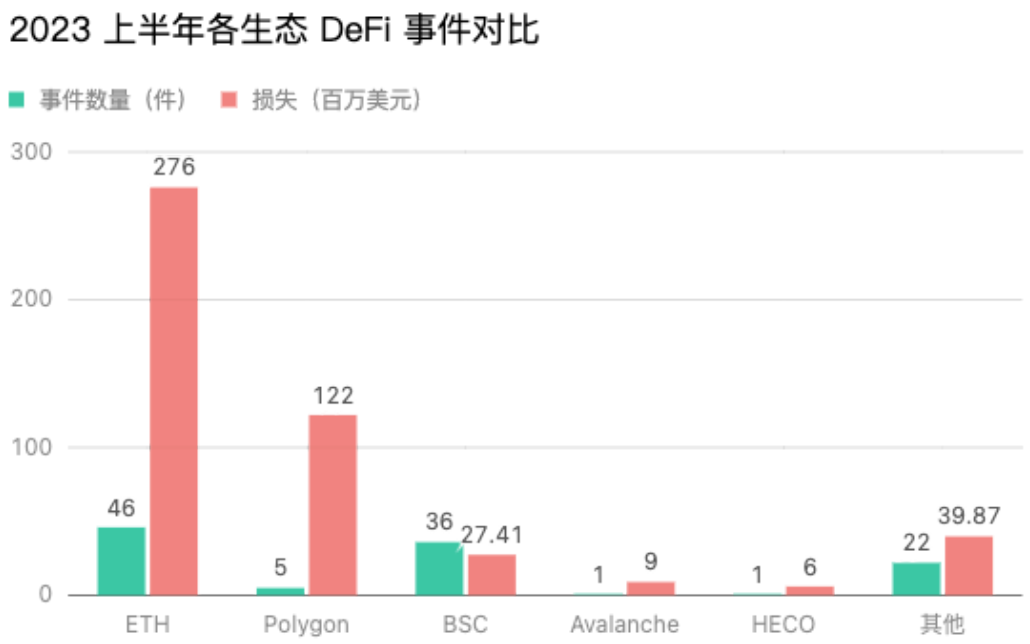
3、DeFi

DeFi 为用户提供了更开放、包容和创新的金融体验，赋予了个人更大的金融自主权，并为全球范围内的用户提供了无缝、安全和透明的金融服务。DeFi 应用程序通常依赖智能合约来执行各种功能，例如交易、借贷和流动性挖矿。然而，由于回报快速、隐私、匿名以及监管执法方面相对落后，DeFi 仍是黑客攻击的理想目标。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年 DeFi 安全事件共 111 件，损失高达 4.8 亿美元，对比 2022 上半年（共 93 件，损失约 5.87 亿美元），损失同比降低 18%。



（2022 和 2023 上半年 DeFi 安全事件损失金额对比图 ）

其中以太坊生态损失最多，约 2.76 亿美元，其次是 Polygon 生态，约 1.22 亿美元。



（2023 上半年各生态 DeFi 事件对比）

常见的 DeFi 攻击类型包括智能合约漏洞利用、闪电贷攻击、流动性挖矿攻击、价格操纵、假代币和 Rug Pull 等。近期发生的 DeFi 安全事件，大部分都和闪电贷有关系。闪电贷本身并不是一种恶意工具，但攻击者可以通过闪电贷在很短的时间内借出大量资金，这些资金可被用来利用代码的漏洞，对价格进行操纵，攻击业务逻辑等等。当然，这里面的关键点还是在于合约漏洞。智能合约之所以“智能”，是因为它极为灵活，能够控制大量的资产和数据。合约一旦部署上链之后，不可篡改，无需人工干预，它的执行过程透明可见，虽然解决了执行过程中的部分“信任”问题，但如果智能合约因存在漏洞被利用，那区块链技术的这些特性反而会成为某种障碍。

例如，2023 年 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。

一个月后，另一个 DeFi 协议 Euler Finance 遭到攻击，攻击者获利约 1.97 亿美金。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（checkLiquidity）提取获得的资金。另外，多个项目也受 Euler Finance 事件影响，如 Balancer 损失 1190 万美元、Yearn Finance 损失 138 万美元、Angle Protocol 损失 1760 万美元、Idle Finance 损失 1099 万美元、Yield Protocol 损失 150 万美元、Inverse Finance 损失 86 万美元。庆幸的是，4 月 4 日，经过成功协商，攻击者已归还盗取的所有资金，其他受影响的项目也在逐步恢复。

随着市场及技术的发展，智能合约正变得越来越复杂多样，相信在未来也必将承载更高的价值，但发展在左，安全在右，确保 DeFi 平台和智能合约的安全性也是至关重要的。一方面，不断出现的合约安全漏洞迫使开发者必须更加全面且专注地构建安全、稳健、恢复力强的智能合约；另一方面，DeFi 项目方可以委托专业的第三方安全公司或审计机构对智能合约和代码进行审计并根据审计结果及时修复发现的漏洞和安全问题。此外，漏洞披露和合规机制也是保护 DeFi 项目方和用户免受攻击的重要手段。

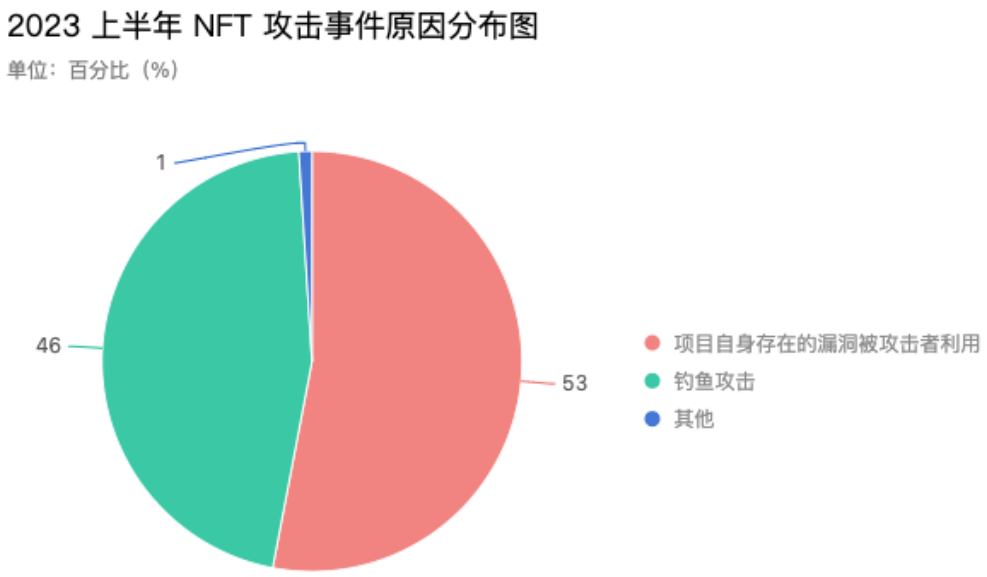
4、跨链桥

跨链桥，区块链的基础设施之一，为区块链网络之间的互操作性、资产流动性、数据传输、去中心化金融和跨链治理提供了基础设施和解决方案。然而，由于跨链桥通常需要处理多个区块链之间的通信和资产转移，涉及到复杂的协议和技术，这种复杂性导致出现漏洞和被攻击的概率变大。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年跨链桥安全事件共 7 件，损失高达 137 万美元。对比 2022 上半年（共 7 件，损失约 10.43 亿美元），损失大幅降低。

通过这些安全事件不难发现，跨链桥很容易存在基础面和技术面的缺陷，无论是假充值问题、私钥泄露问题还是多重签名验证问题，跨链桥安全常常与设计逻辑挂钩，这也是由它们的互操作性引发的重要挑战。如果跨链桥存在安全漏洞或遭到攻击，用户的资产可能面临被窃取或篡改的风险，因为跨链桥涉及资产的锁定、解锁和转移。因此，保障跨链桥的安全性和可靠性对确保用户的资产得到有效的保护及防止不必要的损失具有重要意义。首先，可以通过增加签名者的比例来减少被攻击的风险；其次，可以与安全公司合作，无论是审计还是反洗钱方面，都有助于提高跨链桥的安全性；最后，可以通过发布漏洞赏金的方式加强跨链桥的安全性。

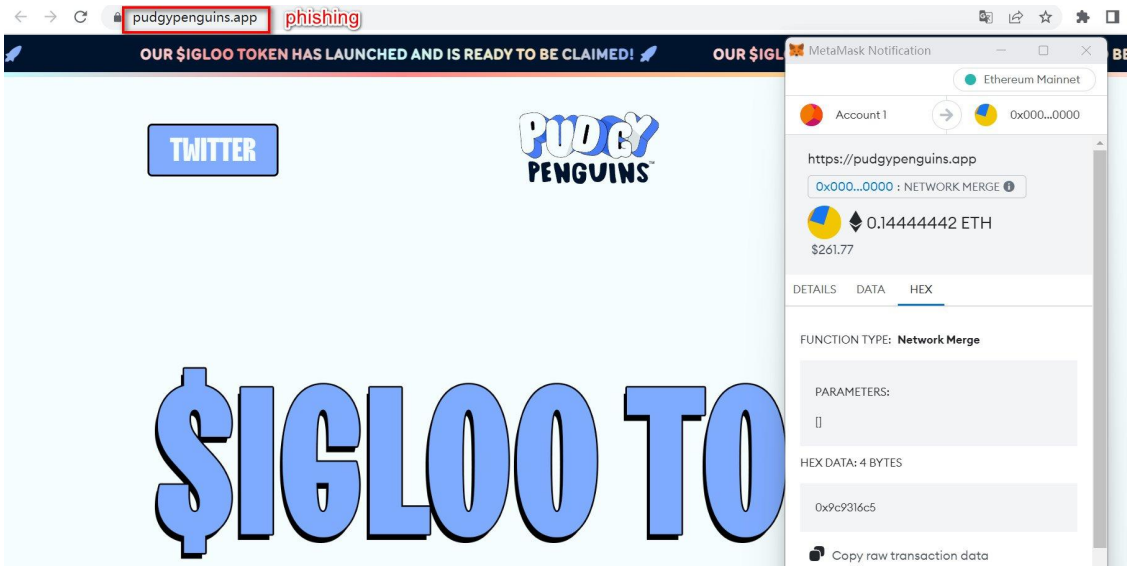
5、NFT

NFT（非同质化代币）代表了数字资产的独特性和所有权，NFT 使得数字艺术品、虚拟土地、游戏道具等可以被确权和拥有，为数字资产赋予了真实且不可替代的价值。随之而来的是 NFT 市场的发展和 NFT 艺术品的高价值也吸引了黑客的关注。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年 NFT 安全事件共 13 件，损失高达 631 万美元。2023 上半年 NFT 安全事件中，53% 源于项目自身存在的漏洞被攻击者利用，其次是钓鱼攻击，占比为 46%。



（2023 上半年 NFT 攻击事件原因分布图）

在 NFT 钓鱼攻击中，多数都是由于官方 Discord/Twitter 等媒体平台被黑，黑客发布钓鱼链接诱骗用户。

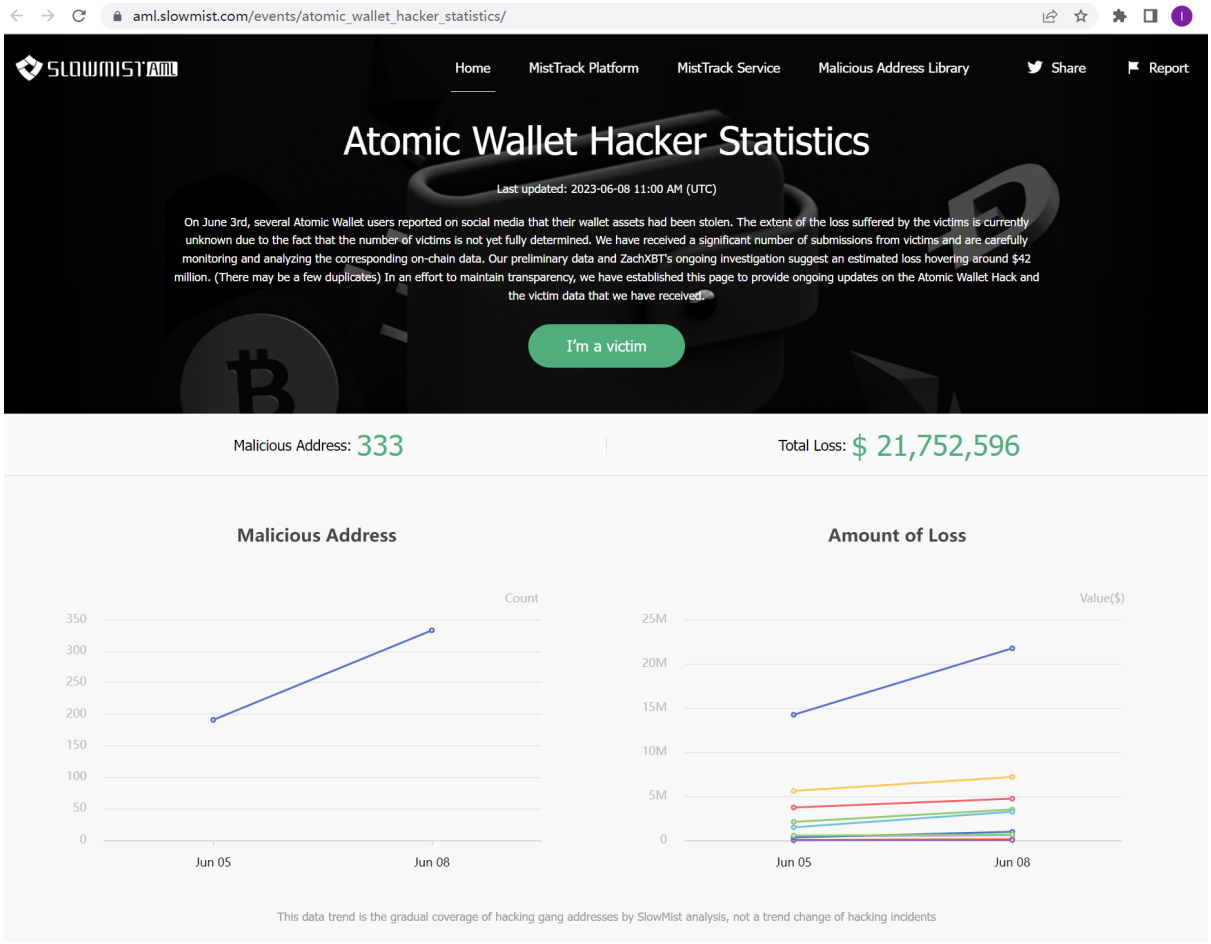


用户和平台应加强安全意识，采取适当的防范手段，包括保持警惕、仔细审查交易和应用来源、进行安全审计、使用可靠的钱包和平台等，以确保 NFT 安全性和对资产的保护。

6、钱包

钱包作为区块链世界的入口，提供资产管理、安全性保障、用户体验、去中心化控制和互操作性等功能，在区块链世界扮演着关键角色。它们是用户与区块链世界的接口，为用户提供了方便、安全和自主的区块链体验，这也导致钱包容易成为黑客攻击的目标。根据慢雾区块链被黑事件档案库(SlowMist Hacked) 统计，截至 6 月 30 日，2023 上半年钱包安全事件共 5 件，损失高达 1.09 亿美元。其中，波及范围最广、造成损失最多的事件是 Atomic Wallet Hack 事件。

6 月 3 日，一些 Atomic Wallet 用户在社交媒体上报告，他们的钱包资产被盗。到 6 月 4 日，根据众多受害者提供的信息，AtomicWallet 黑客事件的估计损失约为 1483 万美元。到 6 月 8 日，黑客造成的损失已经飙升到 2175 万美元，比之前的估计增加了 763 万美元。据统计，目前被盗金额已达到 1 亿美金，而被盗发生的原因我们不得而知，官方表示仍在调查中。在分析过程中，我们也收到大量受害者提交的信息，为了保持透明度，我们建立了一个专题页面，以持续更新有关 Atomic Wallet 攻击的信息和我们收到的受害者数据。



(https://aml.slowmist.com/events/atomic_wallet_hacker_statistics/)

鉴于用户使用钱包的频率较高，且钱包安全直接关系到用户的资产安全，用户应保持警惕，采取相应的安全措施，如选择安全可靠的钱包、保护好私钥、避免点击可疑链接和下载未知来源的软件，最大程度地防范黑客攻击的风险。

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，如：

- 钓鱼网站提醒：通过生态或者社区的力量汇聚各类钓鱼网站，并在用户与这些钓鱼网站交互的时候对风险进行醒目地提醒和告警。
- 签名的识别和提醒：识别并提醒 eth_sign、personal_sign、signTypedData 这类签名的请求，并重点提醒 eth_sign 盲签的风险。

- 所见即所签：钱包中可以对合约调用进行详尽解析机制，避免 Approve 钓鱼，让用户知道 DApp 交易构造时的详细内容。
- 预执行机制：通过交易预执行机制可以帮助用户了解到交易广播执行后的效果，有助于用户对交易执行进行预判。
- 尾号相同的诈骗提醒：在展示地址的时候醒目的提醒用户检查完整的目标地址，避免尾号相同的诈骗问题。设置白名单地址机制，用户可以将常用的地址加入到白名单中，避免类似尾号相同的攻击。
- 在交易显示上，可以增加对小额或者无价值代币交易的隐藏功能，避免尾号钓鱼。
- AML 合规提醒：在转账的时候通过 AML 机制提醒用户转账的目标地址是否会触发 AML 的规则。

对个人用户来说，风险主要在“域名、签名”两个核心点。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》。

7、资金归还

在 2023 上半年中，在遭受攻击后仍能全部或部分收回损失资金的事件共有 10 起。在这 10 起事件中，被盗资金总计约 2.32 亿美元，其中的 2.19 亿美元被返还，占被盗资金的 94%。在这 10 起事件中，有 3 个协议的资金被全部退回。资金被盗后又归还或许将成为一个新趋势，无论是依靠赏金还是合理谈判的方式，这背后都需要一个完整且全面的策略，否则一不小心就会再次成为攻击者的猎物。

区块链的匿名性和去中心化性导致被盗资金追回难度大，然而，用户和项目方仍可以通过以下方式增加追回资金的可能性：

1）立即通知相关机构：向当地执法机构、金融监管机构和相关的区块链项目团队报案和申诉。提供详细的信息和证据，并配合相关机构的调查；
2）联系交易平台：如果资金被盗是在某个交易平台上发生的，立即与其联系，并提供有关事件的详细信息。交易平台可能会采取措施调查并协助解决问题；
3）与社区合作：将事件公之于众，并与相关社区成员合作，共享信息和经验。其他用户可能提供有关攻击者或攻击技术的有用信息；

4)寻求专业帮助:咨询专业的区块链安全公司或律师，寻求法律和技术方面的专业帮助。他们可以提供相关建议和指导，帮助尽可能追回资金或采取其他合适的法律措施。

当然，最重要的是采取预防措施，降低资金被盗的风险，包括使用安全可靠的钱包和交易平台;保护好私钥和访问凭证;避免点击可疑链接和下载未知来源的软件;以及保持安全意识和知识更新。

三、反洗钱

1、反洗钱及监管动态

2023 上半年部分反洗钱及监管动态如下:

Tether:2023 上半年共计屏蔽了 85 个 ETH 地址，这些地址上的 USDT-ERC20 资产被冻结不可转移。

Circle:2023 上半年共计屏蔽了 20 个 ETH 地址，这些地址上的 USDC-ERC20 资金被冻结不可转移。

ChipMixer:3 月 15 日，据欧盟执法合作署 (Europol) 表示，德国和美国相关机构已从加密货币混合器 ChipMixer 没收 4400 万欧元资金。欧洲刑警组织表示有关当局关闭了该平台的基础设施，没收了四台服务器、7 TB 数据和 1909.4 BTC（4770 万美元）。

美国财政部:4 月 24 日制裁了三名为朝鲜黑客团队 Lazarus Group 提供支持的朝鲜人;5 月 20 日制裁帮助俄罗斯转移资金的加密钱包;5 月 24 日制裁与朝鲜政府有关的加密钱包。

中国香港:5 月 31 日，香港虚拟资产评级机构 HKVAC 宣布正式成立，并将推出“虚拟资产指数”及“虚拟资产交易所评级”。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。

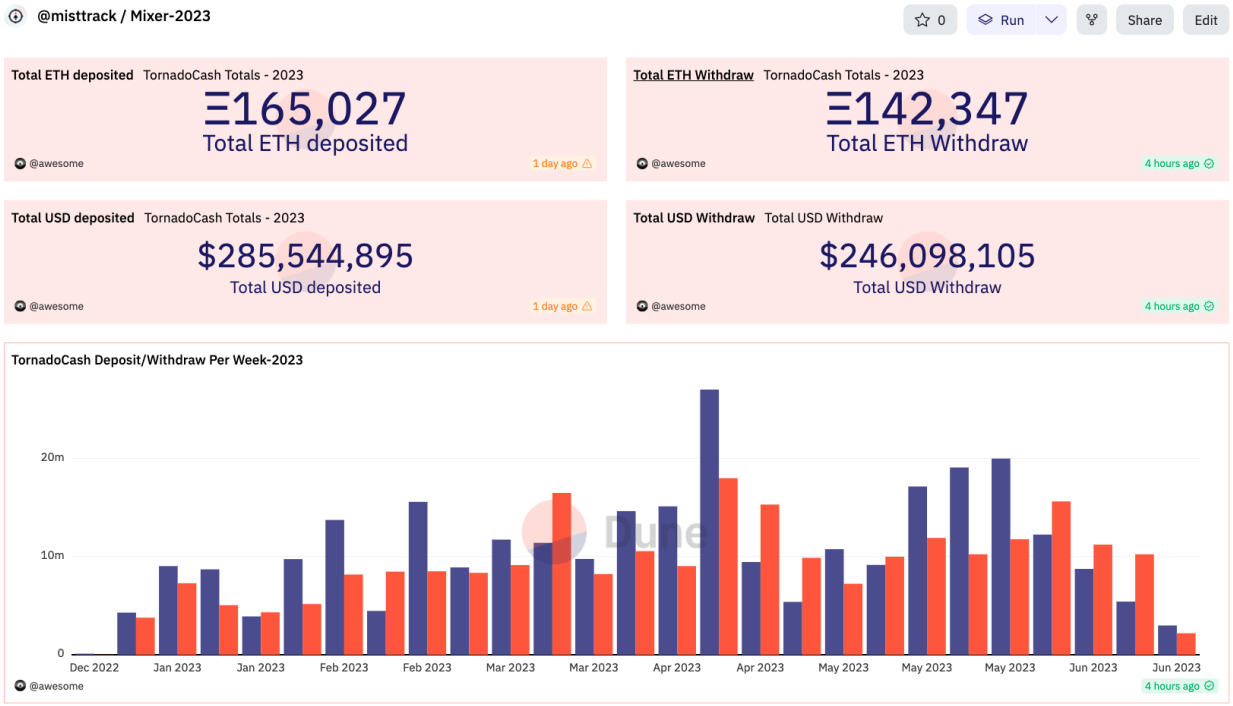
印尼:6 月 18 日，印尼商品期货交易监督机构 (Bappebti) 发布了在印尼可交易的加密资产清单。同时印度尼西亚计划于今年建立由国家支持的加密交易所。

英国：6 月 19 日，英国上议院投票通过了《金融服务和市场法案 (Financial Services and Markets Bill, FSMB)》，该法案将加密货币的相关金融活动和市场活动定义为一种受监管的活动，并将稳定币视为一种合法的支付方式来实施金融监管。

法国：6 月 19 日，法国市场监管机构发布关于 DeFi 的讨论文件，表示支持 DeFi 全球规则。

2、混币平台

2.1 Tornado Cash



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

2023 上半年用户共计存入 165,027 ETH（约 2.85 亿美元）到 Tornado.Cash，共计从 Tornado.Cash 提款 142,347 ETH（约 2.46 亿美元）。

2.2 eXch

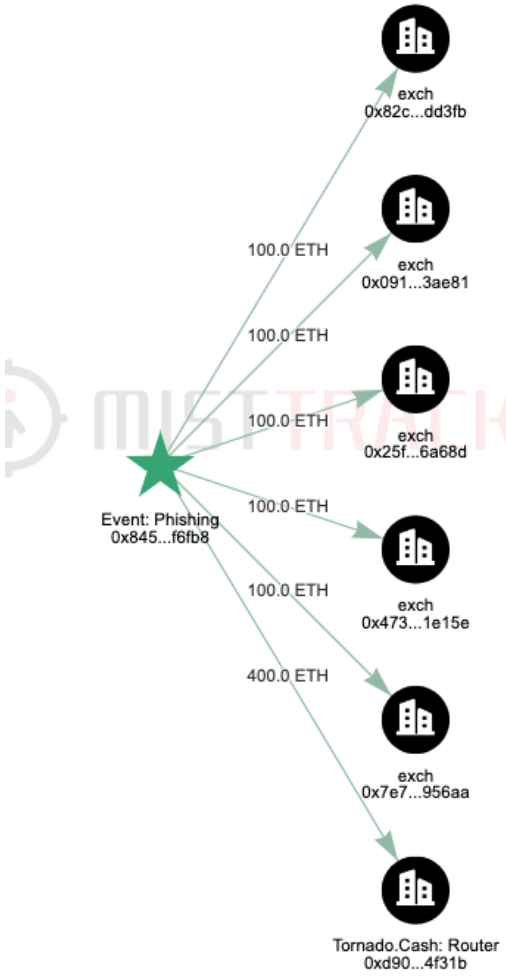
(https://dune.com/misttrack/mixer-2023)

2023 上半年用户共计存入 9,983 ETH（约 1772 万美元）到 eXch，共计存入 6,608,354 ERC20 稳定币（约 660 万美元）到 eXch。

3、钓鱼团伙

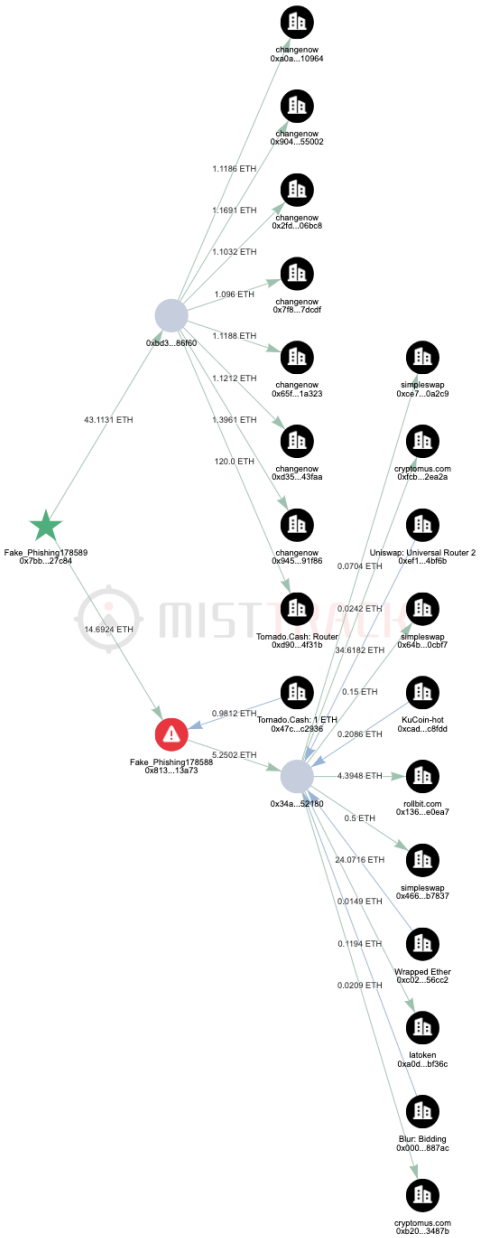
3.1 Pink Drainer

6 月 9 日，发生了多起 Discord 和 Twitter 被黑事件，包括 Evomos, Pika Protocol, OpenAI CTO, Orbiter Finance 等。这些事件都与一个名为 Pink Drainer 的组织有关，他们通过社会工程攻击获取 Discord Token，再通过 Discord 管理员帐户发送网络钓鱼链接，许多用户误打开恶意网站并签署恶意签名，导致资产损失。据数据，该团伙已经盗窃了约 300 万美元的资产，受害人近 1932 人。其中，一位受害者损失了价值近 32 万美元的 NFT。



3.2 Vemon Drainer

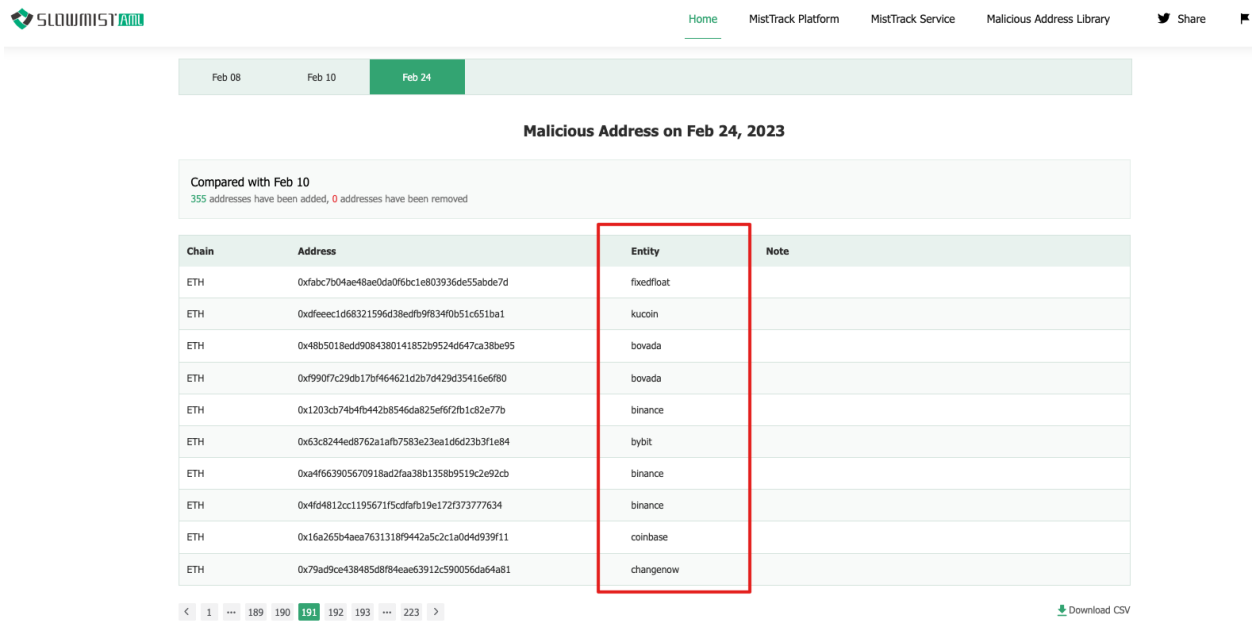
Venom Drainer 是一个钓鱼服务提供商。根据 ScamSniffer 的数据，该团伙已经从 15000 名受害者那里骗取了 2700 万美元。该服务商创建了超过 530 个钓鱼网站，针对包括 Arbitrum、Blur、zkSync、Optimism 和 MetaMask 等在内的170 多个品牌进行攻击。他们使用各种骗术，如通过 Permit 或 Approve 获得用户的批准，然后转移用户的 ERC20 代币到链上，或者诱骗用户签署恶意 NFT 列表，这些恶意列表包含更低的上市价格，通常为 0。一旦用户签署，他们的 NFT 可以通过列表签名被转移。该团伙声称已经实现了基于 Blur 的钓鱼模块，并从 3 月 20 日开始尝试招募人员，以便向知名的加密项目 Discord 的管理员发送私人消息或工单，以参与发起钓鱼活动，并获得 15% 的收益分成。根据 MistTrack 分析，Venom Drainer 团伙主要通过 Tornado Cash、ChangeNOW、SimpleSwap 等平台洗钱。



3.3 Monkey Drainer

Monkey Drainer 是一个臭名昭著的网络钓鱼组织，曾窃取数百万美元。2023 年 3 月 1 日，Monkey Drainer 突然关闭服务并销毁了所有相关文件、服务器和设备。据慢雾分析，该组织主要通过虚假大 V 推特账号、Discord 群等发布虚假 NFT 相关的带有恶意 Mint 的诱饵网站进行钓鱼，涉及 2000 多个域名。钓鱼模板使用了供应链灰色产业链提供的模板，如广告售卖说明、钓鱼供应链支

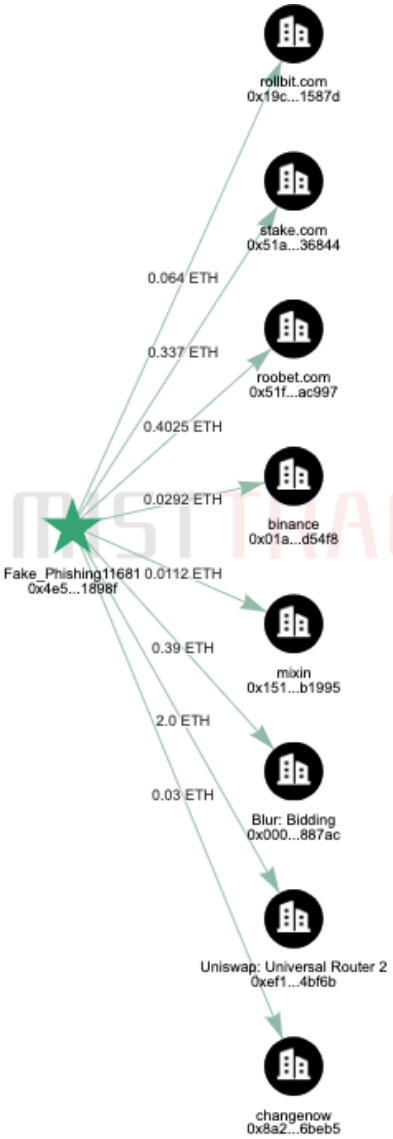
持功能。核心代码使用混淆、诱导的手段让受害者进行 Seaport、Permit 等签名，同时使用 Permit USDC 的离线授权签名机制等等，升级了原来的钓鱼机制。Monkey Drainer 组织通过钓鱼的方式共计获利约 16,506,602 美元，其中钓鱼 NFT 获利约合 9,374,344 美元，ERC20 Token 获利约 7,132,257 美元，其中主要获利 ERC20 Token 类型为 USDC、USDT、LINK、ENS、stETH。该组织没有在每个站点采用专门网站统计受害者访问记录这种功能，而是使用简单粗暴的方式直接钓鱼，批量部署，猜测是使用钓鱼模版批量化自动部署。



(https://aml.slowmist.com/events/monkey_drainer_statistics/)

3.4 Pussy Drainer

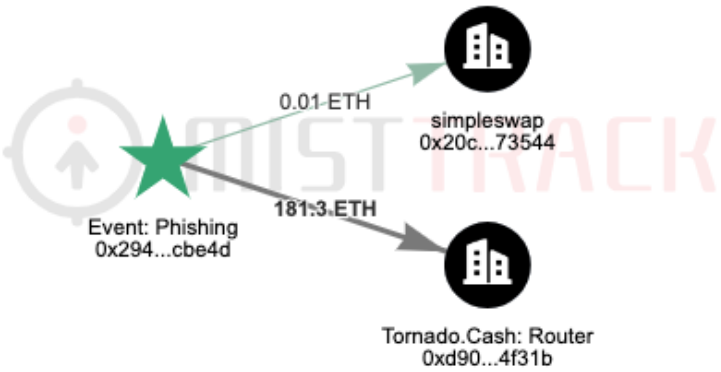
自 1 月 6 日起，Pussy Drainer 钓鱼活动导致了 3000 多人受害，总计被盗金额约为 1500 万美元。最大的受害者损失了价值 230 万美元的资产。



3.5 Inferno Drainer

5 月 19 日，一个名为 Inferno Drainer 的诈骗厂商逐渐露出水面，该厂商专门从事多链诈骗，主要收取被盗资产的 20% 费用。据数据，目前已发现近 4,888 名受害者，被盗资产约 590 万美元，自 3

月 27 日以来，Inferno 已经创建了超过 689 个钓鱼网站，针对的品牌超过 220 个。根据 MistTrack 分析，Inferno Drainer 团伙主要使用 Tornado Cash、SimpleSwap 等平台进行洗币。



4、黑客团伙

4.1 Lazarus Group

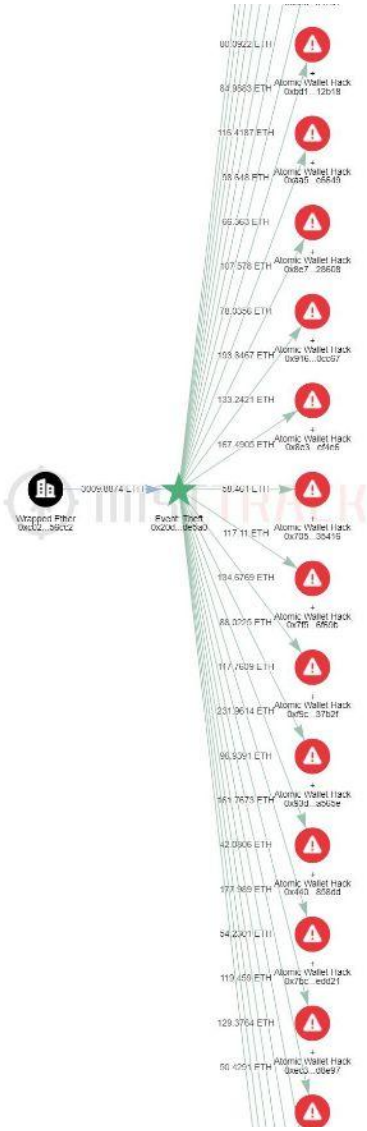
4.1.1 Harmony Hack

2022 年 6 月 23 日，Harmony 跨链桥遭受攻击，损失约 1 亿美元。今年 1 月 13 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，黑客将之前存放在交易平台的 BTC 资金转移。1 月 23 日，FBI 确认 朝鲜黑客团伙 Lazarus Group 应该对 Harmony Hack 事件负责。经过几天的多层转移，部分资金再次转移到交易平台，另一部分资金通过 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。在此过程中，黑客使用了新的洗钱方式，据 MistTrack 分析，其跨链路径为 BTC Network -> Avalanche -> ETH Network -> TRON Network。

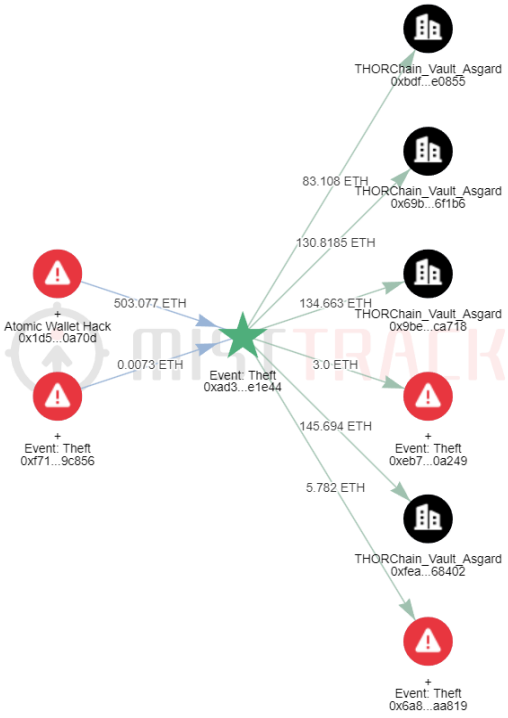
4.1.2 Atomic Wallet Hack

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。据 MistTrack 分析，目前已出现以下三种洗钱方式：

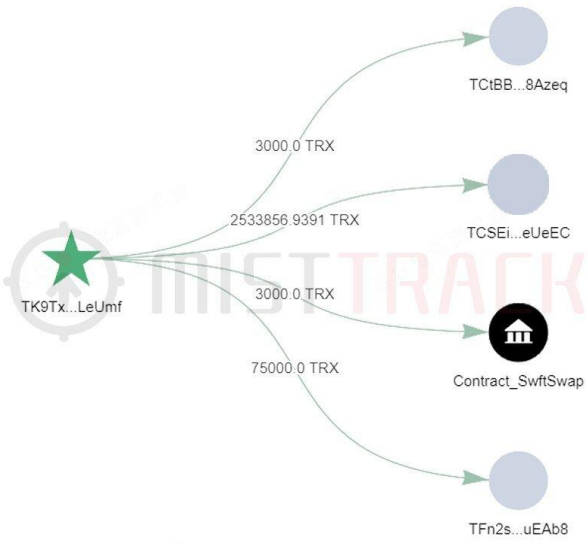
1) 黑客分别部署两个兑换合约，其一先将 ETH 兑换为 WETH，其二再将 WETH 兑换为 ETH。接着将兑换后的 ETH 分散转移到多个地址，并再次兑换为 WETH 后跨链到 Avalanche，最后将 WETH 换为 BTC，并从 Avalanche 跨链到 BTC 网络。



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。



四、总结

本报告主要介绍了 2023 上半年的区块链安全事件以及反洗钱态势。我们希望本报告能够为区块链行业和个人提供有价值的见解，帮助大家更好地理解和应对不断变化的区块链安全威胁，促进区块链安全的持续发展和创新，共同建立更安全、可信赖的区块链生态系统。

最后，致谢每一位生态伙伴。这其中包括我们的服务客户、媒体合作伙伴、黑手册贡献者、慢雾区伙伴。在此特别感谢 Safeheron, BugRap, Keystone, Scam Sniffer, GoPlus, Eigenphi, Chainbase, SunSec, Alphatu, Steven 等伙伴。正是你们的鼎力相助，更加坚定了我们不断进取、继续做好区块链守护者的决心，希望我们继续强强联合，并肩努力，为区块链黑暗森林带来更多的光亮。

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