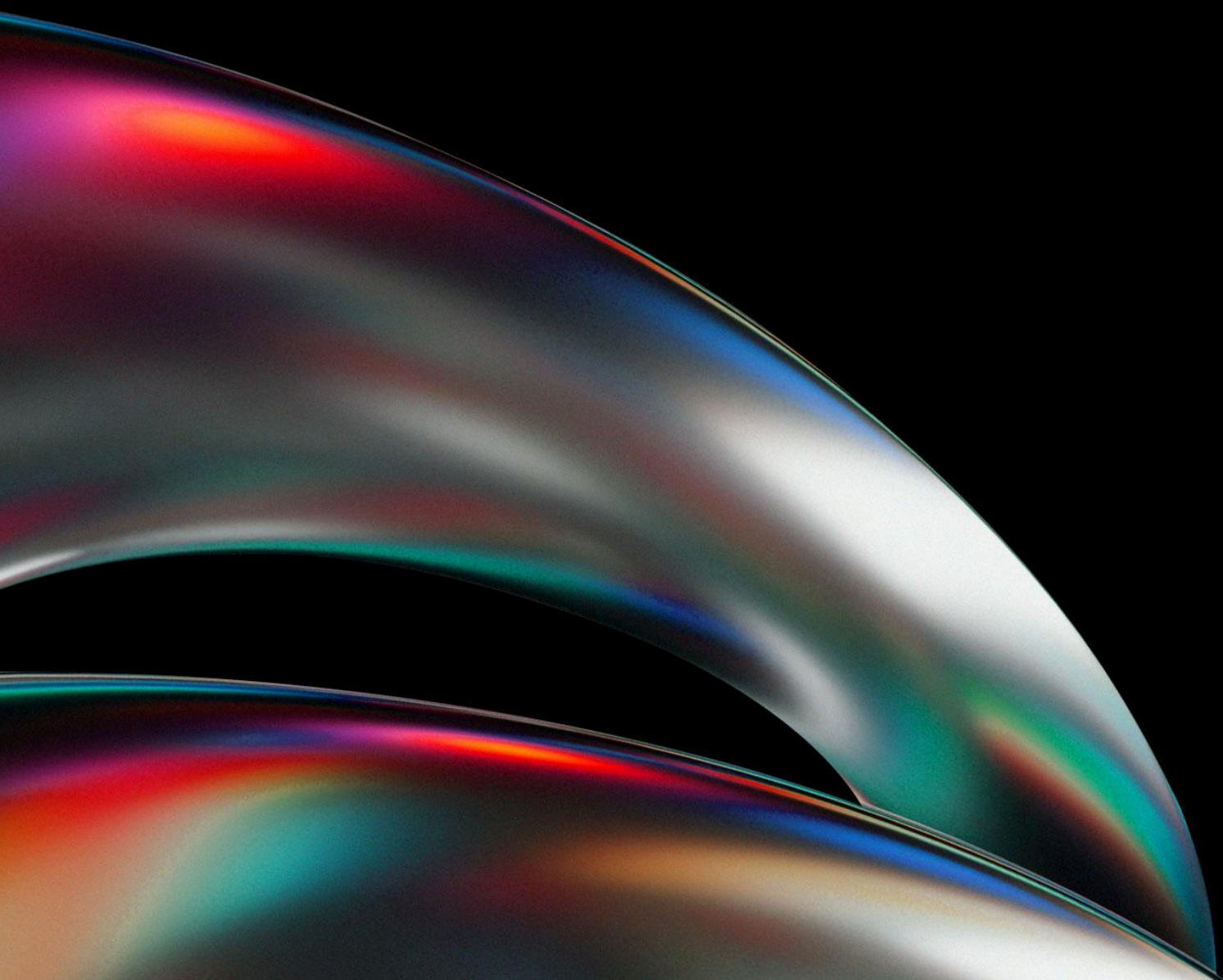
SLOWMIST 2024 上半年

区块链安全与反洗钱报告



目录

一、前言

2024 上半年，加密货币市场取得了重大进展，尤其是美国证券交易委员会（SEC）出乎意料地修改规则，允许创建现货以太坊交易所交易基金（ETF）。另一方面，监管机构继续集中发力于加密货币行业，对加密货币交易所及其部分高调高管进行了打击，包括前 FTX 首席执行官 SBF 的亲密盟友。

在监管政策方面，随着监管机构和公众对于加密货币及其背后的区块链科技的理解不断加深，各国在这个领域的政策态度出现了明显的不同。这些态度大体上可被划分为：积极拥护、模糊不定和严格禁止三种。虽然各国对于加密货币的态度不一，但毫无疑问，2024 上半年所产生的政策趋势标志着加密市场正处在合规化的进程中。与此同时，许多新兴趋势和主题正在涌现，加密货币用户和 Web3 开发者数量不断飞速增长，AI 模型逐渐变得完善。据 CoinMarketCap 的数据显示，截至 6 月 30 日，全球加密货币市场的总市值已经达到了约 2.34 万亿美元，这也充分展示了全球区块链市场的增长势头越发强劲有力。

在此背景下，本报告重点关注区块链生态系统安全和反洗钱（AML）安全两大方面：第一部分概述了 2024 上半年区块链的安全状况以及上半年常见的网络钓鱼/盗窃技术；第二部分回顾了反洗钱监管动态，分析了黑客团体和洗钱工具的活动，并提供了上半年安全事件冻结和归还资金的统计数据，由此探讨区块链生态的反洗钱情况，让大家对当前和未来区块链的安全风险有一个全面认识。

二、区块链安全态势

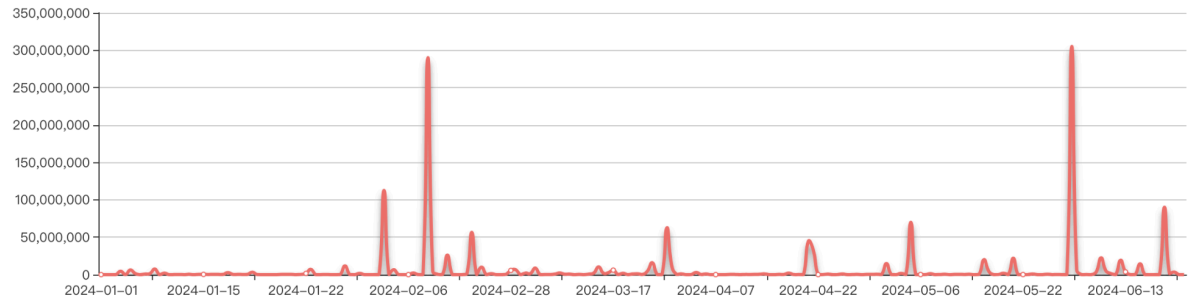
2.1 区块链安全事件总览

根据慢雾区块链被黑事件档案库 (SlowMist Hacked) 的不完全统计，2024 上半年安全事件共 223 件，损失高达 14.3 亿美元。对比 2023 上半年（共 185 件，损失约 9.2 亿美元），损失同比上升 55.43%。（注：本报告未将个人损失纳入统计）

[SlowMist Hacked Statistical]:

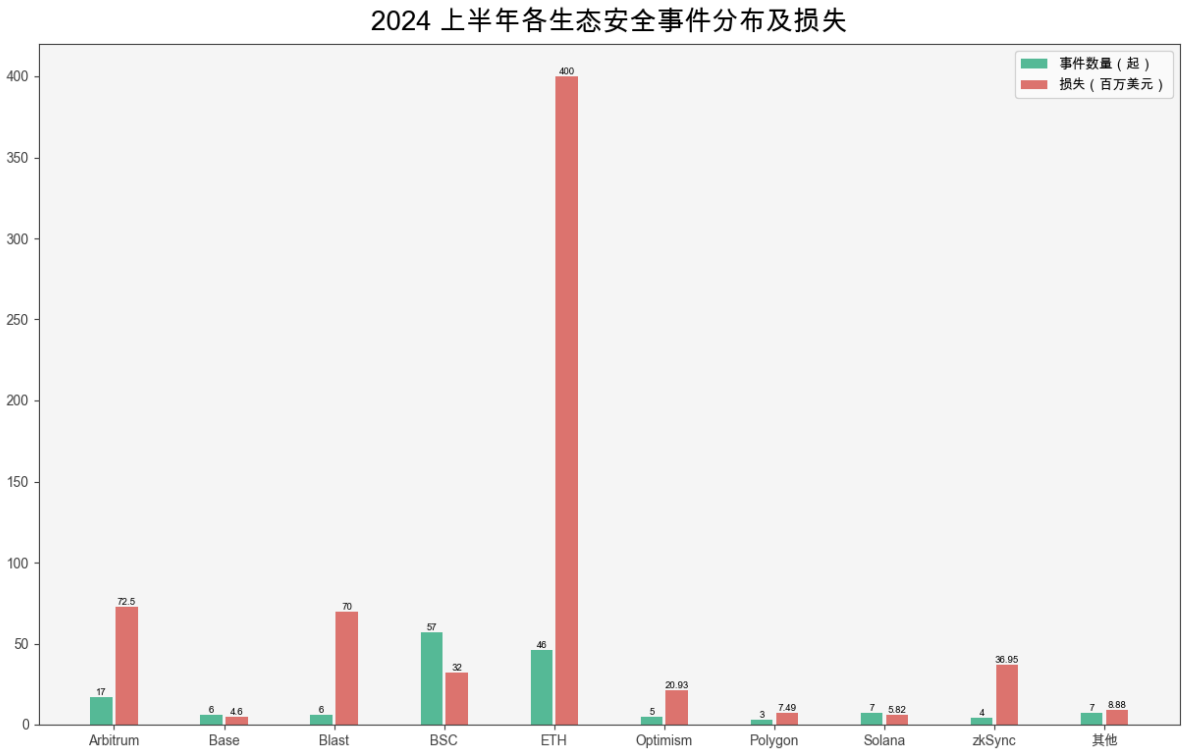
Total 2024 hack event(s) 223 ;

The total amount of money lost by blockchain hackers is about $ 1,433,749,533.00 ;



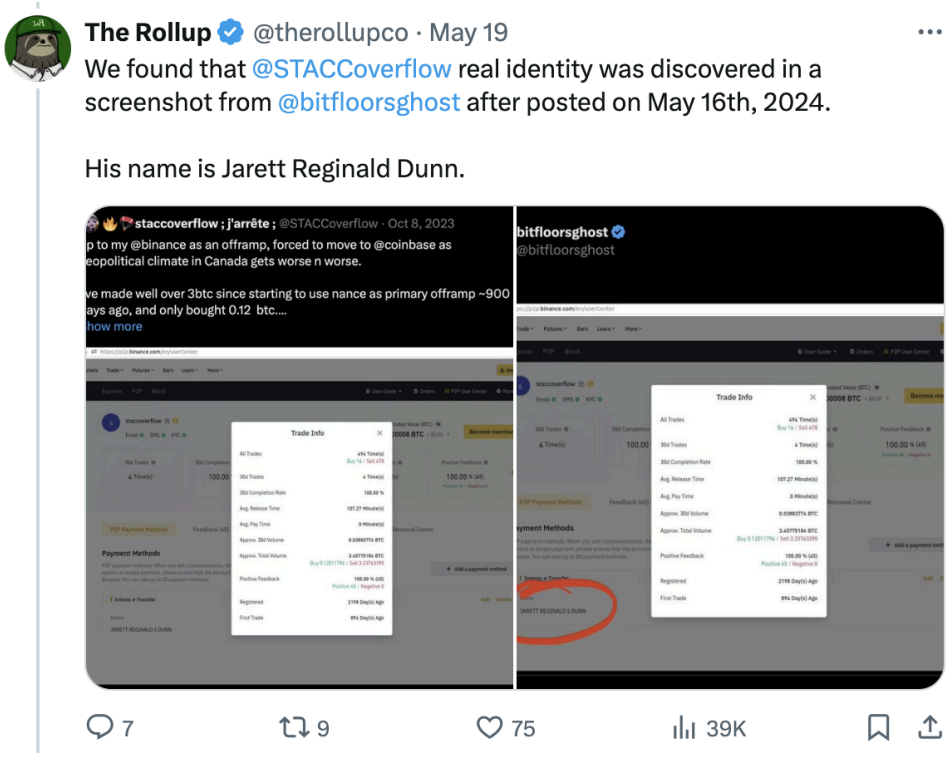
(https://hacked.slowmist.io/)

从生态来看，Ethereum 损失最高，达 4 亿美元。其次是 Arbitrum，约 7246 万美元，再者为 Blast，约 7000 万美元。此外，BSC 安全事件最多，达 57 件，损失约 3212 万美元。

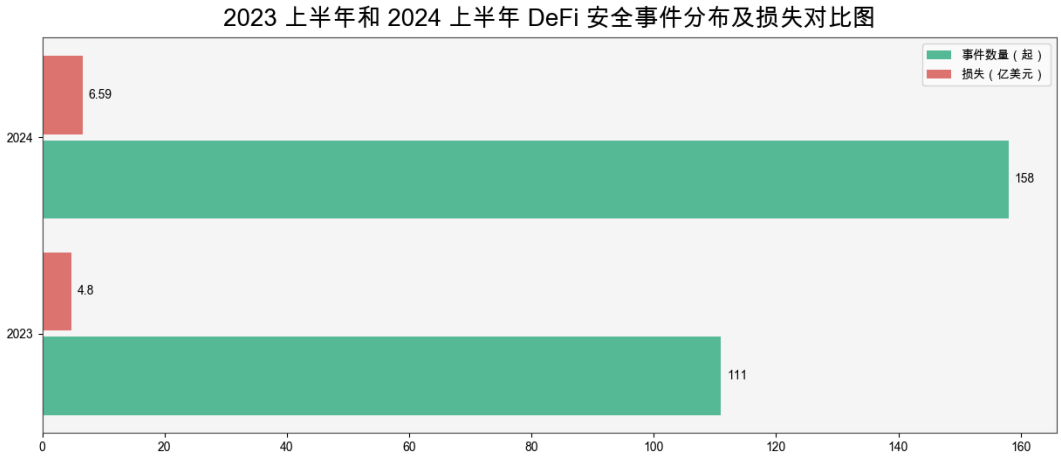


(2024 上半年各生态安全事件分布及损失)

值得注意的是，随着 Solana 在 2024 年迅猛崛起，其生态上的安全事件也明显增多。例如 5 月 16 日，基于 Solana 的代币启动器 pump.fun 遭遇闪电贷攻击，攻击者将价值 8000 万美元的资产随机空投至 Slerf、Stacc、Saga 等持有者地址。pump.fun 表示，攻击是因为某位前员工利用其在公司的特权非法获取了提款权限，借助借贷协议实施了闪电贷攻击，在其 bonding curve 合约的 4500 万美元流动性中，只有约 190 万美元受到影响。5 月 19 日，推特用户 The Rollup 称，pump.fun 攻击者 @STACCoverflow 在伦敦被英国执法部门逮捕并拘留，随后被保释，其真实名称或为 Jarett Reginald Dunn。



从项目赛道来看，DeFi 是最常受到攻击的领域。2024 上半年 DeFi 类型安全事件共 158 件，占事件总数的 70.85%，损失高达 6.59 亿美元，对比 2023 上半年（共 111 件，损失约 4.8 亿美元），损失同比上升 37.29%。



(2023 上半年和 2024 上半年 DeFi 安全事件分布及损失对比图)

其次是交易平台上的安全事件损失高达 5.24 亿美元，其中 DMM Bitcoin 事件就占据了 3.05 亿美元，该事件也是 2024 上半年损失最大的安全事件。5 月 31 日，日本加密货币交易所 DMM Bitcoin 表示，其官方钱包中的 4502.9 BTC 被非法转移，造成价值约 482 亿日元(3.05 亿美元)的损失。日本金融厅的一名代表表示已根据《支付服务法》向 DMM Bitcoin 发出报告请求令，要求其提供失窃原因报告和客户赔偿计划。DMM Bitcoin 表示目前共计筹集 550 亿日元(约 3.54 亿美元)，用于赔偿用户的、与被盗数量等值的比特币已于 6 月 14 日完成采购，且关于此次被盗事件的原因仍在调查中。据了解，DMM Bitcoin 安全事件的损失金额在加密货币黑客攻击史上排名第七，是自 2022 年 12 月以来最大的一次攻击。同时，此前日本曾发生过两起重大加密货币交易所黑客攻击事件，即 2014 年的 Mt.Gox 事件和 2018 年的 Coincheck 事件，被盗金额分别为 4.5 亿美元和 5.34 亿美元。此次 DMM Bitcoin 攻击事件价值成为日本第三大此类案件。

2024年5月31日（金）13時26分頃に、当社ウォレットからビットコイン（BTC)の不正流出を検知しました。

被害状況の詳細は引き続き調査中となりますが、現段階で判明しているものは下記の通りです。また、不正流出への対策はすでに行いましたが、追加の安全確保を行うべく一部サービスの利用制限を実施いたしました。

お客様にはご不便をおかけいたしますことを深くお詫び申し上げます。

■暗号資産の流出状況について

当社ウォレットより、不正流出したビットコイン（BTC）の数量は、4,502.9BTC（約482億円相当）と判明いたしました。

■お客様の預りビットコイン（BTC）について

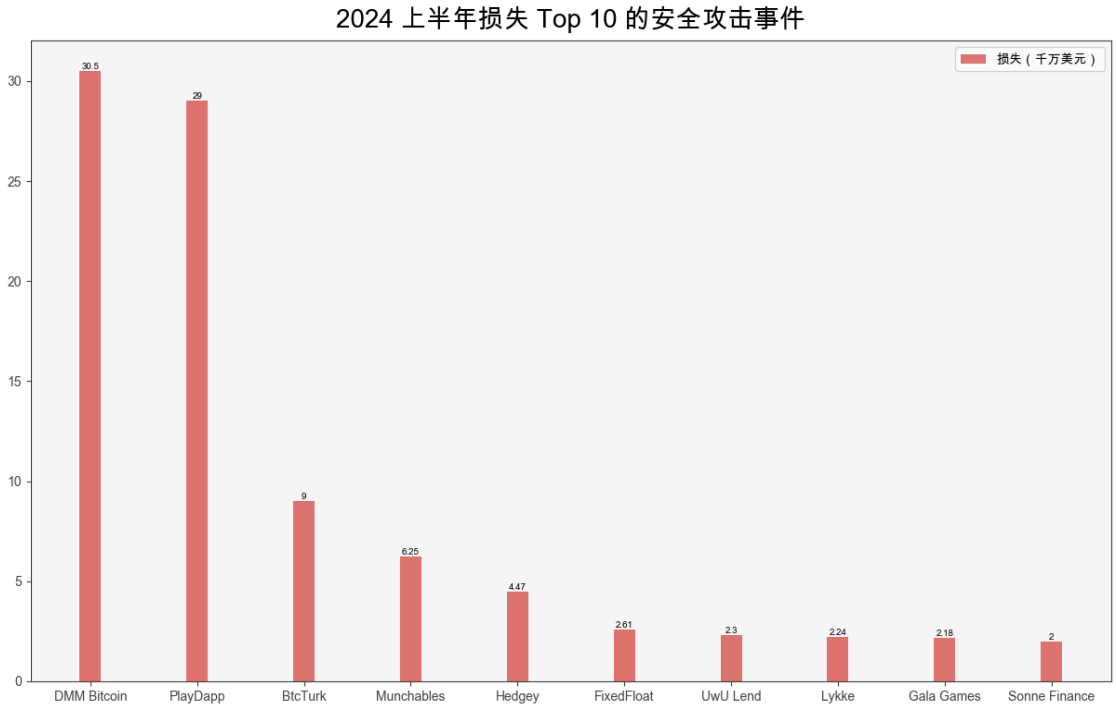
お客様の預りビットコイン（BTC）全量については、流出相当分のBTCを、グループ会社からの支援のもと調達を行い、全額保証いたしますのでご安心ください。

■サービスの利用制限について

以下のサービスの利用を制限させていただきました。

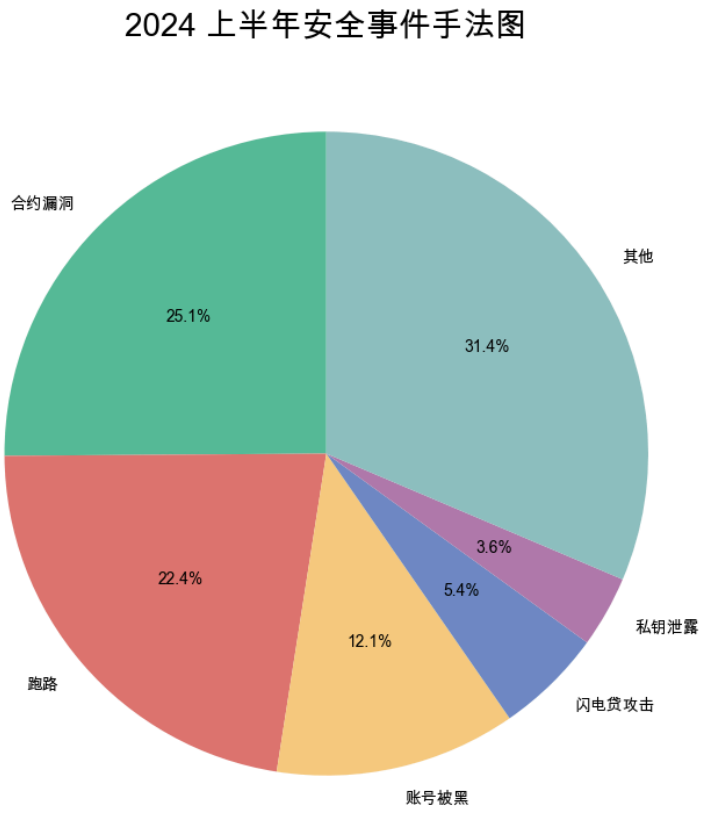
・新規口座開設の審査
・暗号資産の出庫処理
・現物取引の買い注文を停止（売却のみ受け付け）
・レバレッジ取引の新規建玉注文を停止（決済注文のみ受け付け）

从损失情况来看，有两起事件的损失规模达到上亿美元，以下为 2024 上半年损失 Top 10 的安全攻击事件：



(2024 上半年损失 Top10 的安全攻击事件)

从安全事件原因来看，合约漏洞事件最多，达 56 件，损失约 1.04 亿美元。其次为跑路导致的安全事件，达 50 件。2024 上半年损失第二大的 PlayDapp 事件，则是由于私钥泄露。2 月 10 日，基于以太坊的游戏平台 PlayDapp 表示由于私钥泄露遭受攻击，攻击者未经授权铸造了 2 亿枚 PLA 代币（价值 3650 万美元）。事件发生后不久，PlayDapp 通过链上交易向攻击者发送消息，要求归还被盗资金并提供 100 万美元白帽奖励，谈判失败；2 月 12 日黑客又铸造了 15.9 亿枚 PLA 代币（2.539 亿美元），并将资金分散到多个链上地址和交易平台。



(2024 上半年安全事件手法图)

2.2 钓鱼/盗窃手法

此小节摘取了慢雾 SlowMist 于 2024 上半年披露的部分钓鱼和盗窃手法。

2.2.1 相同首尾号钓鱼

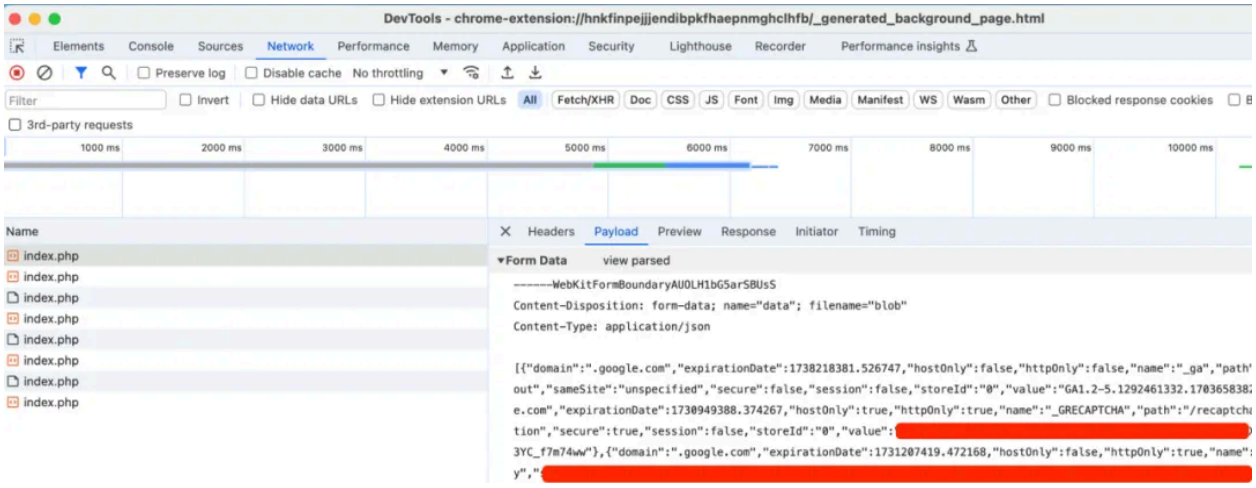
2024 年 5 月 3 日，据 Web3 反诈骗平台 Scam Sniffer 的监测，一名大额资产持有者（“巨鲸”）遭遇了相同首尾号地址钓鱼攻击，被钓走 1155 枚 WBTC，价值约 7000 万美元。这位受害者以 700 万

美元即可让攻击者安稳生活为由，而 7000 万美元的巨额赃款将可能为其带来无尽的麻烦，试图说服对方，且受害者多次通过链上信息向攻击者传达让其保留 10% 的赃款，希望剩下 90% 能归还的意愿。初期，攻击者并无反应，几天后突然转了 51 个 ETH 给受害者，并让受害者留下 Telegram 号，最终攻击者将资产全部归还。

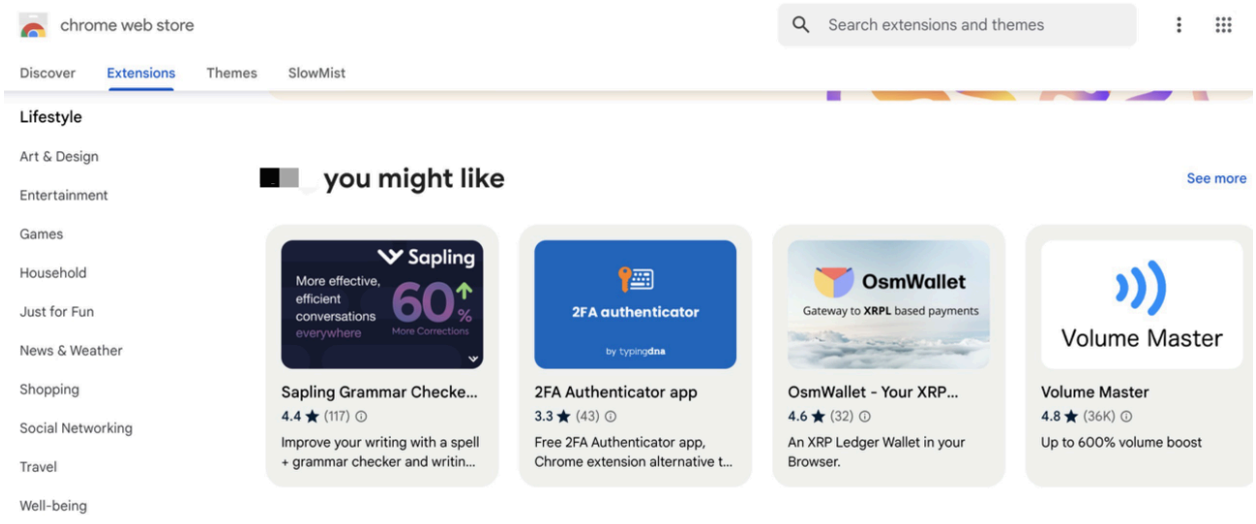
相同首尾号钓鱼攻击手法已经存在很长一段时间，但此次事件的损失数额实在巨大。一般来说，攻击者会提前批量生成大量钓鱼地址、分布式部署批量程序，瞄准交易规模较大或频率较高的用户，一旦这些用户发生转账，黑客会立即使用碰撞出来的钓鱼地址不断往用户地址空投小额资金（例如 0.01 USDT、0.001 USDT、0 ETH 等），利用攻击者地址首尾数和用户地址首尾数几乎一样的特点向目标转账地址发起钓鱼攻击，对用户的交易记录进行污染。由于用户习惯从钱包历史记录里复制最近转账信息，且一般只会注意首尾几位数字，稍有不慎就可能导致资产损失。建议用户将常用转账地址保存到钱包的地址簿当中，下次转账可以从钱包的地址簿中找到，同时开启钱包的小额过滤功能，屏蔽此类恶意转账，减少被钓鱼风险。总的来说，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，务必仔细核对地址，对于此类突然出现的转账记录，用户必须保持警惕，不可因一时贪图小利而忽视风险。

2.2.2 恶意扩展程序

2024 年 3 月 1 日，有推特用户反馈其账户存在异常情况，损失了 100 万美元，但未引起公众的关注。5 月，有网友怀疑受害者可能安装了一个有高度评价的恶意扩展程序（暂未与受害者直接核实此信息），它可以窃取用户访问的网站上的所有 cookies，并且有人付钱给一些有影响力的人来推广它。由于 Google 已经下架了该恶意扩展，我们只能通过快照信息中的历史数据进行调查。在测试过程中，我们发现该扩展程序中潜藏了一些可疑的恶意代码，测试过程中 cookies 被发送到了外部服务器，这就导致攻击者拿到用户认证、凭证等信息，在一些交易网站进行对敲攻击，盗窃用户的加密资产。



Chrome 扩展（Chrome Extension）是为 Google Chrome 设计的插件，用于增强浏览器的功能并优化用户体验。它们一般由 HTML、CSS、JavaScript 以及其他网页技术构建，通常包括基本信息配置文件 manifest.json，背景脚本，内容脚本，及用户界面等部分。Chrome 扩展的应用覆盖各类浏览场景，例如广告拦截 uBlock Origin、隐私与安全工具 LastPass、生产力工具 Todoist、开发者工具 React Developer Tools 及 加密货币工具 MetaMask 等，为我们的工作和生活提供了许多便利。



然而，Chrome 扩展在获取特定功能所需的权限后，可能访问用户敏感数据，如 cookies 和认证信息等。这一点在使用恶意的 Chrome 扩展时尤其明显，恶意扩展可利用已请求的权限直接访问和操作用户的浏览器环境和数据。例如，通过广泛的权限访问，操作网络请求、读取和写入页面内

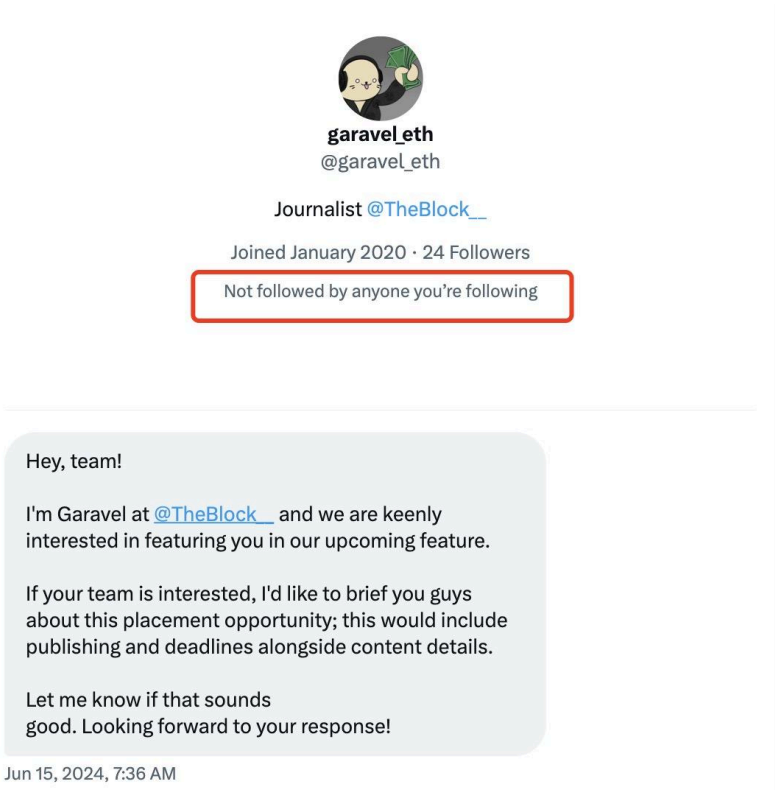
容、访问浏览器存储、操作剪贴板以及伪装成合法网站等方式，盗取用户的权限和认证信息。如果恶意扩展盗取了 cookies，它可能会访问账户、更改账户设置、提取资金，甚至冒充用户进行社会工程攻击。面对这一情况，用户可能会产生诸如断网或者更换设备等极端想法。然而，事实上我们可以采取更合理的方式防范风险：

对于个人用户，建议只安装来自可信来源的扩展，安装不同的浏览器以隔离插件和交易资金，安装杀毒软件（如卡巴斯基、Bitdefender、AVG）并定期检查设备，提高对于 Chrome 扩展权限请求的审慎性，以保护自身信息与资金安全；对于交易平台，可以全局启用二次验证 (2FA) 并采取多种验证方式，如短信、邮件、Google Authenticator 和硬件令牌，及时向用户发送有关账户登录、密码更改、资金提取等重要操作的通知，提供紧急情况下用户可以快速冻结账户的选项。同时，使用机器学习和大数据分析监控用户行为，识别异常交易模式和账户活动，对频繁更改账户信息、频繁尝试登录失败等可疑行为进行预警和限制。还可以通过各渠道向用户普及安全知识，提示用户注意浏览器扩展的风险和如何保护账户，提供官方的浏览器插件或扩展，帮助用户增强账户安全。

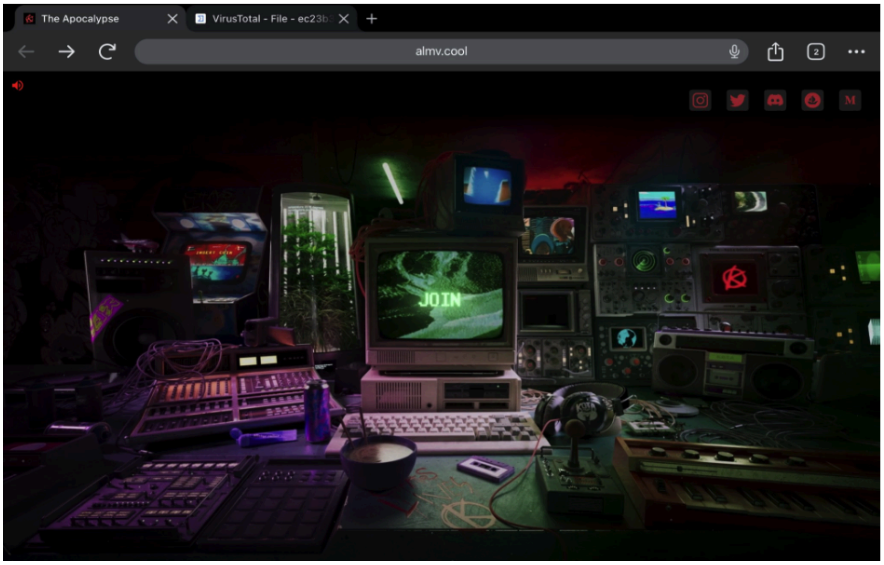
2.2.3 恶意木马程序

恶意木马程序也是加密货币领域一种频繁出现的威胁，攻击者通常将木马程序伪装成其他类型的程序或者文件来欺骗用户下载和安装，一旦入侵用户的电脑或移动设备，就会在后台运行并进行各种恶意活动。

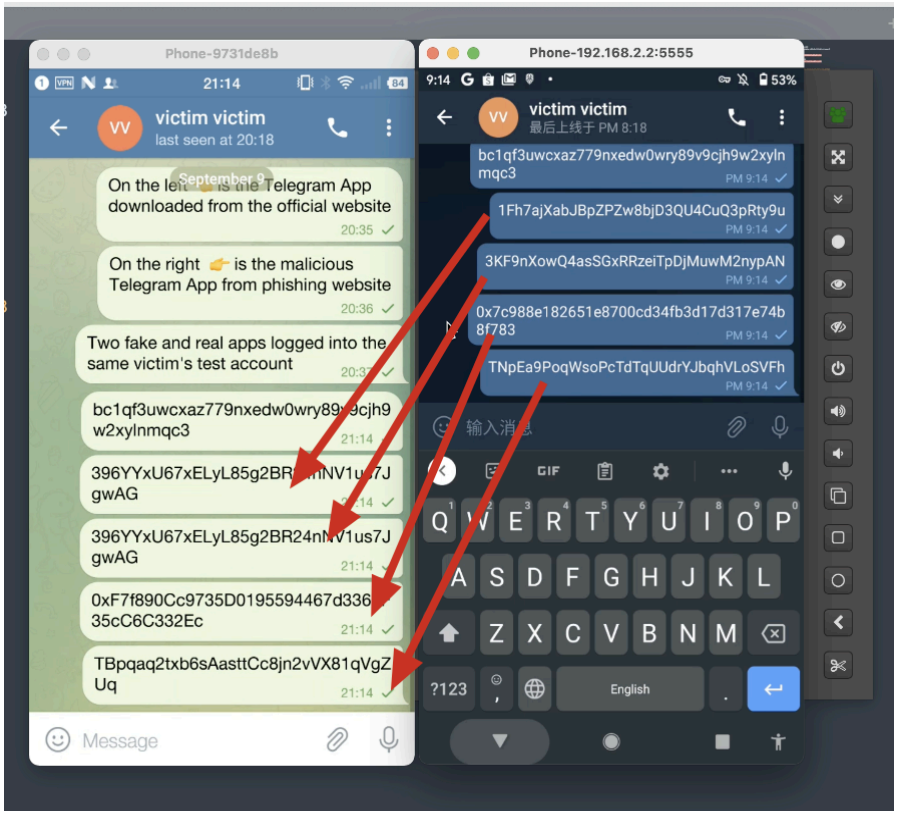
例如，许多骗子以“寻找兼职翻译、知名媒体记者采访、伪装成投资人提出合作”等为诱饵，骗取用户信任，并让用户下载所谓的可即时翻译的会议软件。然而，这个“会议软件”实际上就是一个木马程序。利用 Whois 查看其域名信息，往往会发现这个软件的“官网”是近期新注册的，再深入挖掘，可能会发现该域名 IP 过去有被标记为恶意的记录。一旦用户下载了这个“会议软件”，它会扫描用户电脑上的文件，然后过滤包含 Wallet、Key 等关键词的文件上传到攻击者远端控制的服务器，达到盗取加密货币的目的。一般来说，在线杀毒软件能分析的文件大小约 50 M，PC 端杀毒软件能分析的文件大小约 500 M，有些木马文件巨大就是为了躲避杀毒软件的查杀，这些木马大多以每月 100 美元的价格被提供给犯罪分子，而木马创建者轻松入账。



据受害者反馈，有些骗子会以更巧妙的方式诱骗用户下载他们的钓鱼软件，如冠以“游戏测试”之名，设立看起来很真实的网站和全套白皮书，让用户下载游戏去体验和了解他们的"公司产品"，而这些“游戏”其实也是恶意程序。一不小心下载到链游木马，不论用户的电脑里有什么，木马都可以悄无声息地盗走，包括用户的钱包密码和本地文件，甚至还可能盗取用户浏览器中保存的各种账号权限、系统信息等个人隐私。



除此之外，利用通讯平台如 Telegram 传播木马的可能性较高。许多来自第三方的汉化版 APP，暗藏着钓鱼和后台木马的威胁，随意使用可能会引发电脑遭受病毒或木马的侵袭。例如受害者在收到其他人发送过来的钱包地址想要进行转账操作时，受害者在复制粘贴过程中，被感染的设备会将剪贴板上的地址更改为攻击者的地址，导致转账到攻击者的地址，造成资金损失。此外，部分木马程序甚至会记录用户的键盘输入行为，以获取用户的密码和私钥信息。

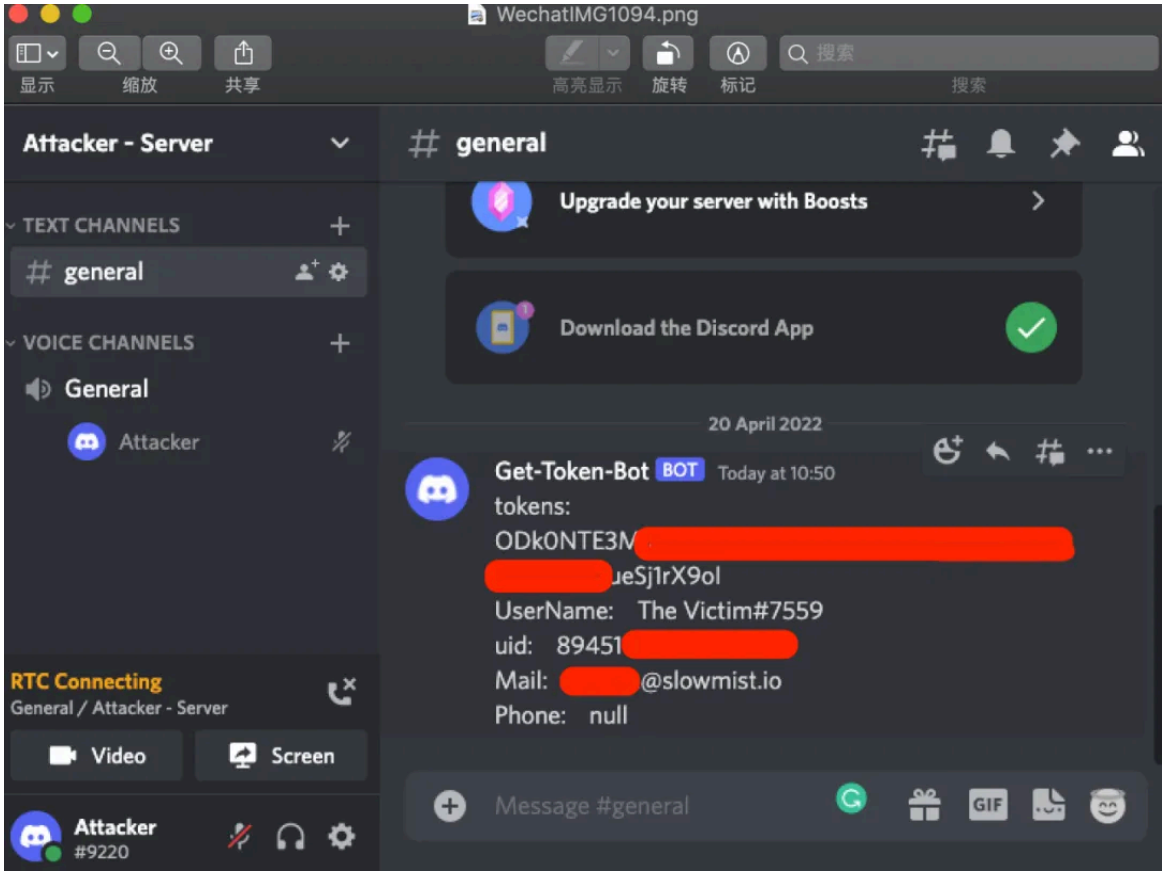


一旦遭遇木马攻击，应该立即断开网络连接，进一步阻止木马的活动；及时转移资金并更新各种在线账户和应用的权限设置；同时下载知名杀毒软件进行查杀，清除可能潜伏在你的设备上的恶意程序，必要时可以重置系统。为了避免遭遇木马风险，需要采取一些主动防御措施，例如重视安

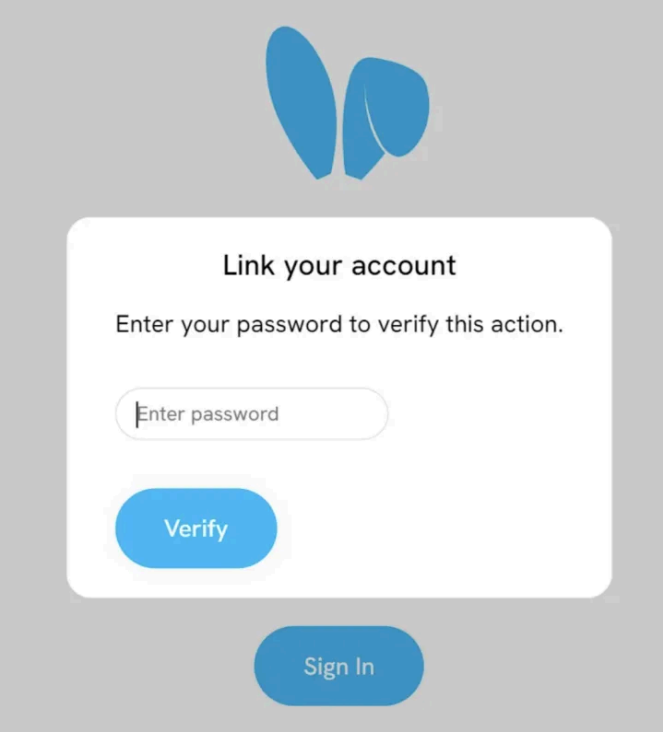
全更新，保持操作系统和你使用的安全软件始终处在最新状态；不要下载来源不明的文件、程序或点击来源不明的电子邮件、链接。对于大额的资产，尝试使用硬件钱包进行管理存储，这是一种更安全的方式；同时，定期备份和更新加密货币钱包是非常必要的。

2.2.4 恶意书签钓鱼

现行的浏览器均配有自带的书签管理器功能，其便利性无庸置疑。然而，这一便利性也可能成为黑客利用的工具。让你将精心构造恶意的钓鱼页面添加至书签中，这些页面中可能含有恶意 JavaScript 代码。当您点击该书签时，它会在当前浏览器标签页的域下执行。例如，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，如果攻击者获得项目方的 Discord Token 就可以直接自动化接管项目方的 Discord 账户相关权限，发布钓鱼链接，造成用户资金损失。理论上，浏览器是有同源策略等防护策略的，若操作不是 Discord 产生的，Discord 的页面上不应有任何响应，但恶意书签却能绕过这个限制，导致用户的 Token 和个人信息被发送到黑客的频道，权限一并失效。



以一个具体事件为例，受害者是去中心化社交平台 Friend.tech 用户，黑客冒充为知名媒体记者，并在推特上拥有上万粉丝。黑客以采访为由接触受害者（一个 KOL），并在采访结束后向他发送了一个含有恶意程序的钓鱼网页，让他填写资料。填写好资料后，受害者点击 Verify，这时网页提示出现错误，盗币者便引导受害者在 Google Chrome 里将 Verify 链接加到书签，让受害者打开 Friend.tech 后再点击该书签。按照这个操作，页面上弹出要求受害者输入密码的验证框。最终，受害者的 Friend.tech 帐户及相关资金被盗，共计损失约 14.2 ETH。



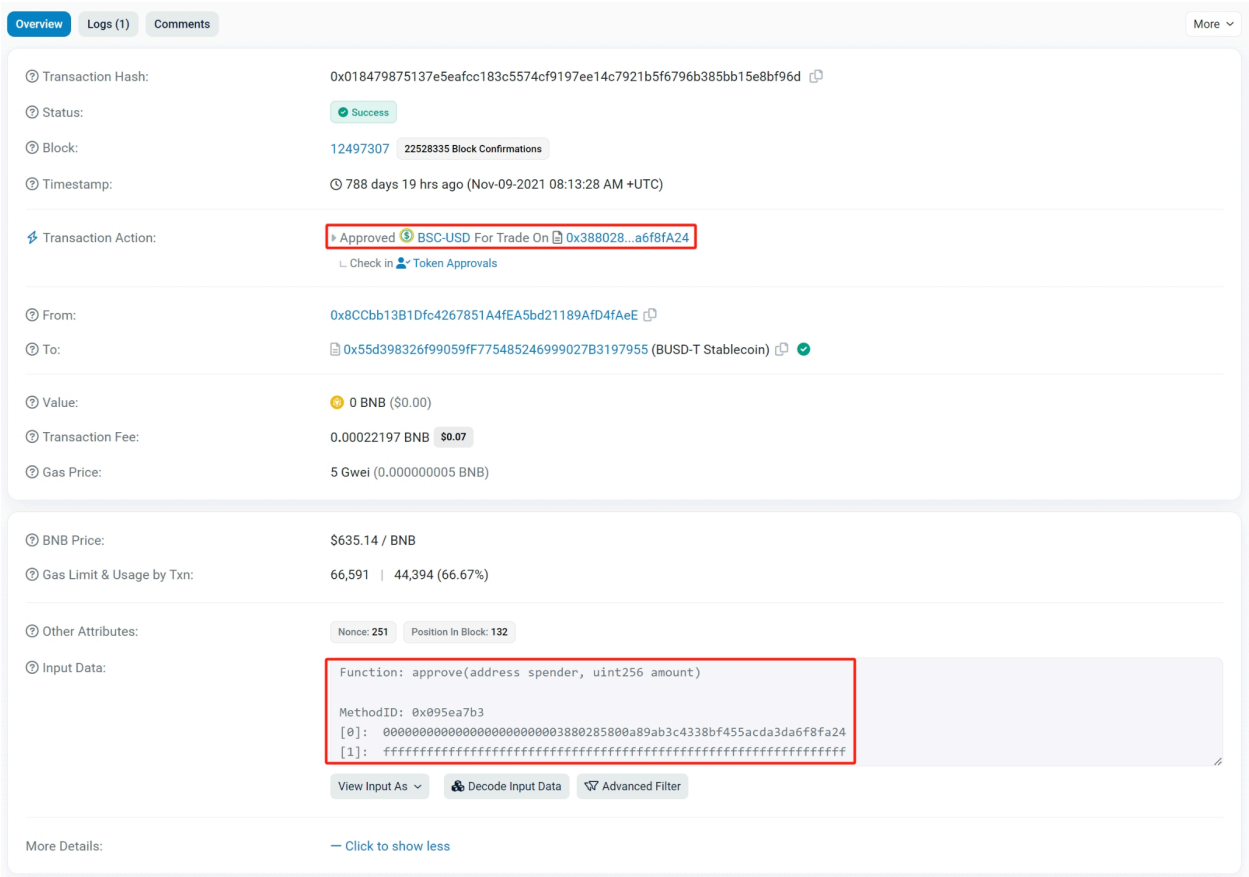
受害者在被盗后立即公开了遭遇，并寻求我们的帮助。我们追踪发现资金转到了一个平台，并立即联系该平台进行临时冻结风控。该平台表示在 72 小时内需要执法单位介入，否则无法继续冻结不法资金。在多方努力和协助下，受害者完成报案，并进入到与刑事局、检察官合作，向法院声请扣押裁定的流程。历经三个半月，受害者最终成功取回被盗资金。此案例具有特殊意义。受害者在意识到自己被诈骗后立即公开遭遇并联系了我们，我们在 6 小时内及时跟进并使用链上反洗钱追踪平台 MistTrack 进行分析，得出结果后迅速联系相关平台冻结了被盗资金。此案成为了一个里程碑，它或许是台湾司法历史上第一起没有嫌疑人信息、没有被告身份的情况下，仅通过区块链追踪分析证明非法资金流向与加密货币资产所有者，帮助执法机构进行冻结、扣押，并最后将资金返还给受害者的案件。作为用户，关键点在于尽管 Web 上有很多的扩展看起来非常友好和灵

活，但书签不能阻止网络请求，在用户手动触发执行的那一刻，仍需要注意任何添加操作和代码都可能是恶意的，始终对一切保持怀疑。

2.2.5 签名授权钓鱼

签名是资金安全的重灾区，“签名钓鱼”目前已成为威胁用户资产安全的主要攻击手段。此小节主要介绍种类繁杂的签名钓鱼方式中最常见的三种：

Approve 是存在于 ERC-20 代币标准中的常见授权方法。它授权第三方（如智能合约）在代币持有者的名义下花费一定数量的代币。用户需要预先为某个智能合约授权一定数量的代币，此后，该合约便可在任何时间调用 transferFrom 功能转移这些代币。如果用户不慎为恶意合约授权，这些被授权的代币可能会被立刻转移。值得注意的是，受害者钱包地址中可以看到 Approve 的授权痕迹。



Permit 是基于 ERC-20 标准引入的扩展授权方式，通过消息签名来授权第三方花费代币，而非直接调用智能合约。简单来说，用户可以通过签名来批准他人转移自己的 Token。黑客可以利用这种方法来进行攻击，例如，他们可以建立一个钓鱼网站，将登录钱包的按钮替换为 Permit，从而轻易地获取到用户的签名。

Permit2 并非 ERC-20 的标准功能，而是由 Uniswap 为了用户便利性而推出的一种特性。此功能让 Uniswap 的用户在使用过程中只需要支付一次 Gas 费用。然而，需要注意的是，如果你曾使用过 Uniswap，并且你向合约授权了无限额度，那么你可能会成为 Permit2 钓鱼攻击的目标。

Permit 和 Permit2 是离线签名方式，受害者钱包地址无需支付 Gas，钓鱼者钱包地址会提供授权上链操作，因此，这两种签名的授权痕迹只能在钓鱼者的钱包地址中看到。

鉴于签名钓鱼攻击的严重性和复杂性，我们建议用户务必对签名过程保持警惕，确保每一次签名操作的安全性。同时，要定期检查自身钱包地址的授权痕迹，不定时使用 Revoke.cash，ScamSniffer 等工具查看是否有异常授权并及时取消，避免资金损失。

三、反洗钱态势

3.1 反洗钱与监管动态

此小节将重点介绍加密货币领域反洗钱（AML）与监管动态的重大进展。

3.1.1 中国法院

2024 年上半年中国大陆法院共计有 163 个关于虚拟币的判决，其中刑事判决 121 起，民事判决 42 起。

3.1.2 中国香港

香港，作为全球金融和科技创新的重要枢纽，其在虚拟资产领域的政策动向对整个行业具有深远的影响。2024 年香港虚拟资产监管迎来了全面合规的新阶段。

2 月 8 日，香港政府就设立虚拟资产场外交易服务（OTC）提供者发牌制度的立法建议展开公众咨询。比如根据立法建议书，所有虚拟资产场外交易服务，不论是通过线下实体店（包括自动柜员机）还是线上网站服务都必须获得香港海关颁发的相关牌照。

3 月 12 日，香港金融管理局推出稳定币开发和发行的监管沙盒，遵循 2022 年开始的讨论文件。沙盒旨在鼓励在受控环境中安全开发稳定币，监管决策可以根据需要进行迭代。

4 月 15 日，中国公募基金旗下香港子公司博时国际、华夏基金（香港）、嘉实国际发行虚拟资产现货 ETF 产品已获得香港证监会原则上批准。

4 月 30 日，6 支香港首批发行的虚拟资产现货 ETF 正式在香港交易所敲钟上市，并开放交易，成为亚洲首批虚拟资产现货 ETF。

3.1.3 新加坡

1 月 18 日，新加坡金管局发言人表示，新加坡散户投资者可参与的集体投资计划（collective investment schemes，简称 CIS）受《证券及期货法令》监管，涵盖 ETF。他们可投资的资产类型受限。目前，比特币和其他数码支付代币（加密货币）（DPT）不属于零售 CIS 的合格资产。

4 月 2 日，新加坡金融管理局（MAS）对支付服务法案（PS Act）及其附属立法进行了修订，扩大了 MAS 监管的支付服务范围，并对数字支付代币（DPT）服务提供商施加了用户保护和金融稳定性相关的要求。修订内容包括：规范 DPT 的托管服务、DPT 之间的传输及兑换的便利化，以及跨国汇款服务的规范化；赋予 MAS 权力对 DPT 服务提供商施加与反洗钱、反恐融资、用户保护和金融稳定性相关的要求；并设置过渡安排，要求相关实体在规定时间内向 MAS 通报并提交许可申请。

3.1.4 美国监管

- **SEC**

1. SEC 诉 TradeStation Crypto, Inc. 案：位于佛罗里达州普兰泰申的 TradeStation Crypto, Inc. 因未能注册其加密借贷产品的发行和销售，遭 SEC 指控。该产品允许美国投资者存入或购买加密资产以获得承诺的利息。TradeStation 同意支付 150 万美元的罚款以解决这些指控，体现了 SEC 监管加密借贷产品的承诺。

2. SEC 诉 Sewell 及 Rockwell Capital Management LLC 案：Brian Sewell 及其公司 Rockwell Capital Management 就针对 Sewell 在线加密交易课程"美国比特币学院"学生的欺诈指控达成和解。该欺诈计划使 15 名学生损失了 120 万美元，体现了 SEC 保护教育环境免受欺诈性投资计划侵害的努力。

3. SEC 诉 Lee 等人案：Xue Lee（又名 Sam Lee）和 Brenda Chunga（又名 Bitcoin Beautee）因参与加密资产庞氏骗局 HyperFund 而受到指控，该骗局从全球投资者那里筹集了超过 17 亿美元。此案凸显了 SEC 打击利用投资者信任、承诺不切实际回报的大规模国际欺诈行为的行动。

4. 比特币现货 ETF：2024 年 1 月 10 日，SEC 批准了几种现货比特币交易所交易产品（ETP）股票的上市和交易，此前的一项法院裁决批评了之前的不批准行为。主席 Gary Gensler 强调，此次批准仅限于比特币 ETP，确保它们提供充分的信息披露，并在防止欺诈的受监管交易所上交易。SEC 将执行现有的投资者保护标准，并密切监控合规情况。Gensler 还对比特币的投机性和风险性提出警告，建议投资者保持谨慎。

- **OFAC**

1. 美国财政部制裁逃避制裁的俄罗斯实体：2024 年 3 月 25 日，美国财政部外国资产控制办公室（OFAC）制裁了 13 家实体和 2 名个人，原因是他们在俄罗斯通过虚拟资产服务和技术采购协助规避美国制裁。其中包括五个由之前被指认者控制的实体。这些指认是继七国集团（G7）在二月份承诺打击逃避制裁行为后作出的，针对的是在俄罗斯对乌克兰的战争中支持俄罗斯金融基础设施的公司。值得注意的是，莫斯科的金融科技公司如 B-Crypto、Masterchain 和 Laitkhaus 等，因为俄罗斯金融机构提供交易便利而被指认。制裁将封锁所有被指认者在美国的财产，并禁止美国与他们进行交易。此外，帮助俄罗斯军事工业基地的外国金融机构也可能受到制裁。这一行动旨在遏制俄罗斯利用替代支付机制和虚拟资产来规避制裁和资助军事活动。

2. 美国制裁俄罗斯 LockBit 勒索软件集团关联方：2024 年 2 月 20 日，美国对俄罗斯 LockBit 勒索软件集团的关联方进行了制裁，将数名个人列入 OFAC 的特别指定国民（SDN）名单中。关键人物包括 Ivan Gennadievich Kondratiev，他有多个别名并与多个数字货币地址关联，以及 Artur Ravilevich Sungatov，他也与多个电子邮件地址和数字货币地址关联。这些制裁是为应对网络威胁和执行与乌克兰/俄罗斯相关的制裁法规而采取的部分持续努力。

3. 美国制裁网络犯罪组织 911 S5 僵尸网络：2024 年 5 月 28 日，美国制裁了一个与 911 S5 僵尸网络有关的网络犯罪网络，将若干个人和实体列入外国资产管制处的特别指定国民（SDN）名单。主要人物包括刘景平和王云禾，他们都持有多个数字货币地址，并与新加坡、泰国和中国的多个地点有关联。Lily Suites Company Limited、Spicy Code Company Limited 和 Tulip Biz Pattaya Group Company Limited 等实体也被指认。这些行动是打击网络犯罪和执行制裁法规更广泛努力的一部分。

3.1.5 欧洲议会

- 欧盟

2024 年 4 月 24 日，欧洲议会通过了加强打击洗钱和恐怖主义融资的新法律。主要措施：包括公众可以访问过去五年的受益所有权登记信息；欧盟范围内的现金支付限额为 10,000 欧元；从 2029 年起加强对金融实体和足球俱乐部的尽职调查；在法兰克福设立一个新的机构 — 反洗钱局（AMLA），负责监督高风险实体并确保合规。这些法律旨在提高透明度，赋予金融情报机构权力，并对金融交易实施更严格的监管。

3.1.6 中东地区

- 土耳其

2024 年 6 月 27 日，土耳其议会通过了一项法案，对加密资产实施严格监管。未经授权的加密服务提供商将面临 3 至 5 年的监禁。资本市场委员会（SPK）将负责这些提供商的授权和监管，确保其符合既定标准。严重的处罚包括对挪用或滥用资源者判处最高 22 年的监禁。平台必须遵守透明、公平的市场惯例，并维护交易的安全记录。与银行相关的活动必须获得银行监管和监督局 (BDDK) 的批准。

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。随着加密货币市场的不断发展，健全的监管框架和国际合作对于应对其挑战变得越来越重要。

3.2 安全事件反洗钱

3.2.1 资金冻结数据

Tether：2024 上半年，共有 374 个 ETH 地址被风控，这些地址上的 USDT-ERC20 资产被冻结，不可转移。
Circle：2024 上半年，共有 28 个 ETH 地址被封锁，这些地址上的 USDC-ERC20 资金被冻结，不可转移。

在慢雾 InMist Lab 威胁情报合作网络的大力支持下，2024 上半年 SlowMist 协助客户、合作伙伴及公开被黑事件冻结资金约 2439 万美元。

3.2.2 资金归还数据

2024 上半年，遭受攻击后仍能全部或部分收回损失资金的事件共有 16 起。在这 16 起事件中，被盗资金总计约 1.13 亿美元，其中将近 9864 万美元被返还，占被盗资金的 87.3%。

3.3 黑客团伙画像及动态

3.3.1 Lazarus Group

2024 年，臭名昭著的朝鲜黑客组织 Lazarus Group 仍在加密货币相关的洗钱活动中扮演重要角色。根据最新统计数据，Lazarus Group 对大部分资金流入加密货币混合服务商 Tornado Cash 负有责任。

- 作案手法

Lazarus Group 将大量资金存入 Tornado Cash 以掩盖其资金来源，然后采用多层次混合策略进一步逃避侦查。下面是他们其中一种方法的详细示例，这种方法通常以 BTC 为目标，因为 BTC 有巨大的流动性池，使得洗钱更容易。

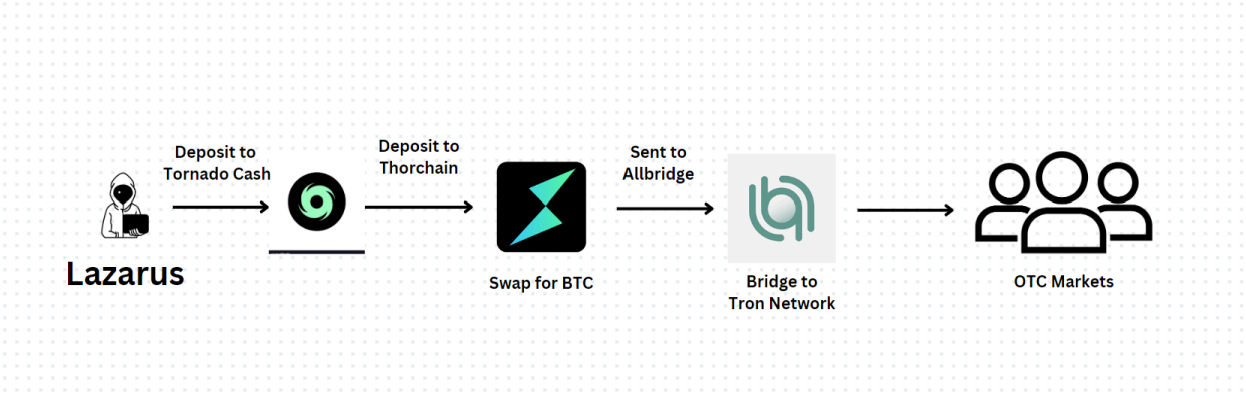
1. 在 Tornado Cash 初步混合：资金首先被存入 Tornado Cash，后与其他用户的资金混合，以切断交易线索并匿名化资金来源。

2. 通过 Thorchain 转换：将清洗过的资金发到跨链流动性协议 Thorchain，资金从以太坊转换为比特币，增加了一层混淆。

3. 分散到各地址：转换后的比特币被分散到不同的地址，使交易历史更加复杂，并分散了资金。

4. 跨链到 TRON：然后资金被跨链到 TRON 链，利用较低的监管审查进一步混合资产。

5. 场外交易（OTC）：最后，洗过的资金通过场外交易进一步清洗，使犯罪分子能够将数字资产转换为法定货币或其他加密货币，同时尽量减少 KYC 暴露。



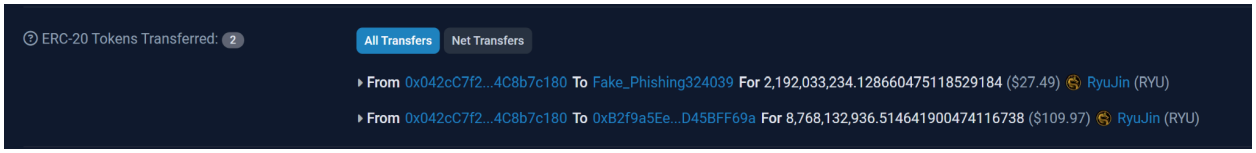
- 新的作案手法

随着新协议的不断发展，Lazarus Group 采用了越来越复杂的洗钱技术。他们复杂的作案手法涉及多层混合策略和利用各种区块链技术，包括跨链和去中心化交易所。使我们的调查更加复杂的是，Lazarus Group 开始利用 tBTC 协议将资金转移到以太坊，这也给监管机构和金融机构追踪和拦截非法交易带来了巨大挑战。

3.3.2 Drainers

Drainer 服务（Drain-as-a-Service），是指提供工具和基础设施，通过网络钓鱼攻击从受害者钱包中窃取加密货币的非法操作。这些服务，例如 Pink Drainer 和 Inferno Drainer，提供全面的网络钓鱼工具包并按佣金制运作，从被盗资金中抽取分成。尽管某些个别服务可能由于财务目标达成或执法压力而关闭，但新的服务不断涌现，使加密社区始终面临威胁。

有效判断自己是不是 Drainer 服务受害者的一种方法是检查的转账记录。通常，你的资金会被分配到两个地址，较小的金额是给 Drainer 服务，而较大的金额则被转移到诈骗者的地址。



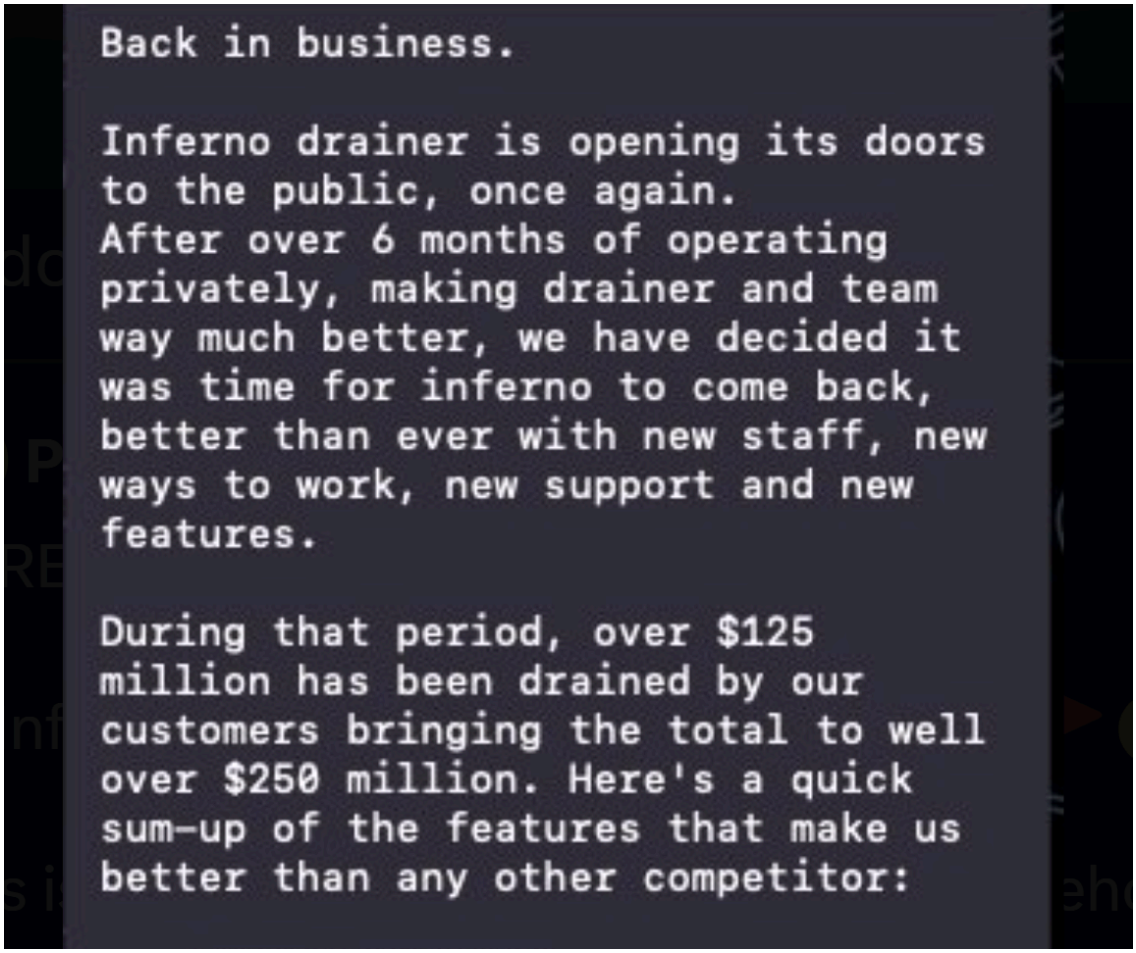
1. Pink Drainer：Pink Drainer 在帮助盗取 21,000 多名受害者超过 8,500 万美元后，最近宣布退出市场。该服务通过提供工具包供骗子使用，以诱骗受害者签署恶意合约来掏空其钱包。Pink Drainer 声称已实现其目标，并承诺安全销毁所有存储信息，以防止进一步使用。

Pink Private Announcements

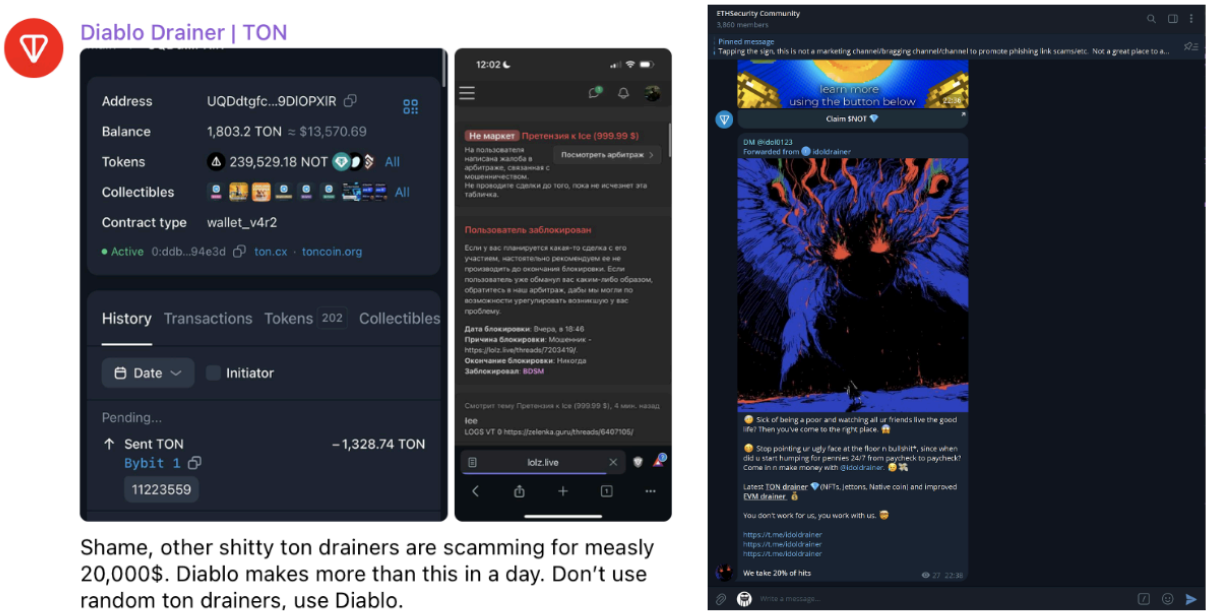
copy

```
We have reached our goal and now, according to plan, it's time to for us to retire.

After this message's publication, we will begin winding down all of our infrastructure. All
stored information will be wiped and securely destroyed.

We are truly happy to have supported all of you for over a year without any scams,
backdooring, or major incidents. This entire thing grew so much larger than we could have
even imagined it would have when we had started. We apologize for the lack of prior notice
about our departure, but I think most of you will understand.

Beware of impersonators; we are not planning on returning in the future. If any message
claiming to be from us is not signed by one of our wallets (0x636/0x9fa), it is not from us.

It is very likely that our retirement will have no major impact on the scene, people will
move on to other drainers just as quickly as they moved to us.

If you have enough money right now to financially support yourself, we advise you hold onto
it and take a step back from the grind and enjoy what this world has to offer. Life is too
short to get caught in the perpetual cycle of needlessly spending, going broke, and trying to
make it back.

We thank every single one of you for the trust, dedication, and respect you have shown to us
and our service, especially those of you who were here from the very beginning.

Goodbye. 💔
```

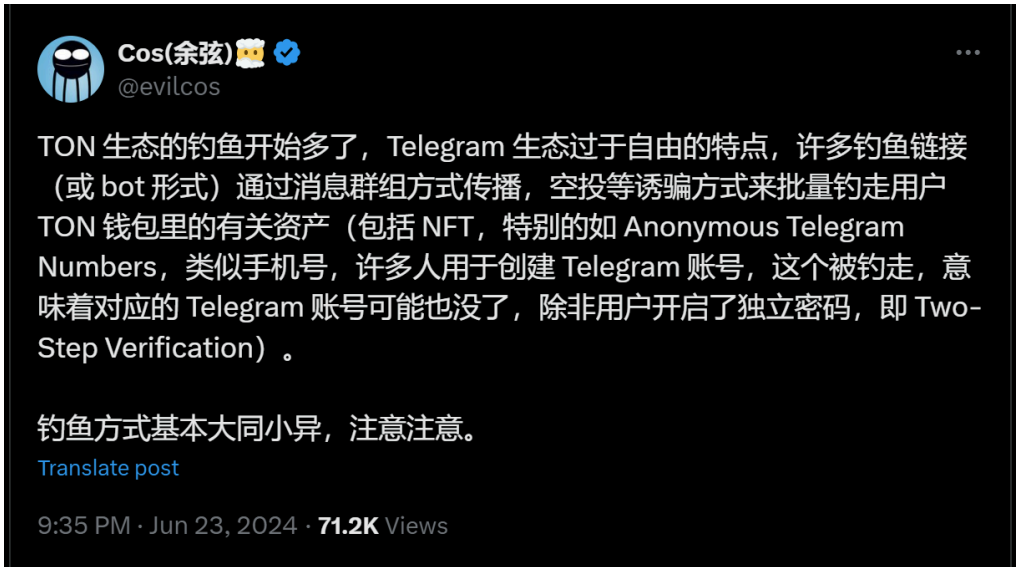
2. Inferno Drainer：Inferno Drainer 在停止运营前盗取了超过 2 亿美元的资产。其运营方式与 Pink Drainer 非常相似。近期，在 Pink Drainer 宣布退出后，Inferno Drainer 宣布将重新投入运营。



3. Diablo Drainer：虽然大多数 Drainer 专注于 EVM 链，但由于 TON 链的流行，我们最近看到 Diablo Drainer 对 TON 网络用户的攻击有所增加。这些服务通常使用类似的网络钓鱼策略和恶意合约签名来掏空加密钱包，它们通常在地下论坛或 Telegram 等加密消息渠道打广告。



4. TON 生态系统中的网络钓鱼活动



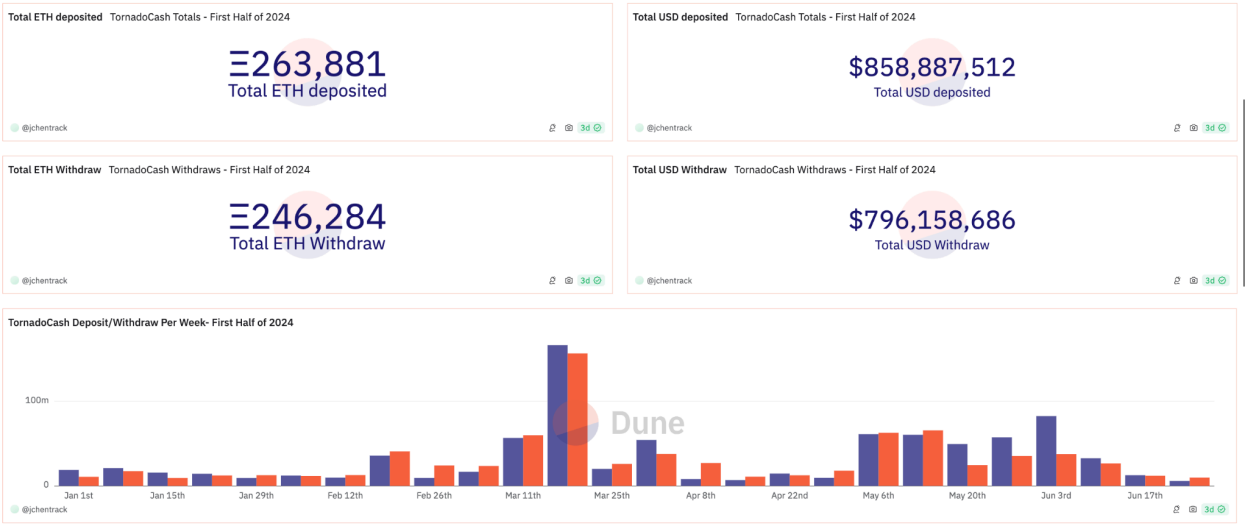
正如 SlowMist 的创始人 Cos 的推文所说，TON 生态系统中的网络钓鱼活动显著增加。Telegram 的去中心化性质和自由度使其成为作恶者的沃土。钓鱼链接通过信息群组、空投等诱骗方式钓走用户的 TON 钱包资产。值得注意的是，类似于手机号码功能的匿名 Telegram 号码已经成为创建

Telegram 账户的流行方法。然而，越来越多的这些号码被网络钓鱼。如果被盗用，这些号码可能导致相关的 Telegram 账户丢失，特别是对于那些没有启用两步验证的用户来说。

这些 Drainer 服务大多数都很隐蔽，运作得就像是普通的商业行为，而实际上它们在从毫无防备的受害者那里窃取资金。随着新的 Drainer 服务不断涌现，加密社区必须保持警惕，持续学习最新的网络钓鱼策略，并仔细检查异常交易。打击这些复杂骗局的斗争仍在继续，提高防范意识是第一道防线。

3.4 洗钱工具

3.4.1 Tornado Cash

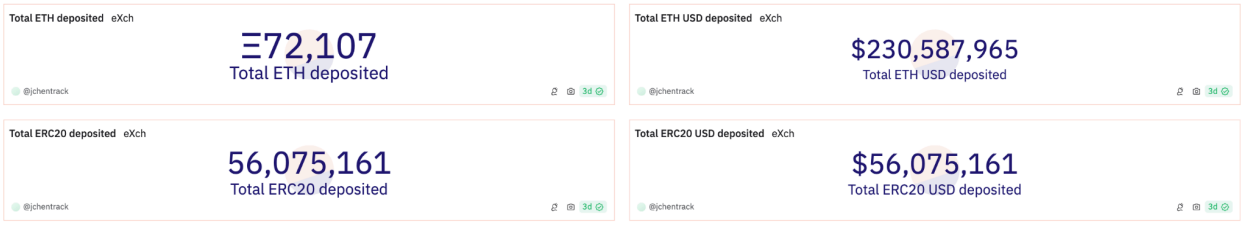


(https://dune.com/misttrack/first-half-of-2024-stats)

2024 年上半年用户共计存入 263,881 ETH（约 8.58 亿美元）到 Tornado Cash，共计从 Tornado Cash 提款 246,284 ETH（约 7.96 亿美元）。

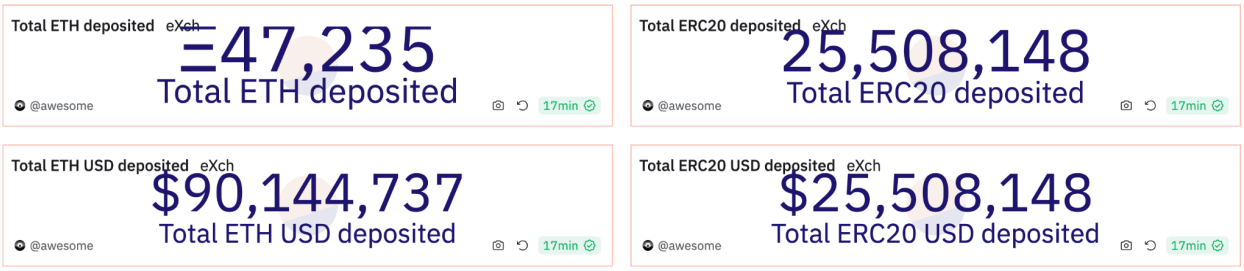
3.4.2 eXch

First half of 2024



(https://dune.com/misttrack/first-half-of-2024-stats)

All of 2023



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

虽然我们无法确定归因于作恶者的确切金额，但发送到 eXch 的资金明显大幅度增加。2024 上半年，ETH 存款从 2023 年的 47,235 笔增加到 71,457 笔，ERC20 存款从 25,508,148 笔增加到 55,115,833 笔。ERC20 的美元存款量也增加了一倍多，反映了交易量和交易价值的显著上升。这一趋势凸显了作恶者在加密货币领域日益增长的活动和潜在威胁。

四、总结

本报告总结了 2024 上半年区块链行业的关键监管合规政策及动态，包括但不限于对加密货币的多角度监管立场以及一系列核心的政策调整。为了呈现更全面的行业画像，我们对 2024 上半年的区块链安全事件和反洗钱趋势做了回顾和概述，对于部分常见的洗钱工具和钓鱼盗窃技巧等进行了解读，并为这类问题提出了有效的防范方法和应对策略。此外，我们还对主要的钓鱼犯罪组织 Wallet Drainers 和黑客团伙 Lazarus Group 进行了披露与分析，以期提供防范此类威胁的参考。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。

总的来说，我们希望这份报告能为读者提供一个关于区块链行业安全现状的剖析和解读，帮助读者更全面地了解区块链行业的安全和反洗钱现状，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

慢雾科技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

SlowMist AML

助力 Web3 行业合规、安全、健康的发展

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