SLOWMIST 2024

Blockchain Security and AML Annual Report

Table of Contents

I. Overview

The year 2024 has been one of navigating challenges. The global macroeconomic landscape remains complex and unpredictable, with geopolitical tensions showing no significant signs of easing. Factors such as adjustments in U.S. Federal Reserve monetary policy, the ongoing Russia-Ukraine conflict, instability in the Middle East, and the continuous tightening of global digital asset regulations have presented the blockchain industry with unprecedented challenges. Yet, the industry has demonstrated resilience and vitality, seeking new directions amidst uncertainties. The security landscape in 2024 continues to face a range of severe challenges, with centralized platforms remaining prime targets. Smart contract flaws and social engineering tactics are frequently exploited, while phishing attacks have grown increasingly covert and sophisticated. Together, these threats reveal the evolving ingenuity of malicious actors and the ongoing need for robust defenses. Supply chain security has also garnered increased attention in 2024. Several high-profile projects suffered malicious code injection attacks, leading to substantial user asset losses. Additionally, the complexity of interactions between on-chain and off-chain systems has enabled attackers to exploit vulnerabilities in the software supply chain, further amplifying potential risks.

Despite daunting security challenges, the blockchain industry in 2024 has made remarkable strides in innovation. Decentralized finance (DeFi) has continued to expand its application boundaries, by growing user numbers and transaction volumes. Tools for on-chain asset custody and management have become more diverse, while cross-chain protocol technologies are gradually improving, paving the way for collaborative development in an ever expanding ecosystem. We also saw the resurgence of NFT’s in 2024, and GameFi projects are emerging from a period of dormancy, attracting significant attention from both users and investors. Meanwhile, advancements in Ethereum and Layer 2 technologies have further enhanced blockchain network efficiency, helping provide additional support for innovative applications. Another noteworthy trend is the convergence of blockchain and artificial intelligence (AI). An increasing number of projects are exploring the integration of AI in on-chain analysis, fraud detection, and user experience optimization, unlocking new possibilities for the industry.

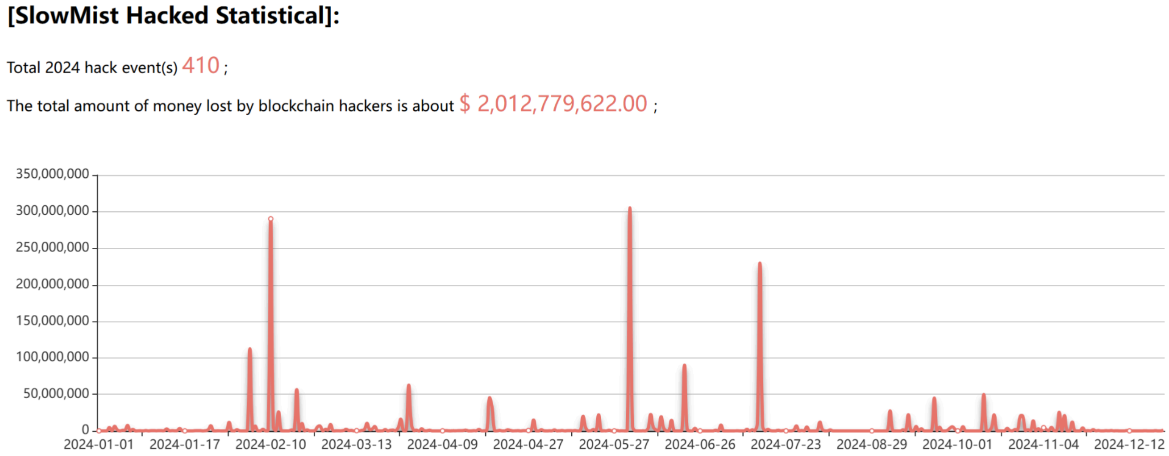
As the blockchain industry continues its rapid development, global regulatory frameworks are steadily taking shape. The U.S. has tightened compliance requirements for cryptocurrency exchanges, while mainland China continues to enforce stringent regulations on virtual asset financial activities, advancing pilot programs for the digital yuan. Hong Kong, on the other hand, has adopted a more favorable stance toward virtual assets, gradually establishing a regulatory framework conducive to industry growth, including the introduction of virtual asset service provider licenses and ETF products. In Europe, the MiCA regulation has officially come into effect, providing clear guidelines for compliant operations in the blockchain and crypto asset sectors. Central banks in various countries have accelerated the research and promotion of digital currencies, laying the foundation for a future digital financial ecosystem. It is foreseeable that compliance will be a defining theme for the industry's development in 2024, with the integration of security and compliance serving as a core driver for healthy growth.

Amid this dynamic landscape, the blockchain industry advances at the intersection of security and innovation. This report provides an in-depth review of key regulatory policies and anti-money laundering (AML) developments in 2024. It summarizes major blockchain security incidents, highlights typical fraud techniques, and features content contributed by the Web3 anti-scam platform ScamSniffer on phishing wallet drainers. Additionally, the report includes a statistical analysis of laundering methods and gains by North Korean hackers. We hope this report serves as a valuable resource for readers, helping industry participants and users gain a more comprehensive understanding of the current state of blockchain security and solutions. Our ultimate goal is to contribute to a safer blockchain ecosystem.

II. Blockchain Security

According to the SlowMist Hacked, a total of 410 security incidents were recorded in 2024, resulting in losses amounting to $2.013 billion. Compared to 2023, which saw 464 incidents and approximately $2.486 billion in losses, the total losses in 2024 represent a year-over-year decrease of 19.02%.

Note: It's important to note that these figures were recorded at the time of the incidents. With the significant increase in cryptocurrency prices since then, the actual value of the losses could be higher. Additionally, these *numbers reflect only publicly known incidents, meaning the real figures are likely much greater due to unreported cases.*



[SlowMist Hacked Statistical]:

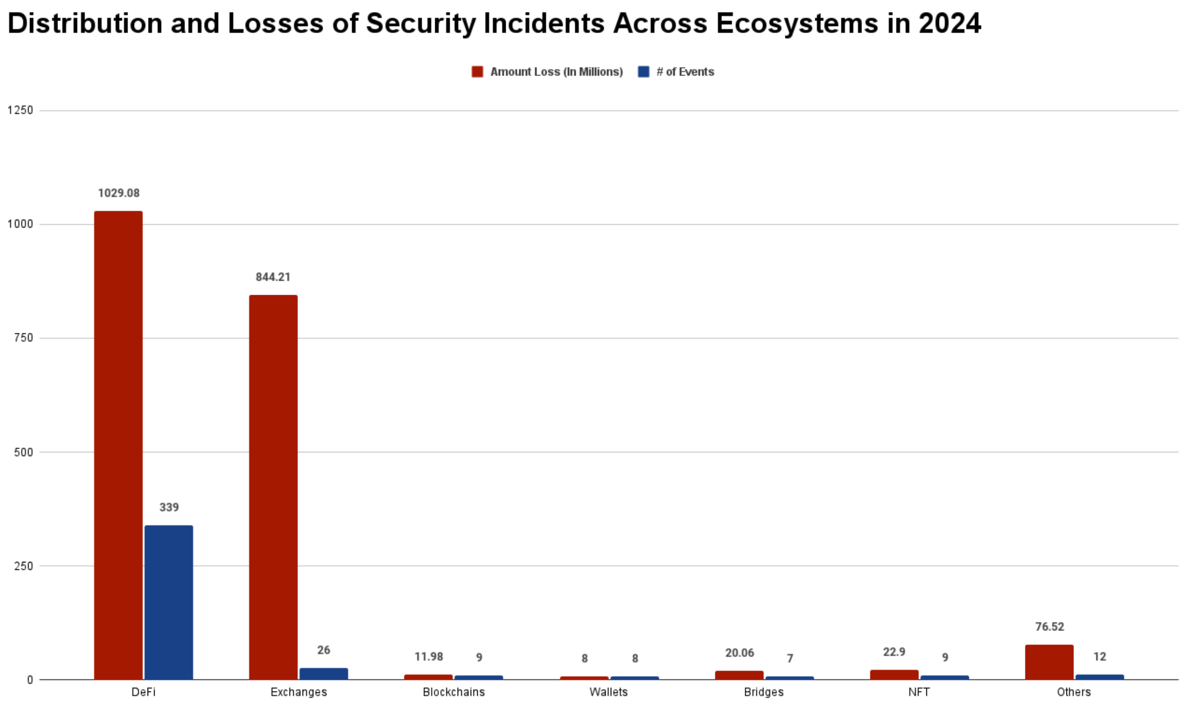
Total 2024 hack event(s) 410 ;

The total amount of money lost by blockchain hackers is about $ 2,012,779,622.00 ;

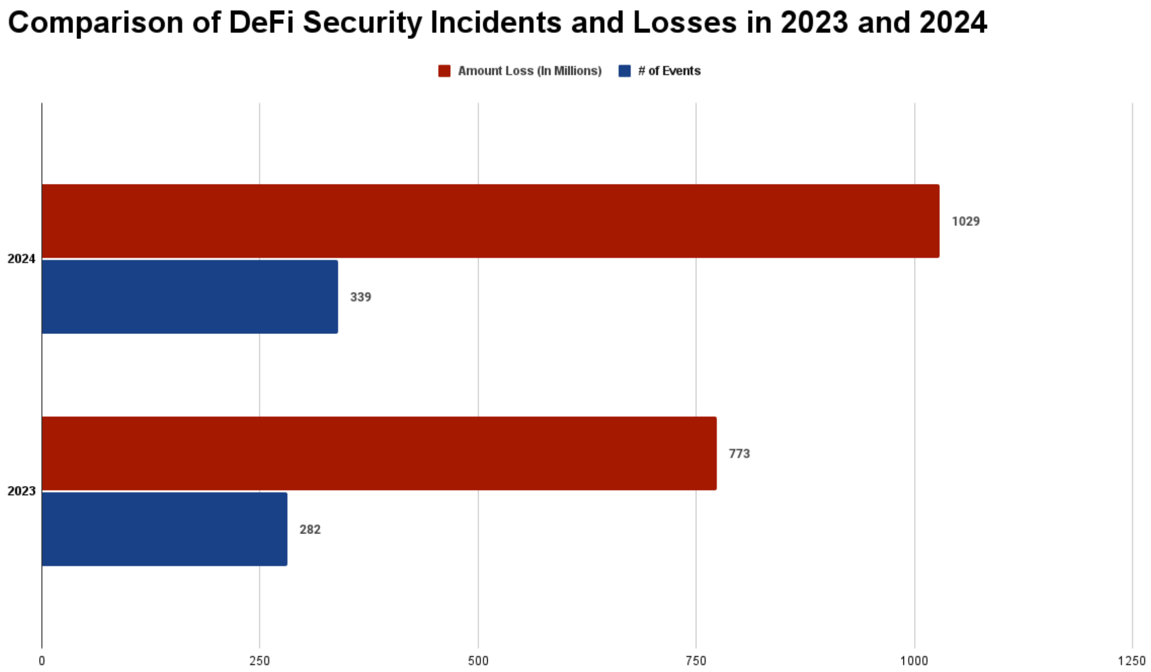
(https://hacked.slowmist.io/statistics/?c=all&d=2024)

2.1 Overview of Blockchain Security Incidents

In terms of type of security incidents, DeFi remains the most frequently targeted sector for attacks. In 2024, a total of 339 DeFi-related security incidents were reported, accounting for 82.68% of all security breaches, with losses reaching an astonishing $1.029 billion. Compared to 2023, which saw 282 incidents resulting in losses of approximately $773 million, this represents a year-over-year increase in losses of 33.12%.

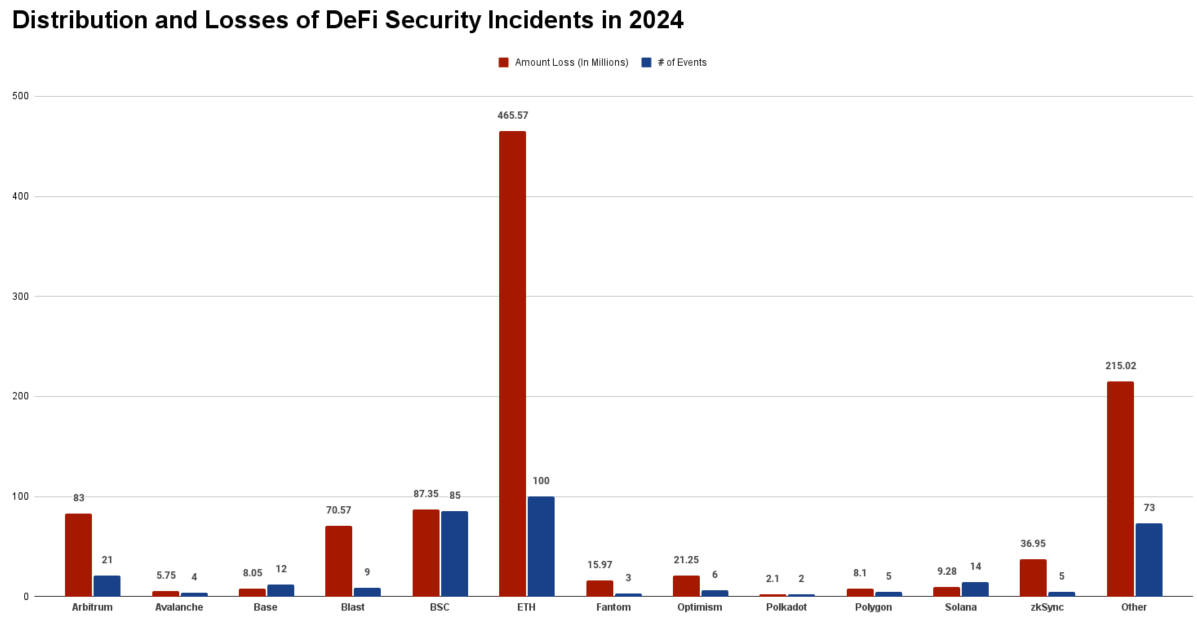


(Distribution and Losses of Security Incidents Across Ecosystems in 2024)



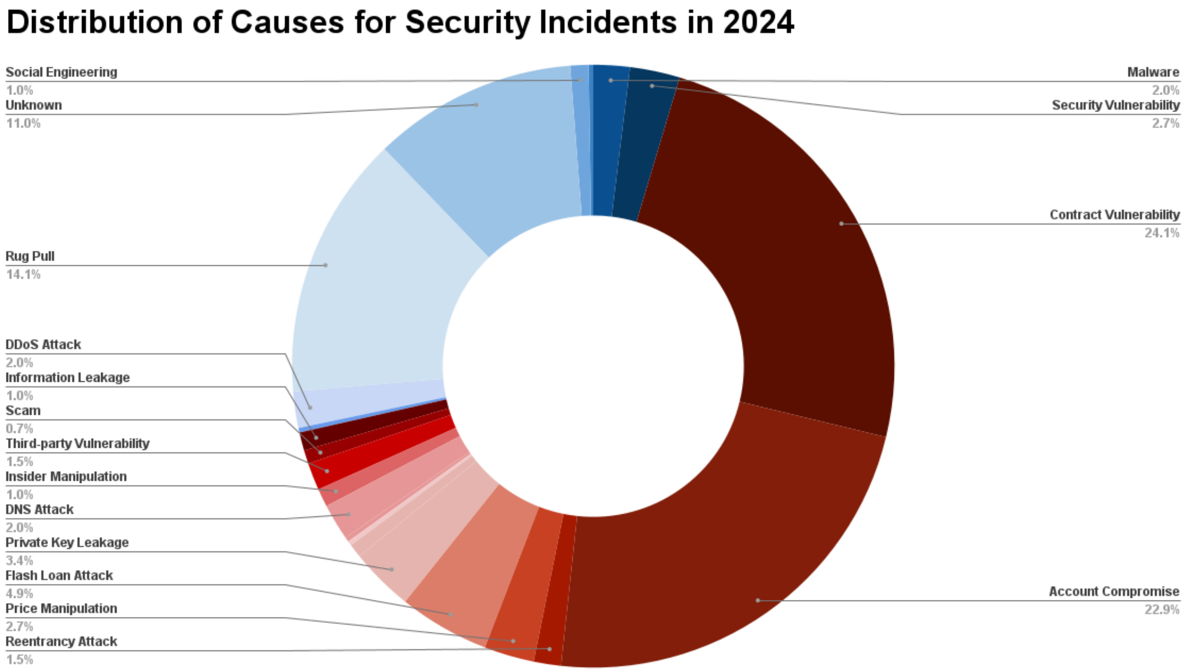
(Comparison of DeFi Security Incidents and Losses in 2023 and 2024)

From a blockchain perspective, Ethereum experienced the highest losses, totaling $465 million, followed by BSC (Binance Smart Chain) with losses amounting to $87.35 million.



(Distribution and Losses of DeFi Security Incidents in 2024)

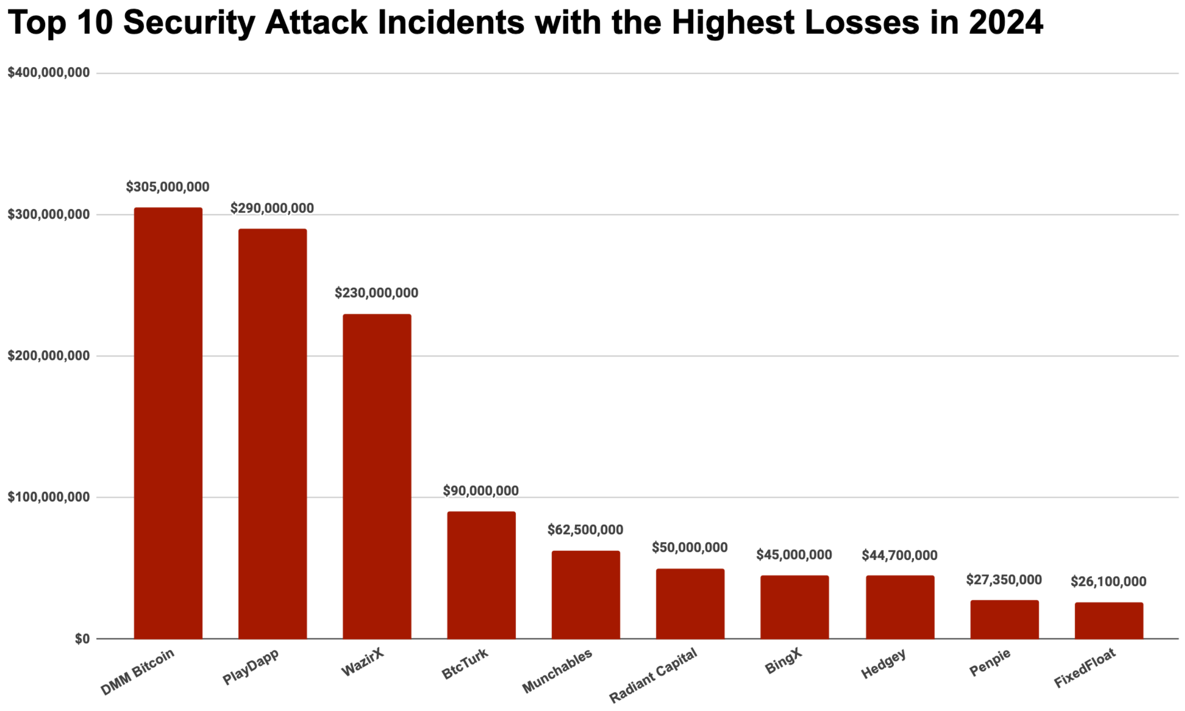
When looking at the causes of these incidents, smart contract vulnerabilities were the most common, with 99 reported incidents resulting in approximately $214 million in losses. The second most frequent cause was account compromises.



(Distribution of Causes for Security Incidents in 2024)

2.2 Top 10 Security Incidents of 2024

This section highlights the Top 10 security incidents in terms of losses for 2024.



(Top 10 Security Attack Incidents with the Highest Losses in 2024)

2.2.1 DMM Bitcoin

On May 31, 2024, Japanese cryptocurrency exchange DMM Bitcoin reported an unauthorized transfer of 4,502.9 BTC from its official wallet, resulting in a loss of approximately 48.2 billion yen (~$330 million). This attack ranks as the seventh-largest in cryptocurrency hacking history and the most significant since December 2022. It is also the third-largest crypto exchange hack in Japan, following the Mt. Gox incident in 2014 ($450 million) and the Coincheck hack in 2018 ($534 million).

On December 23, the FBI, the U.S. Department of Defense Cyber Crime Center (DC3), and the Japanese National Police Agency (NPA) linked the theft to the TraderTraitor campaign, also known as Jade Sleet, UNC4899, or Slow Pisces. TraderTraitor typically employs social engineering attacks targeting multiple employees of the same company.

In March 2024, a North Korean hacker posed as a LinkedIn recruiter and sent a malicious Python script to an employee at Ginco, a Japanese enterprise cryptocurrency wallet software company.

The employee unknowingly uploaded the code to their GitHub page, leading to a breach. By mid-May, the hackers accessed Ginco's unencrypted communication system, enabling them to manipulate legitimate transaction requests from DMM Bitcoin staff, resulting in the theft of 4,502.9 BTC, later traced to wallets controlled by TraderTraitor.

2.2.2 PlayDapp

On February 9, 2024, the blockchain gaming platform PlayDapp suffered an attack where hackers compromised the private key of its PLA token smart contract. The attackers gained ownership and minting rights, creating 200 million PLA tokens and transferring them to their accounts. Despite PlayDapp's efforts to negotiate with the attackers, including offering a $1 million white-hat reward, talks failed.

On February 12, the hackers minted an additional 1.59 billion PLA tokens, but exchange freezes prevented these tokens from entering circulation. Post-incident analysis revealed the attack originated from a phishing email sent to the team on January 16. The email contained a malicious payload disguised as a routine request from a major partner exchange, which installed a tampered remote-access tool, leading to the theft of the admin private key.

2.2.3 WazirX

On July 18, 2024, Indian cryptocurrency exchange WazirX detected suspicious transactions involving its multisig wallet. An investigation revealed that hackers had exploited discrepancies between the interface and actual transactions on Liminal, a service used for transaction verification. This enabled attackers to transfer wallet control to themselves, resulting in losses exceeding $230 million.

2.2.4 BtcTurk

On June 22, 2024, Turkish cryptocurrency exchange BtcTurk suffered an attack, resulting in losses of approximately $90 million. In a statement released on June 22, BtcTurk stated: "The cyberattack affected a portion of the balances of 10 cryptocurrencies in our hot wallet, while the majority of assets stored in cold wallets remain secure." According to Binance CEO Richard Teng, Binance has frozen $5.3 million worth of the stolen assets.

2.2.5 Munchables

On March 27, 2024, Blast ecosystem project Munchables was hacked, leading to losses of $62.5 million. Subsequently, the Blast team recovered $97 million through a multisig wallet after the attackers, former developers of Munchables, returned the funds voluntarily without ransom.

2.2.6 Radiant Capital

On October 17, 2024, Radiant Capital suspended operations on BNB Chain and Arbitrum due to a malicious contract upgrade by attackers who had compromised three multisig wallets. Losses amounted to approximately $50 million. Security firm Mandiant later attributed the attack to UNC4736, a group linked to North Korea.

2.2.7 BingX

On September 20, 2024, Singapore-based cryptocurrency exchange BingX detected unauthorized access to a hot wallet, resulting in losses of $45 million. Analysis by MistTrack suggested links between this incident and the Indodax hack, both involving laundering through addresses associated with Lazarus Group, a North Korean hacking organization.

2.2.8 Hedgey Finance

On April 19, 2024, Hedgey Finance suffered an attack due to inadequate input validation, leading to unauthorized approvals and losses of approximately $44.7 million on Ethereum and Arbitrum.

2.2.9 Penpie

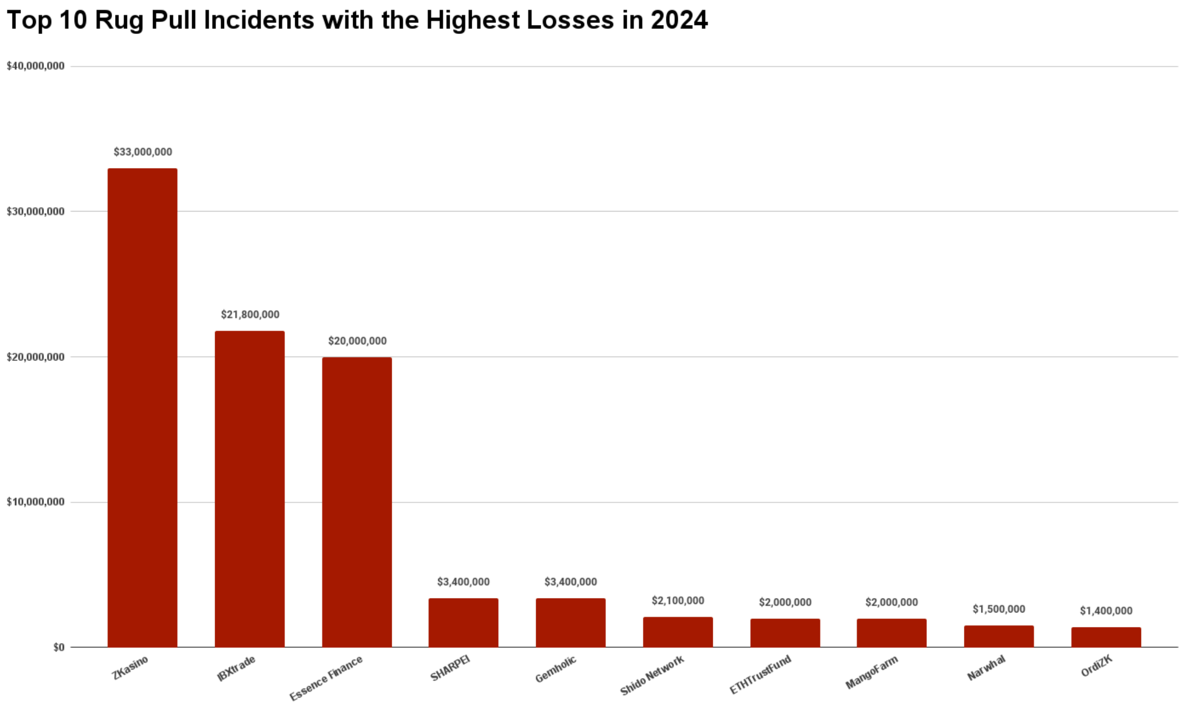
On September 4, 2024, liquidity rewards project Penpie lost approximately $27.35 million in an attack that exploited its incorrect assumptions about Pendle Finance's market creation process. Attackers used malicious smart contracts and flash loans to amplify rewards artificially.

2.2.10 FixedFloat

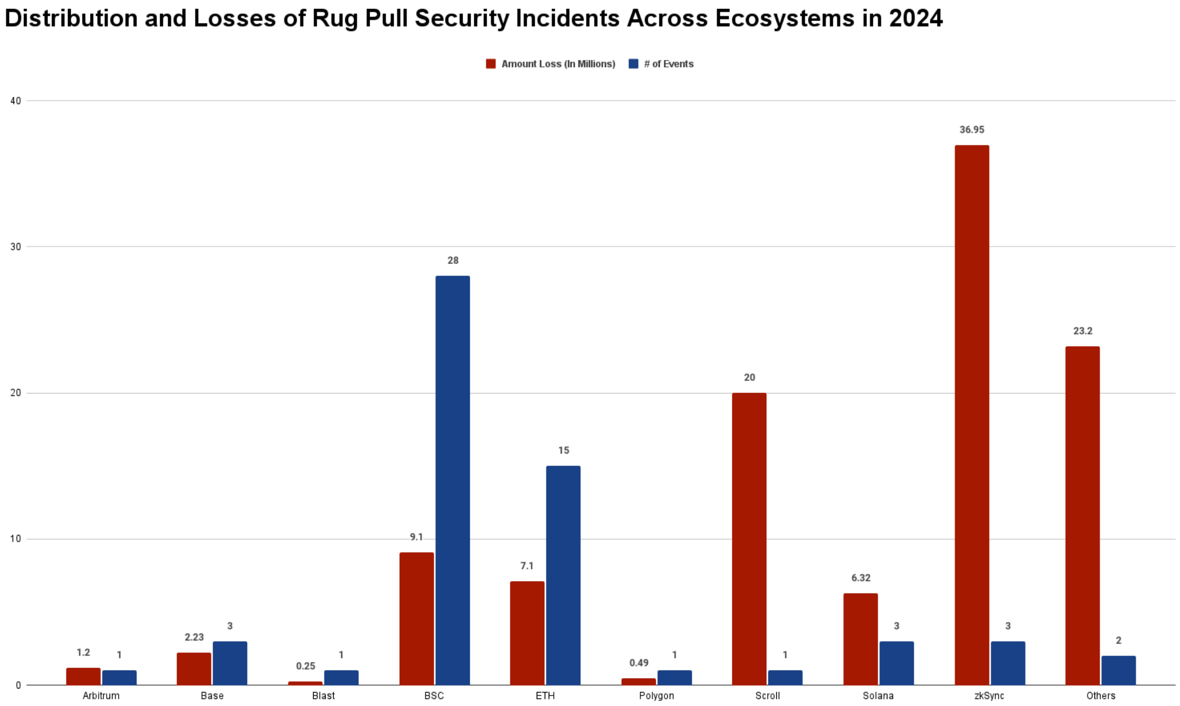
On February 16, 2024, crypto platform FixedFloat lost 409 BTC (~$21.17 million) and 1,728 ETH (~$4.85 million) due to an external vulnerability. A follow-up attack on April 2 increased total losses to approximately $29 million.

2.3 Rug Pull

A Rug Pull is a type of scam in which malicious project teams create hype to attract user investments, only to "pull the rug" by absconding with the funds once the time is right. According to the SlowMist Hacked Database, 58 Rug Pull incidents were recorded in 2024, resulting in losses of approximately $106 million. The zkSync ecosystem experienced the highest losses, totaling $36.95 million, while the BSC (Binance Smart Chain) ecosystem saw the most incidents, with 28 Rug Pulls reported.



(Top 10 Rug Pull Incidents with the Highest Losses in 2024)


Distribution and Losses of Rug Pull Security Incidents Across Ecosystems in 2024

(Distribution and Losses of Rug Pull Security Incidents Across Ecosystems in 2024)

Some projects go to great lengths to create hype, spending heavily to enlist celebrities or industry influencers (KOLs) to endorse and promote their projects. Their goal is to attract attention, quickly amass a user base, and boost project visibility. On the other hand, some projects engage in outright deceptive behavior right from the start of their promotional campaigns. These teams fabricate endorsements, partnerships, or achievements to create a false sense of legitimacy while keeping their operational costs for fraud as low as possible.

For example, on October 23, 2024, the project SHARPEI (SHAR) was launched, using cartoon art of Shar Pei dogs for promotion. With the support of KOLs, its market value skyrocketed to $54 million. However, SHARPEI soon cashed out $3.4 million, causing the token price to plummet by over 96% within seconds. Leaked promotional documents revealed multiple false claims, including fabricated statements about KOL endorsements and partnerships with various platforms and projects.

The rise of meme coins has further fueled speculative and FOMO-driven behavior among users, often leading them to overlook potential risks. Some token issuers don't bother presenting a vision or publishing a whitepaper, relying solely on a concept or slogan to generate hype and attract buyers. The low cost of executing scams has led to a surge in Rug Pull incidents. Once users' funds are stolen, recovering them is typically a long and arduous process. To mitigate these risks, the SlowMist Security Team advises users to thoroughly research a project's background and team before participating and to exercise caution before investing. Being well-informed can help users avoid falling victim to such scams.

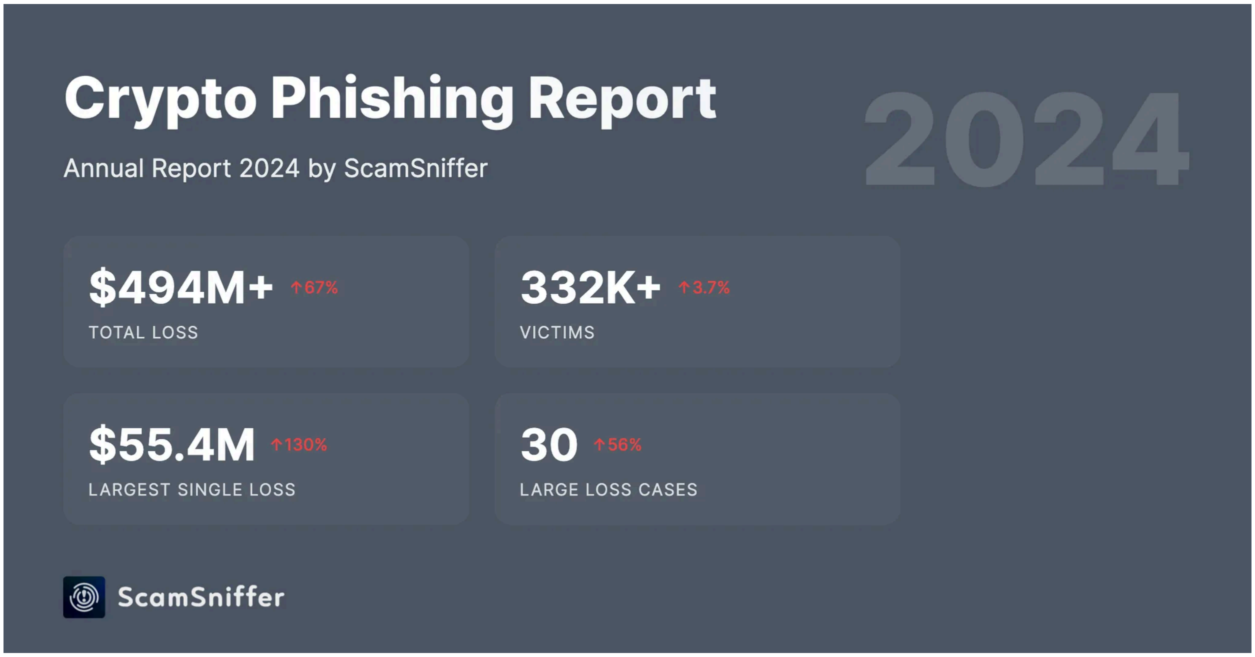
2.4 Phishing Attack

This section focuses on analyzing Wallet Drainer attacks on EVM-compatible chains. Special thanks to ScamSniffer for their valuable contribution to this analysis.

2.4.1 Overview

A Wallet Drainer is a type of attack deployed on phishing websites that steals crypto assets by inducing users to sign malicious transactions. In 2024, such attacks caused approximately $494 million in losses, a 67% increase year-over-year. While the number of victims only increased by 3.7% (reaching 332,000 addresses), the loss per attack increased significantly, with the largest single theft amounting to $55.48M USD.

2.4.2 Key Data Comparison



Crypto Phishing Report

2024

Annual Report 2024 by ScamSniffer

$494M+ ↑67%
TOTAL LOSS

332K+ ↑3.7%
VICTIMS

$55.4M ↑130%
LARGEST SINGLE LOSS

30 ↑56%
LARGE LOSS CASES

ScamSniffer

(Key Data Indicators of Wallet Drainer Attacks in 2024)

(1) 2024 Key Indicators

- Total Loss: $494M USD, up 67%
- Number of Victims: 332,000 addresses, up 3.7%
- Largest Single Theft: $55.48M USD
- Number of Large-scale Thefts: 30

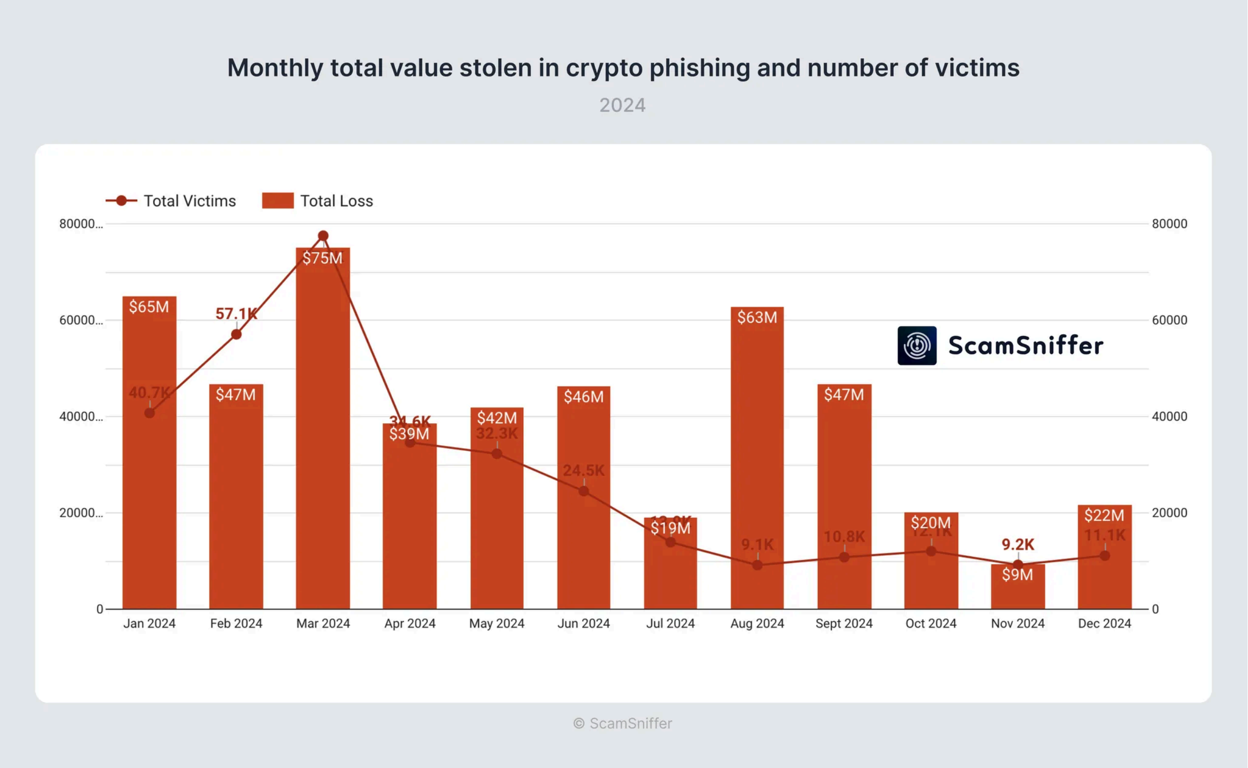
(2) Major Events of the Year

- Q1: Bitcoin price reached all-time high, increased on-chain activity led to rise in phishing
- Q2: Pink Drainer announced exit
- Q3: Market adjustment, phishing activities cooled down, but occasional large-scale incidents occurred
- Q4: Inferno Drainer claimed exit, taken over by Angel

Next, we will analyze in detail the loss data behind these events to reveal trends and potential risks.

2.4.3 Loss Analysis

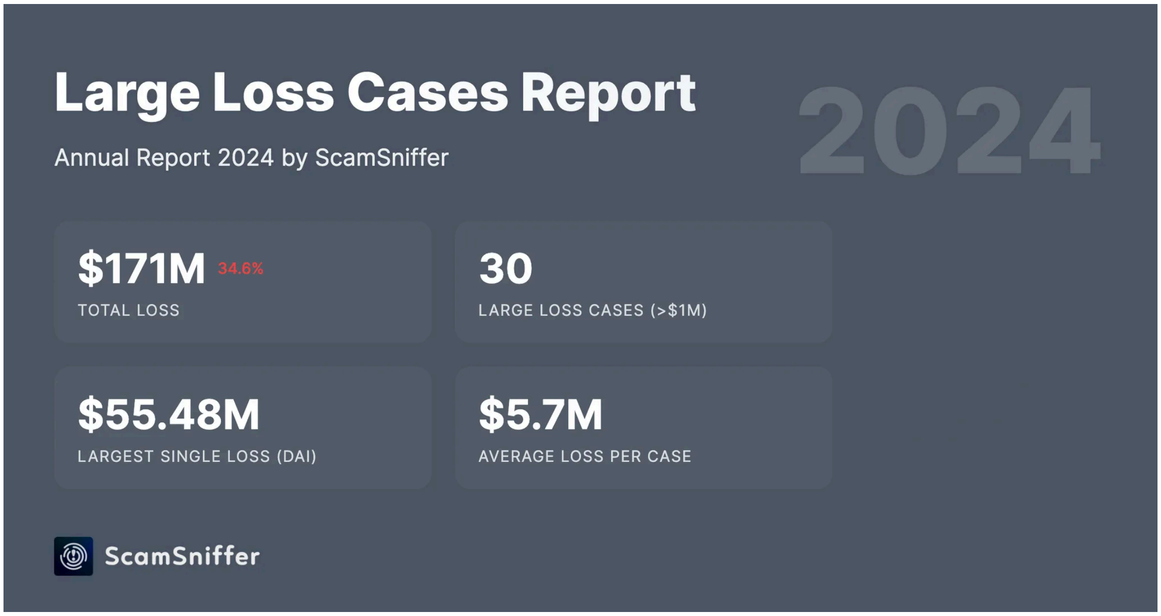
(1) Monthy Overall Loss Trends



The year's attack activities can be divided into three phases:

- The first quarter saw the heaviest losses, reaching $187.2 million with 175,000 victims. March recorded the highest losses at $75.2 million.
- Second and third quarters combined losses totaled $257 million, with victims decreasing to 90,000.
- Fourth quarter losses dropped to $51 million with victims reducing to 30,000, indicating improved security.

(2) Major Case Analysis



Large Loss Cases Report

Annual Report 2024 by ScamSniffer

2024

$171M 34.6%

TOTAL LOSS

30

LARGE LOSS CASES (>$1M)

$55.48M

LARGEST SINGLE LOSS (DAI)

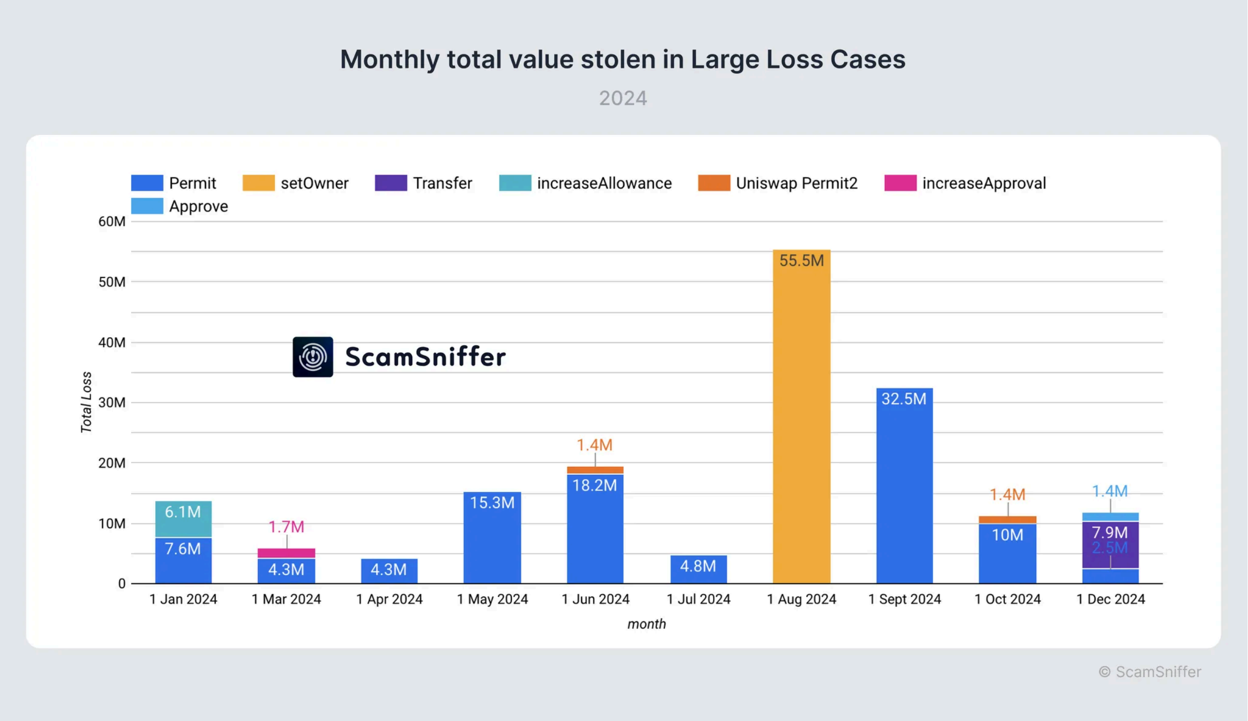
$5.7M

AVERAGE LOSS PER CASE

ScamSniffer

30 cases exceeding $1 million occurred throughout the year, with total losses of $171 million.

- Major Theft Monthly Trend Analysis:

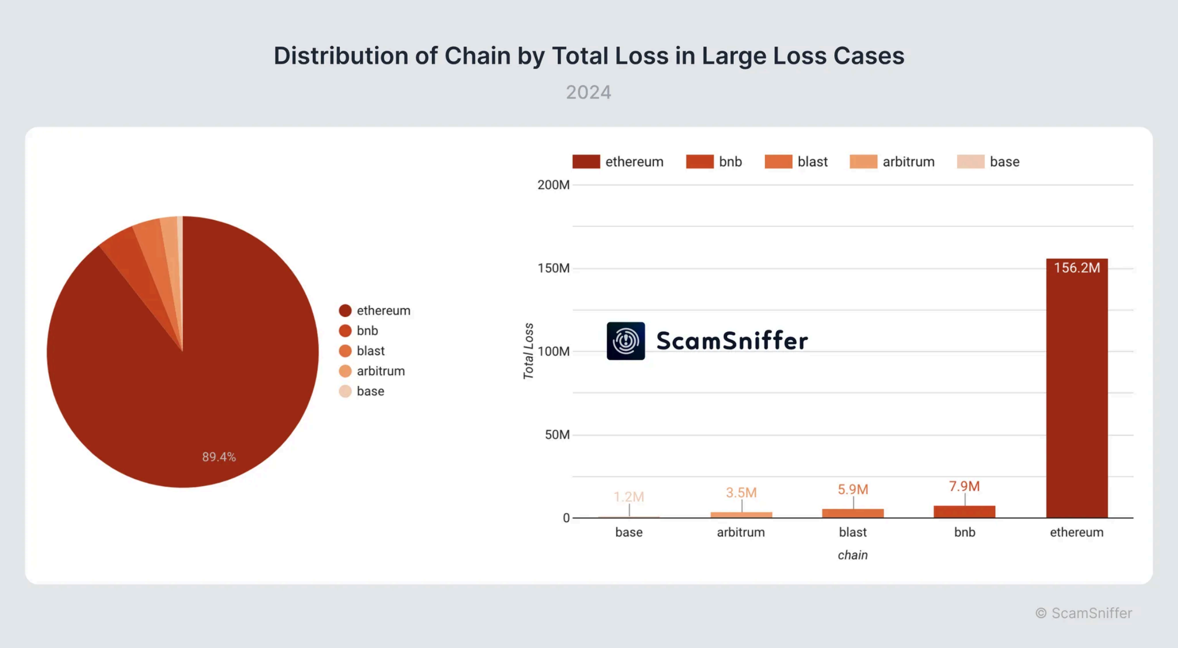


Large-scale theft incidents in 2024 showed distinct phases. The first half (January-June) saw frequent but smaller-scale incidents, with individual losses ranging from $1-8M.

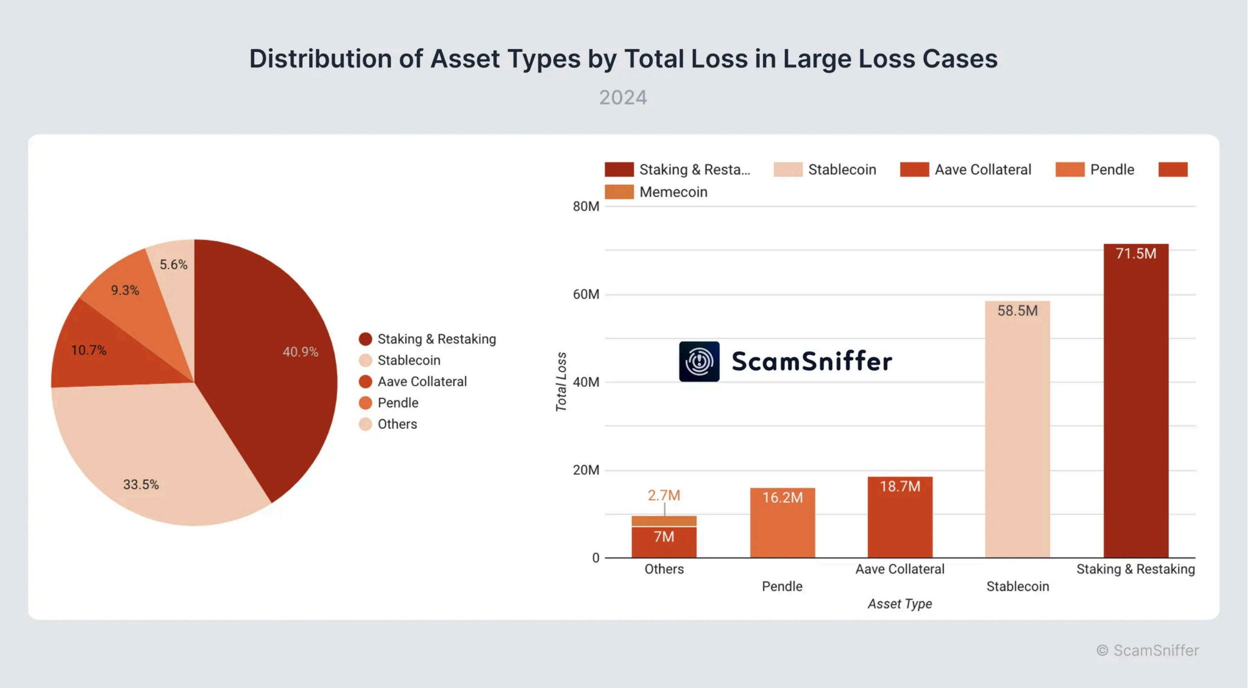
The peak period occurred during July-September, with major losses of $55.48M and $32.51M in August and September respectively, accounting for 52% of the year's total large-scale losses.

The final quarter showed a significant reduction in both frequency and scale, with individual losses mostly ranging from $2-6M, indicating an overall improvement in market security awareness.

- Loss Distribution Characteristics:



- Chain Distribution:
  - Ethereum (25 cases, 85.3%), losses of $156 million
  - Arbitrum (2 cases, $3.55M)
  - Blast (1 case, $5.9M)
  - Base (1 case, $1.2M)
  - BNB Chain (1 case, $7.9M)



Distribution of Asset Types by Total Loss in Large Loss Cases

2024

© ScamSniffer

- Asset Types:

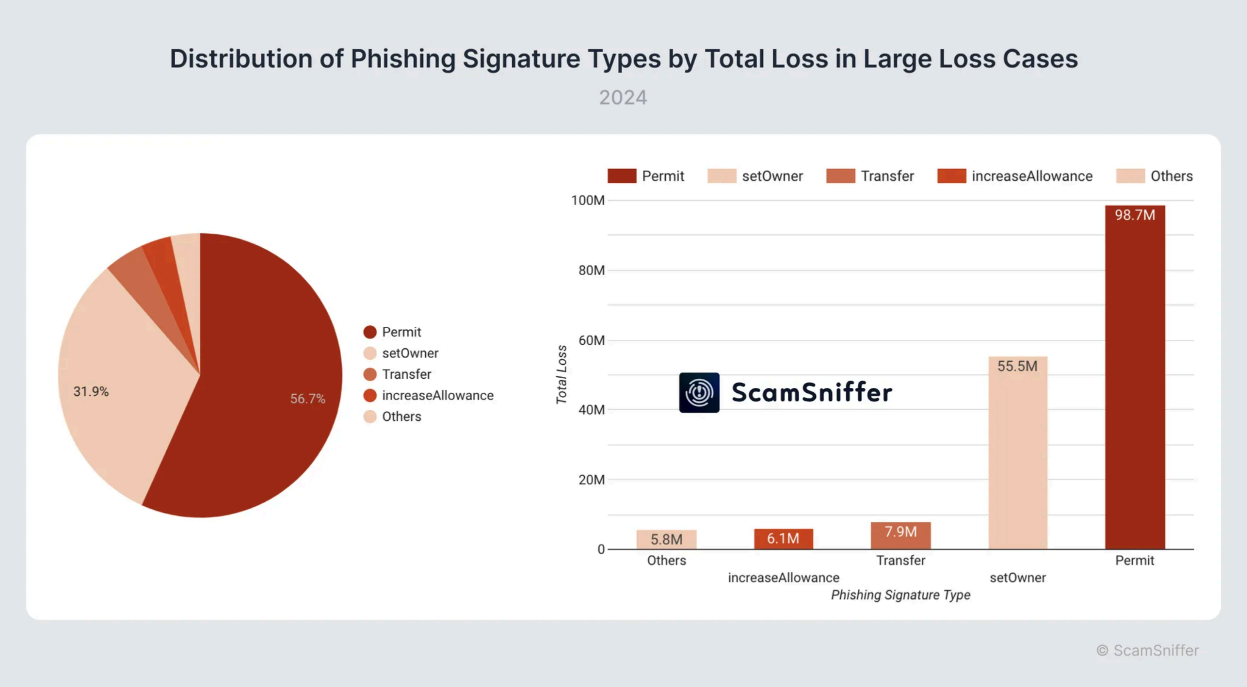
  - Staking & Restaking (40.9%)

  - Stablecoin (33.5%)

  - Aave Collateral (10.7%)

  - Pendle Yield (9.3%)

  - Others (5.6%)



Distribution of Phishing Signature Types by Total Loss in Large Loss Cases

2024

© ScamSniffer

- Phishing Signature Types:

  - Permit (56.7%)

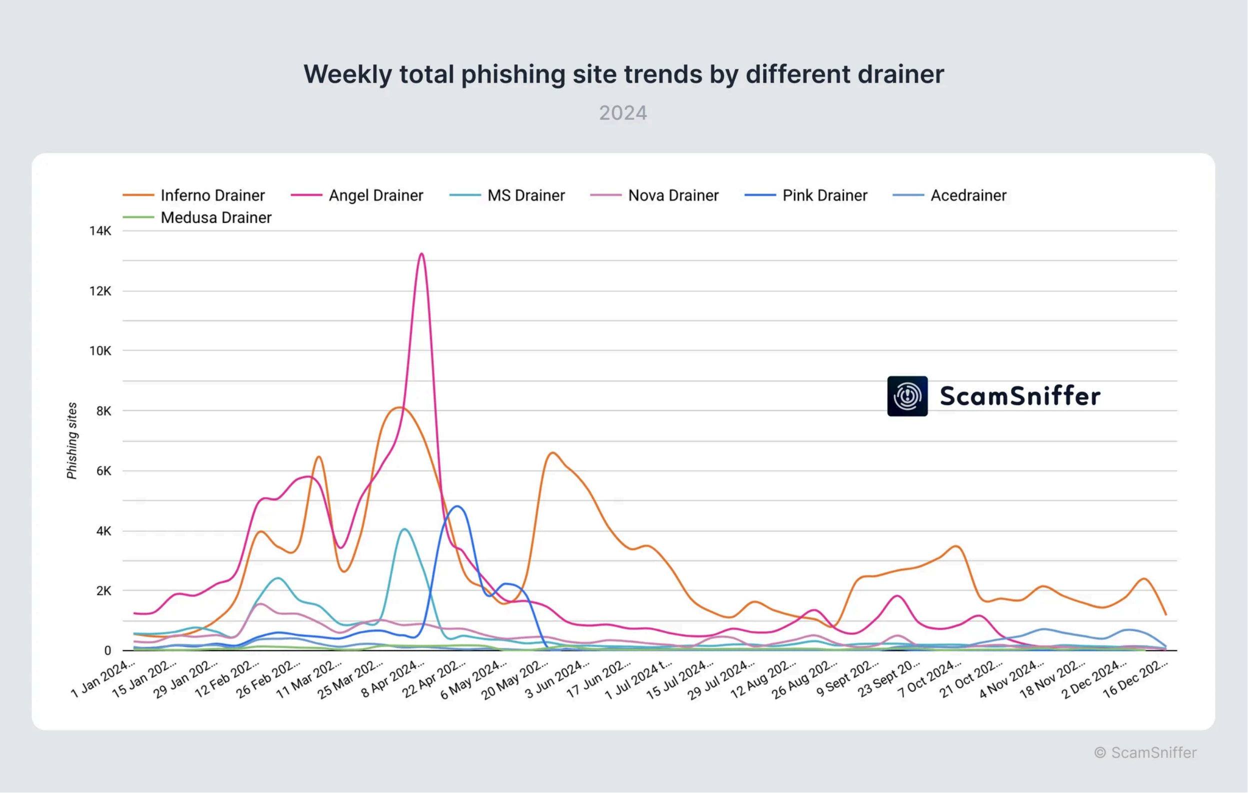
  - setOwner (31.9%)

  - Transfer (4.5%)

  - increaseAllowance (3.5%)

  - Others (3.4%)

2.4.4 Wallet Drainer Evolution


Weekly total phishing site trends by different drainer

2024

© ScamSniffer

(1) The attack landscape evolved significantly throughout the year, marked by several key transitions:

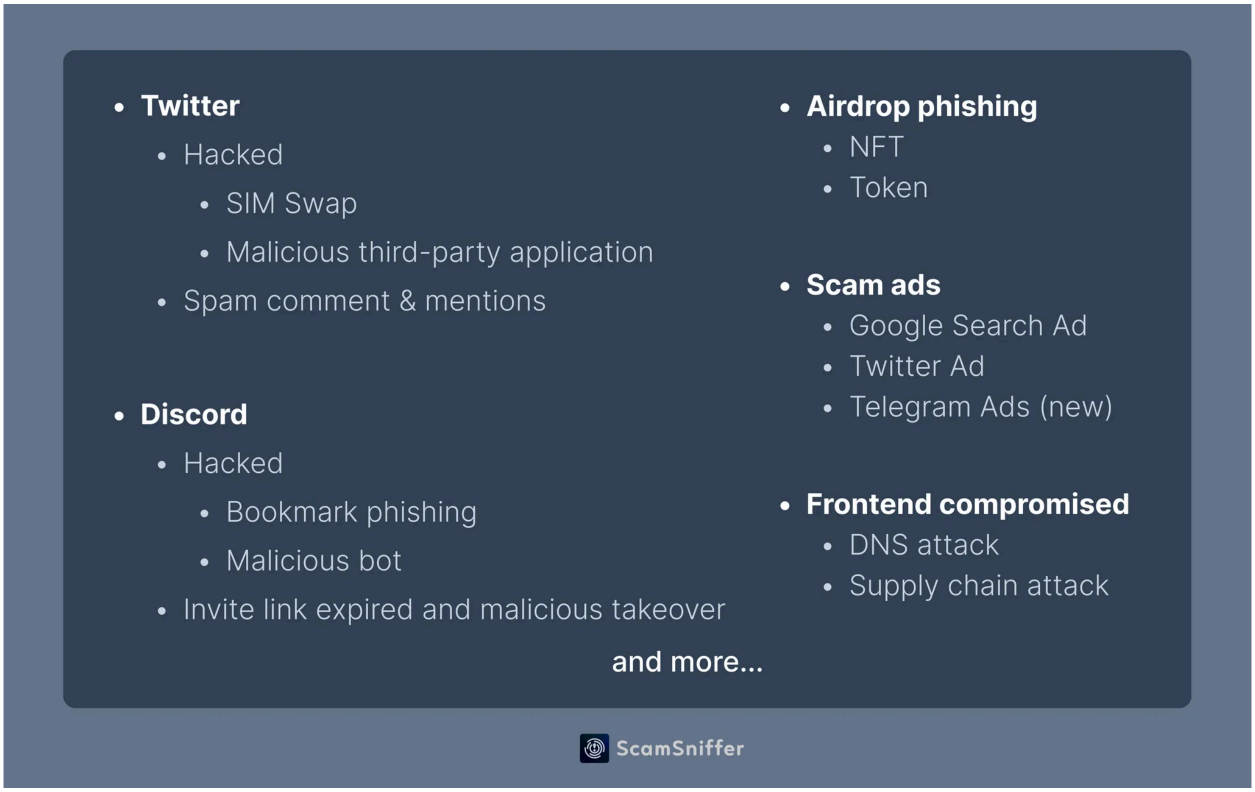
- Pink's Exit (End of May): Held 28% market share, which was subsequently absorbed by Inferno
- Angel's Takeover of Inferno (End of October): Angel's share decreased while Inferno maintained 40-45% market share

(2) Major Events of the Year

- Q1-Q2: Three major players dominated (Angel: 42%, Pink: 28%, Inferno: 22%)
- Q3: Dual competition (Inferno: 43%, Angel: 25%)
- Q4: New landscape (Inferno and Angel: 45%, Acedrainer: 20%, Other new Drainers: 25%)

2.4.5 Distribution Channel Analysis

(1) Main Traffic Sources for Phishing Websites



- **Twitter**
  - Hacked
    - SIM Swap
    - Malicious third-party application
  - Spam comment & mentions
- **Discord**
  - Hacked
    - Bookmark phishing
    - Malicious bot
  - Invite link expired and malicious takeover
- **Airdrop phishing**
  - NFT
  - Token
- **Scam ads**
  - Google Search Ad
  - Twitter Ad
  - Telegram Ads (new)
- **Frontend compromised**
  - DNS attack
  - Supply chain attack

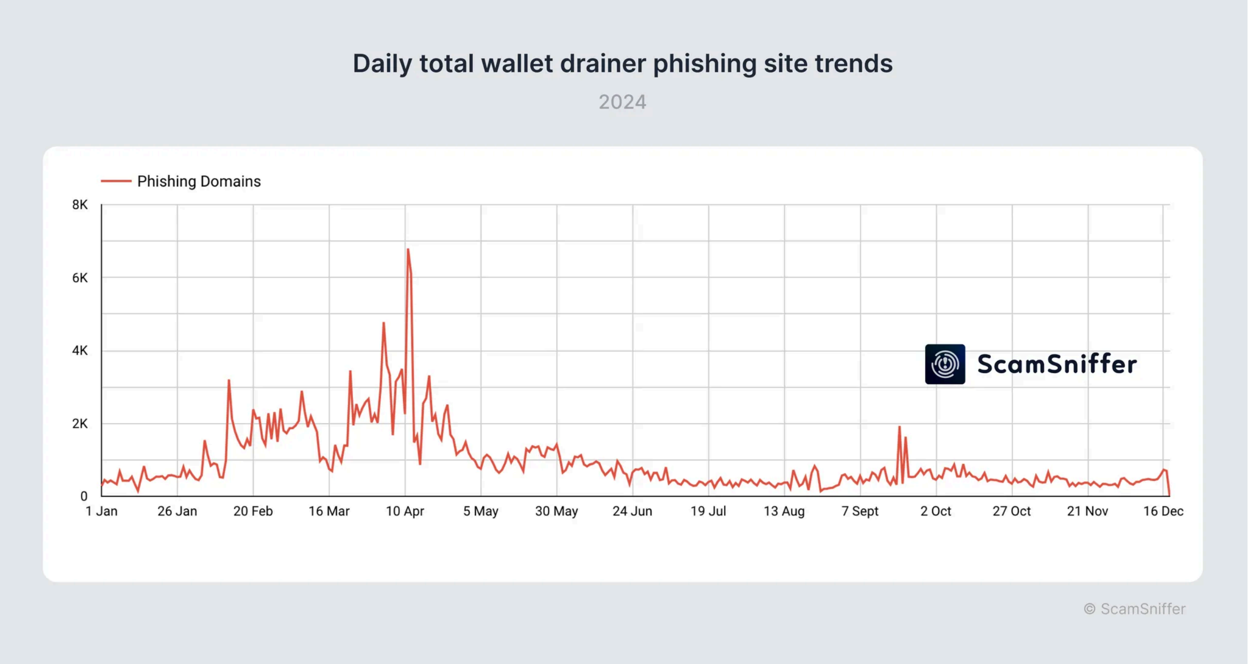
and more...

ScamSniffer

Phishing websites primarily acquire traffic through these channels:

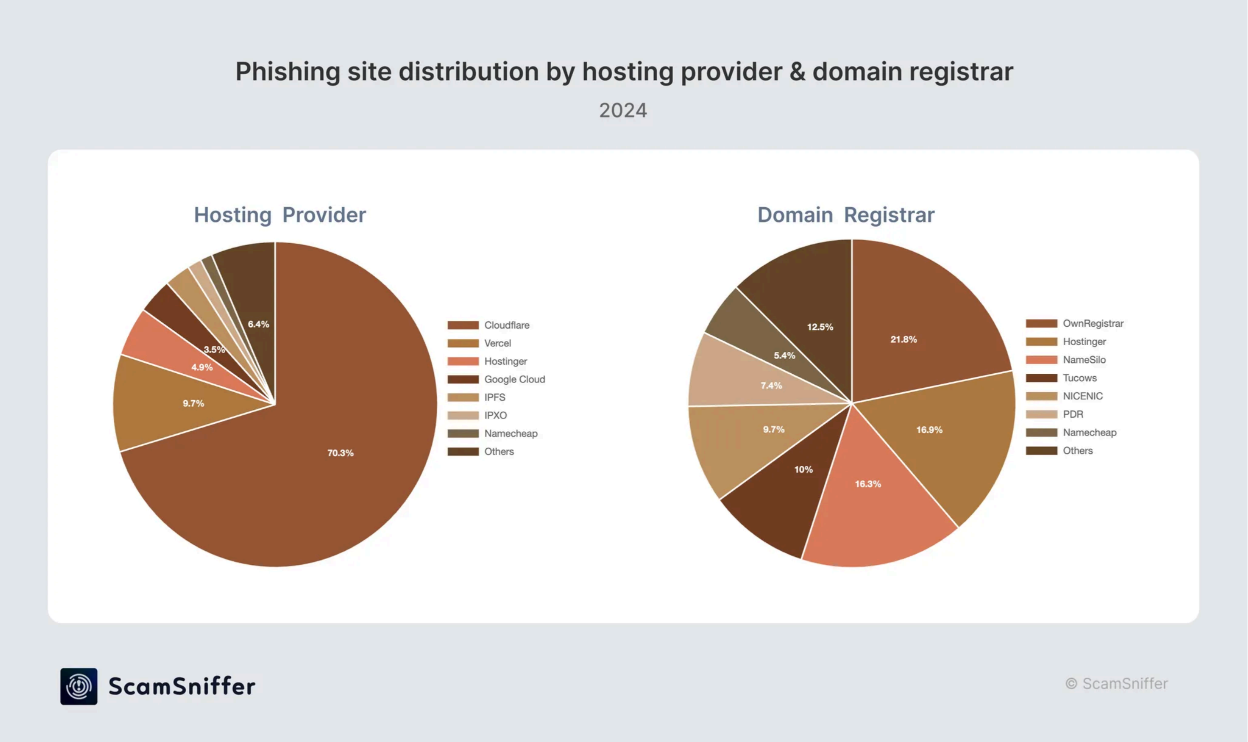
- Hacking: Official project Discord and Twitter accounts compromised, frontend or supply chain attacks
- Organic Traffic: NFT or token airdrops, expired Discord links being taken over
- Paid Traffic: Google Search/Twitter/Telegram advertisements
- Others: Email/Social Media/IM private messages/other sources

(2) Phishing Website Activity Analysis



Q1 showed the highest phishing website activity for the year, explaining the high theft losses during this period. Due to market adjustments and the exit of major Drainers like Pink and Inferno, overall activity levels in the second half of the year were lower than in the first half.

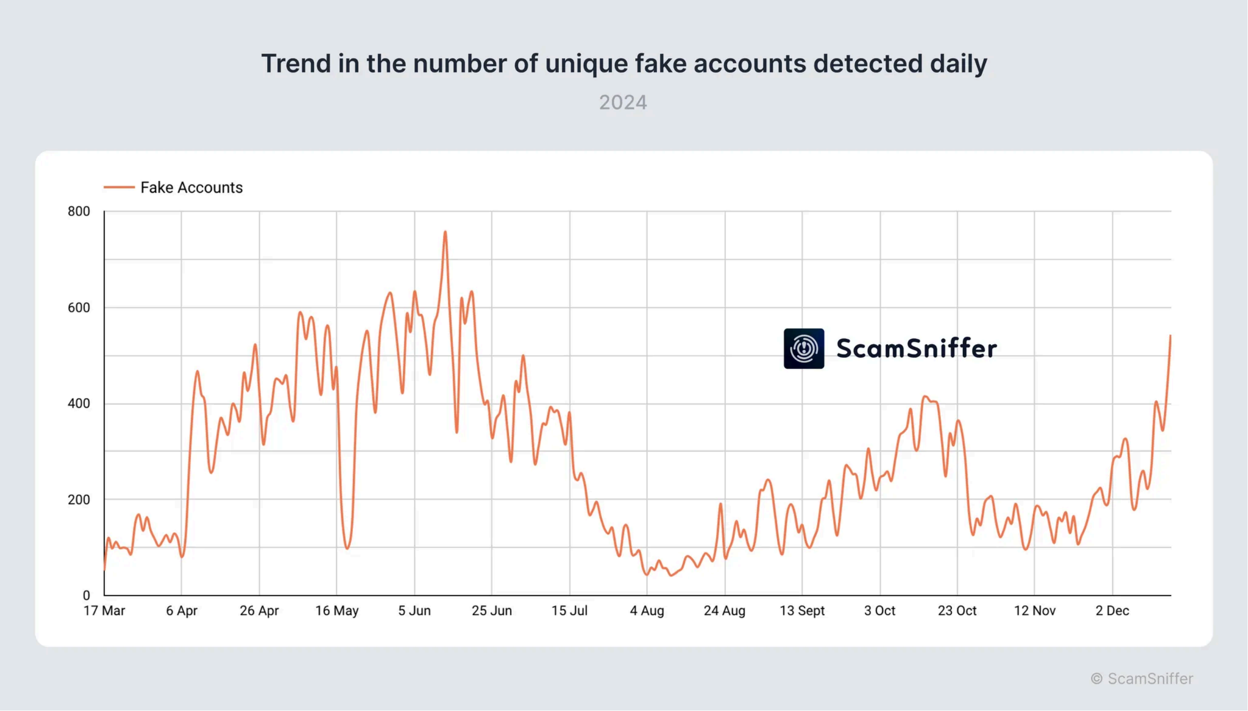
(3) Hosting Services & Domain Registrar Distribution


Phishing site distribution by hosting provider & domain registrar

2024

Most phishing websites are deployed using services like Cloudflare, Vercel, and IPFS. The primary domain registrars used include OwnRegistrar, Hostinger, NameSilo, and Tucows.

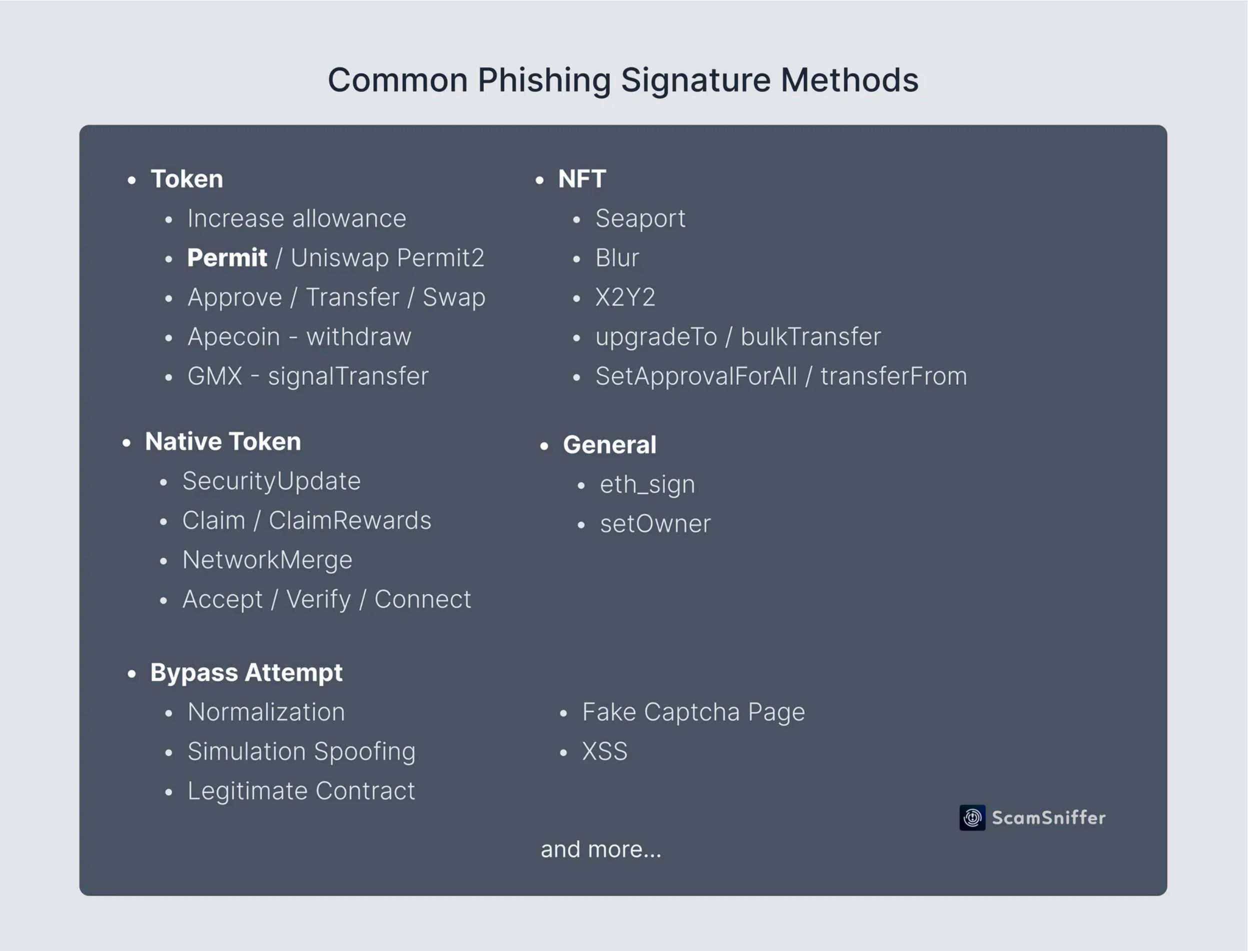
(4) X Platform Fake Account Trends


Trend in the number of unique fake accounts detected daily

2024

The activity of phishing websites closely mirrors overall trends in fake account activity. In the first half of the year, phishing activity was generally high. However, in July, there was a noticeable decline due to increased enforcement by the X platform against fake accounts, coupled with a market-wide correction in the cryptocurrency sector. Despite this decline, phishing activity gradually increased again starting in September and October as market conditions rebounded.

2.4.6 Phishing Signature Methods



Common Phishing Signature Methods

- **Token**
  - Increase allowance
  - **Permit** / Uniswap Permit2
  - Approve / Transfer / Swap
  - Apecoin - withdraw
  - GMX - signalTransfer
- **NFT**
  - Seaport
  - Blur
  - X2Y2
  - upgradeTo / bulkTransfer
  - SetApprovalForAll / transferFrom
- **Native Token**
  - SecurityUpdate
  - Claim / ClaimRewards
  - NetworkMerge
  - Accept / Verify / Connect
- **General**
  - eth_sign
  - setOwner
- **Bypass Attempt**
  - Normalization
  - Simulation Spoofing
  - Legitimate Contract
  - Fake Captcha Page
  - XSS

and more...

ScamSniffer

Permit remains the primary method for token phishing attacks.

Notably, the setOwner phishing signature targeting Proxy ownership modification led to a significant incident in August, resulting in a single victim losing $55 million in DAI.

(1) Detection Bypass

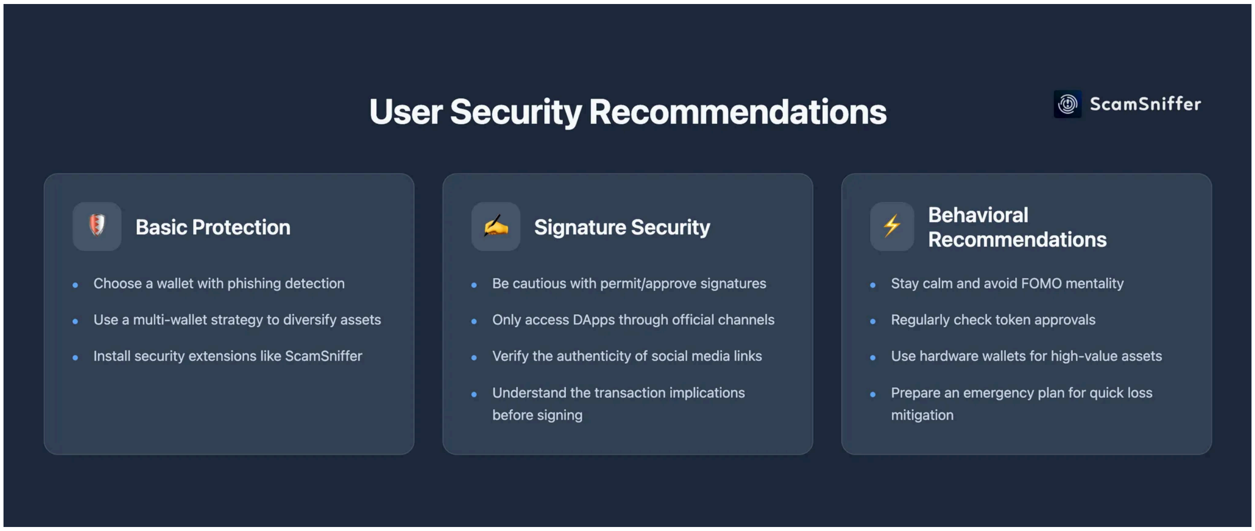
As wallets increase investment in phishing security, Wallet Drainers continue to develop new bypass methods, including:

- Exploiting wallet normalization processes to initiate signatures that wallets can process but security detection layers might miss
- Using legitimate contracts and adding Cloudflare or fake CAPTCHA pages to prevent detection
- Attempting to bypass wallet blacklists through XSS vulnerabilities
- Deceiving wallet simulation results

This remains an ongoing cat-and-mouse game between attackers and defenders.

2.4.7 Security Recommendations

(1) User Security Guidelines



User Security Recommendations

ScamSniffer

Basic Protection

- Choose a wallet with phishing detection
- Use a multi-wallet strategy to diversify assets
- Install security extensions like ScamSniffer

Signature Security

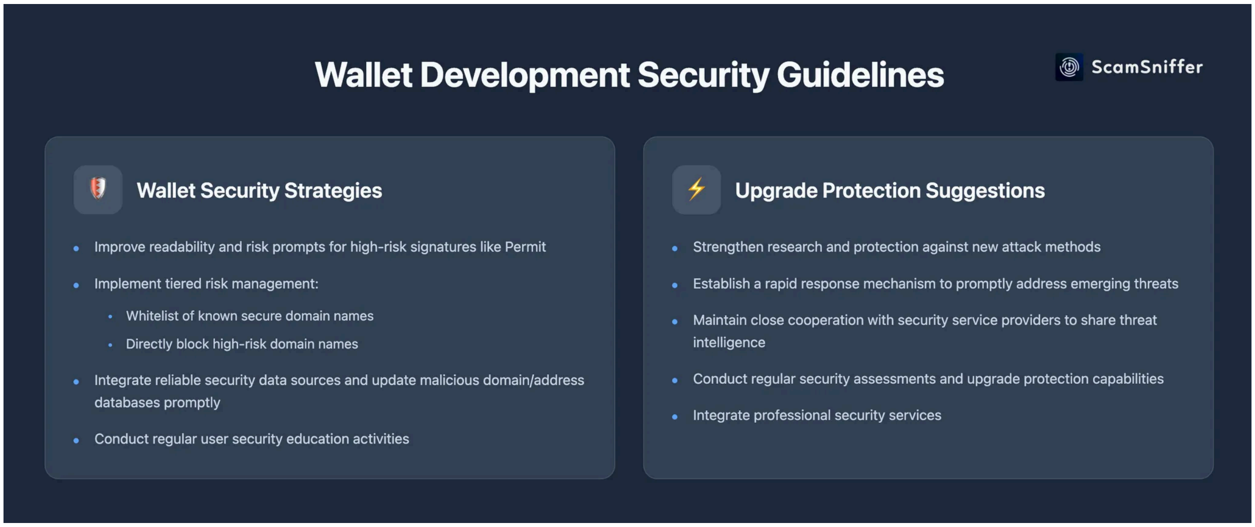
- Be cautious with permit/approve signatures
- Only access DApps through official channels
- Verify the authenticity of social media links
- Understand the transaction implications before signing

Behavioral Recommendations

- Stay calm and avoid FOMO mentality
- Regularly check token approvals
- Use hardware wallets for high-value assets
- Prepare an emergency plan for quick loss mitigation

Web3 security requires both tool protection and proper security awareness and habits. While enjoying Web3 innovation benefits, always prioritize security and remain vigilant. In the decentralized world, everyone is ultimately responsible for protecting their own assets.

(2) Wallet Development Security Guidelines



Wallet Development Security Guidelines

ScamSniffer

Wallet Security Strategies

- Improve readability and risk prompts for high-risk signatures like Permit
- Implement tiered risk management:
  - Whitelist of known secure domain names
  - Directly block high-risk domain names
- Integrate reliable security data sources and update malicious domain/address databases promptly
- Conduct regular user security education activities

Upgrade Protection Suggestions

- Strengthen research and protection against new attack methods
- Establish a rapid response mechanism to promptly address emerging threats
- Maintain close cooperation with security service providers to share threat intelligence
- Conduct regular security assessments and upgrade protection capabilities
- Integrate professional security services

As crucial entry points to the Web3 world, wallets play a key role in protecting user assets. By establishing comprehensive security strategies, continuously upgrading protection capabilities, and actively adopting industry-leading security solutions, wallets can provide users with a more secure and reliable service environment. This is not just a responsibility but also a necessary condition for maintaining advantages in a highly competitive market.

2.4.8 Future Outlook

As of 2024, known losses from phishing signature attacks have reached $790 million. Although these types of attacks decreased in the second half of the year, this might indicate that attackers are shifting towards other attack methods, such as malware and other more covert approaches.

As the Web3 ecosystem continues to develop, the challenges of protecting user assets remain. Regardless of how attack methods evolve, continuous security awareness and building protective capabilities remain key to safeguarding assets.

2.5 Scam Techniques

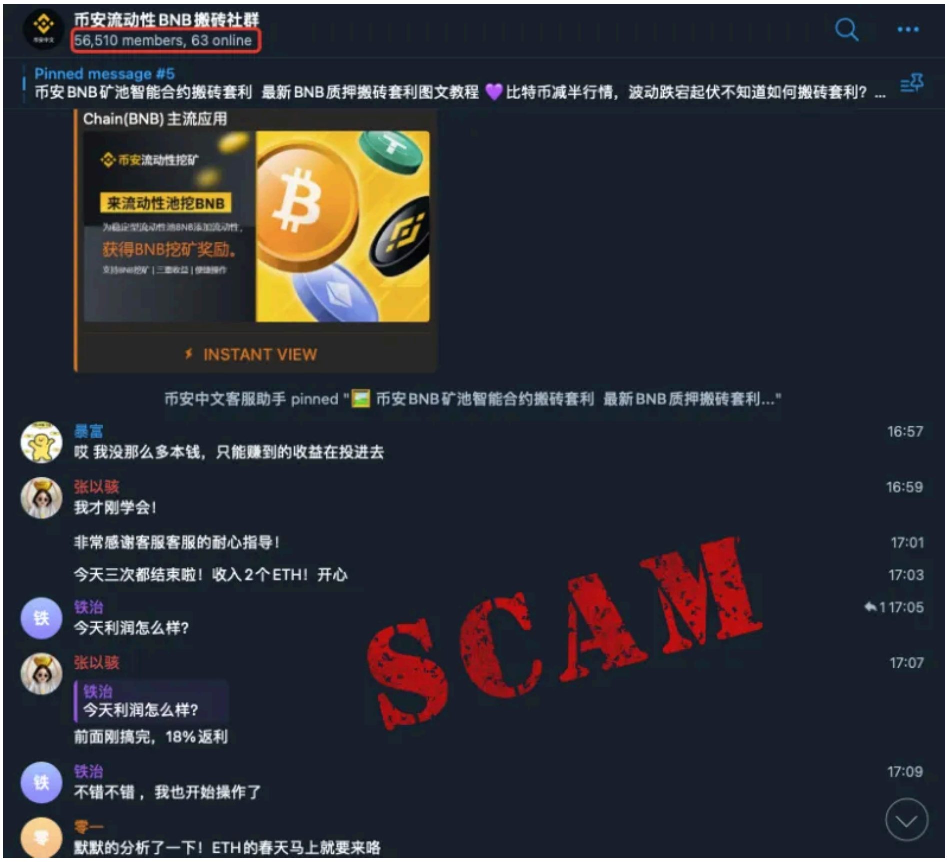
According to the data collected by the SlowMist AML team, scams remain one of the primary causes of losses. This issue has become particularly pronounced with the influx of new users into the Web3 space during bull markets. Many newcomers, unaware of the dangers lurking in the dark forest of blockchain will often fall victim to scams early on.

Scammers take advantage of new users' limited knowledge of the crypto market and their desire for high returns. They use convincing designs and seemingly legitimate operations to gradually lure users into investing their funds. For those who lack experience or strong security awareness, these schemes can be incredibly misleading and hard to recognize as fraud. A recent example is the rise of fake Zoom phishing attacks, which combine social engineering tactics with Trojan malware. Even a single mistake can leave users vulnerable to these scams. Below, we highlight some common types of fraud.

2.5.1 Mining Scams

Mining scams typically operate under the pretense that funds must be "locked in a pool" for a certain period to generate returns. This mechanism delays the realization of the scam, making it harder for users to recognize they've been deceived. Guided by scammers, users often invest more funds in pursuit of higher returns. When users are no longer able to contribute funds, scammers threaten that their principal will become unrecoverable, pushing victims into greater losses under increasing pressure.

Victims have reported that scammers often impersonate well-known exchanges on Telegram, creating fake groups with thousands—even tens of thousands—of members. This large membership count makes the groups appear legitimate and lowers users’ defenses. Many users rely on the number of group members as a way to determine an account's authenticity, a logic that scammers exploit. While it's true that official groups often have large memberships, the reverse isn’t necessarily true. It’s hard to imagine that a scammer would create a group with tens of thousands of members just to target a handful of victims. However, even the casual "chatter" within these groups is often bait designed to lure users into scams. One notable red flag is a group with over 50,000 members but fewer than 100 active participants at any given time. Comparing this to the usual activity levels in other large groups, observant users might recognize something suspicious.



币安流动性 BNB 搬砖社群
56,510 members, 63 online

Pinned message #5
币安BNB矿池智能合约搬砖套利 最新BNB质押搬砖套利图文教程 💜比特币减半行情，波动跌宕起伏不知道如何搬砖套利? ...

Chain(BNB) 主流应用

币安中文客服助手 pinned "🖼 币安BNB矿池智能合约搬砖套利 最新BNB质押搬砖套利..."

暴富 16:57
哎 我没那么多本钱，只能赚到的收益在投进去

张以骇 16:59
我才刚学会!

非常感谢客服客服的耐心指导! 17:01

今天三次都结束啦! 收入2个ETH! 开心 17:03

铁治 1 17:05
今天利润怎么样?

张以骇 17:07
> 铁治
> 今天利润怎么样?

前面刚搞完，18%返利

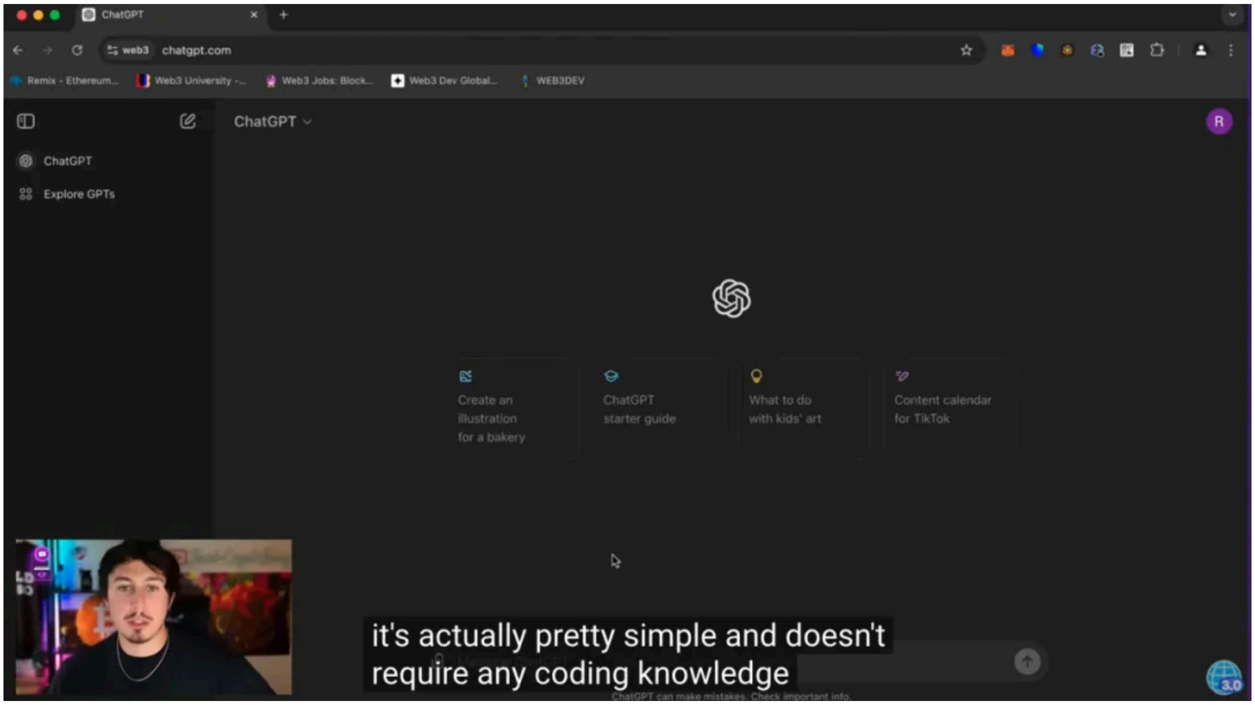
铁治 17:09
不错不错，我也开始操作了

零一
默默的分析了一下! ETH的春天马上就要来咯

Scammers will go the extra mile to deceive beginners, providing detailed step-by-step guides on tasks such as checking staking pools, downloading wallets, and transferring funds to fraudulent contract addresses. By creating the illusion of liquidity mining and offering economic incentives, they successfully lure victims into investing. Once users transfer funds to the scam contract address, they often receive a small return, encouraging them to invest even more in hopes of greater profits—exactly as the scammers planned. Eventually, all of the users' funds are stolen. Adding insult to injury, some scammers return fake tokens as "rewards." Unaware of their worthlessness, users think they've received legitimate profits, only to discover the tokens have no value when they try to trade them. Scammers may also trick users into granting malicious permissions, allowing them to drain the victims' wallets entirely.

2.5.2 Arbitrage Scams

AI tools like ChatGPT have become popular productivity enhancers, and scammers are leveraging this trend to make their schemes appear credible and advanced. For example, they label their scams with the "ChatGPT" brand to grab attention and build trust. However, ChatGPT only briefly features in the scam, usually as part of a fraudulent video tutorial.



it's actually pretty simple and doesn't require any coding knowledge

Scammers claim their "arbitrage bot" can monitor new tokens and significant price changes on Ethereum to identify arbitrage opportunities. All the user has to do, they say, is set it up and wait for profits. To participate, users are instructed to:

- Set up a MetaMask wallet.
- Open a (fake) Remix link provided in the tutorial.
- Paste the scammer's code, compile the bot, and deploy the smart contract.

At this stage, scammers demand an initial fund transfer to the contract, claiming that the more ETH users deposit, the greater their profits will be. But once users follow these steps and click “start,” their funds are transferred to the scammer's wallet through a backdoor in the code.

Using on-chain data and our anti-money laundering platform MistTrack, we analyzed the scammers' wallets. The scammers follow a "wide-net, small-gain" approach, targeting numerous victims for relatively small amounts. Since individual losses are minor, many victims do not pursue the matter, allowing the scammers to remain at large. They often rebrand their scams and continue their fraudulent activities.

2.5.3 Airdrop Scams

In Web3, projects often distribute free tokens to certain wallet addresses as a marketing strategy to increase visibility and attract early users. This process, known as "airdropping," can quickly bring a project into the public eye, build a user base, and boost market influence. To participate in an airdrop, users typically click on links and interact with the project to claim their tokens. However, hackers exploit this process by setting traps at every stage, from fake websites to tools embedded with malicious backdoors.

(1) Fake Airdrops

Fake airdrop scams can be categorized into the following types:

- Hacked Official Accounts Posting Fake Airdrop Messages

We often see security reminders on information platforms that "X account or Discord account of a certain project has been hacked, please do not click on the phishing links posted by hackers." Users usually click on these links based on their trust in the official account, and are then directed to phishing websites disguised as airdrops. Once the private key/mnemonic phrase is entered or relevant permissions are authorized on the phishing website, hackers can steal the user's assets.

- Fake Accounts Spamming Comments with Phishing Links

Hackers create fake accounts resembling official project accounts and spam airdrop announcements in the comment sections of legitimate posts. These comments often include phishing links to mislead users. Additionally, when official accounts announce legitimate airdrops, hackers quickly follow up with fake posts on social media platforms using high-quality spoofed accounts. They lure users into installing fake apps or visiting phishing websites where users mistakenly sign fraudulent transactions or grant harmful permissions.

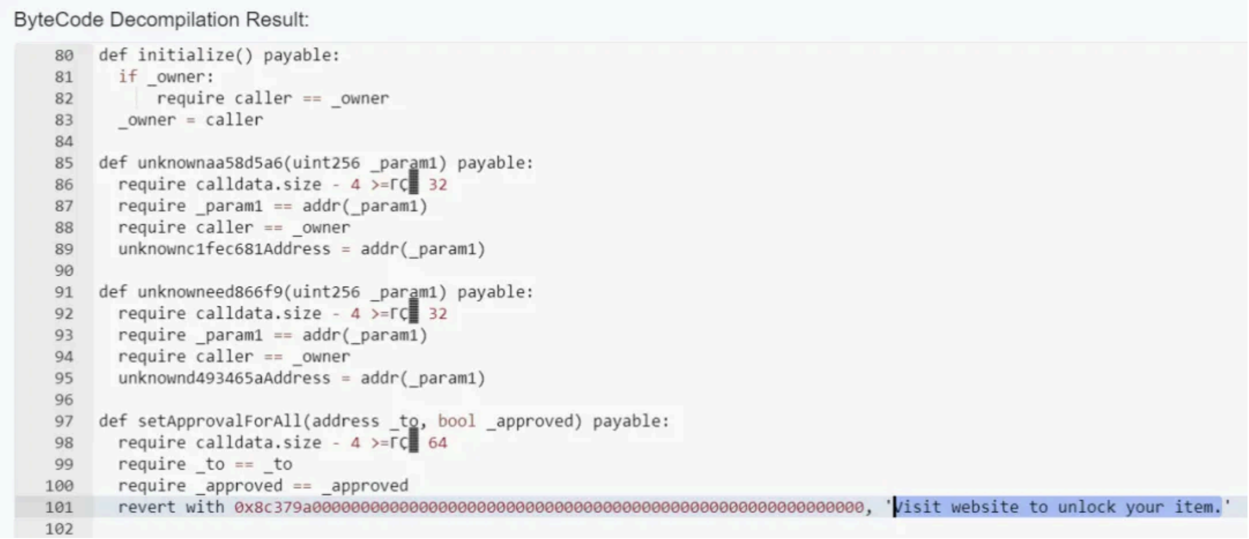
- Social Engineering in Community Groups

Scammers often lurk in Web3 project community groups, targeting users with social engineering tactics. They may pose as helpful individuals or "official support" staff and use airdrops as bait. Scammers instruct victims to perform specific actions, such as transferring tokens, to qualify for the airdrop. Key Tip: Be cautious of anyone who contacts you directly, claiming to be official support or offering guidance on how to participate in an airdrop. These individuals are likely scammers, and what starts as an attempt to claim free tokens can result in significant financial losses.

(2) "Free" Airdropped Tokens

In some cases, users don't need to perform any tasks to receive airdropped tokens—they simply appear in their wallets. However, this "free" gift can be a trap. Hackers may airdrop tokens with no real value to users' wallets. Curious users might try to interact with these tokens by transferring, viewing, or trading them on decentralized exchanges. Upon reverse-engineering a Scam NFT smart contract, we discovered that any attempt to list or transfer the Scam NFT triggers a failure. The error message prompts users to "Visit the website to unlock your item," thereby leading them to a phishing site.

Key Tip: Be wary of interacting with unknown tokens or NFTs in your wallet. Doing so may expose you to phishing scams or malicious contracts.



ByteCode Decompilation Result:

```
def initialize() payable:
  if _owner:
      require caller == _owner
  _owner = caller

def unknownaa58d5a6(uint256 _param1) payable:
  require calldata.size - 4 >=ΓÇ█ 32
  require _param1 == addr(_param1)
  require caller == _owner
  unknownc1fec681Address = addr(_param1)

def unknowneed866f9(uint256 _param1) payable:
  require calldata.size - 4 >=ΓÇ█ 32
  require _param1 == addr(_param1)
  require caller == _owner
  unknownd493465aAddress = addr(_param1)

def setApprovalForAll(address _to, bool _approved) payable:
  require calldata.size - 4 >=ΓÇ█ 64
  require _to == _to
  require _approved == _approved
  revert with 0x8c379a000000000000000000000000000000000000000000000000000000000, 'Visit website to unlock your item.'
```

When users visit a phishing site linked to a Scam NFT, it allows hackers to carry out the following actions:

- Mass "Zero-Cost Purchases" of Valuable NFTs

Hackers exploit phishing tactics to acquire NFTs without payment. See detailed analysis in the "Zero-Cost Purchase" NFT phishing report.

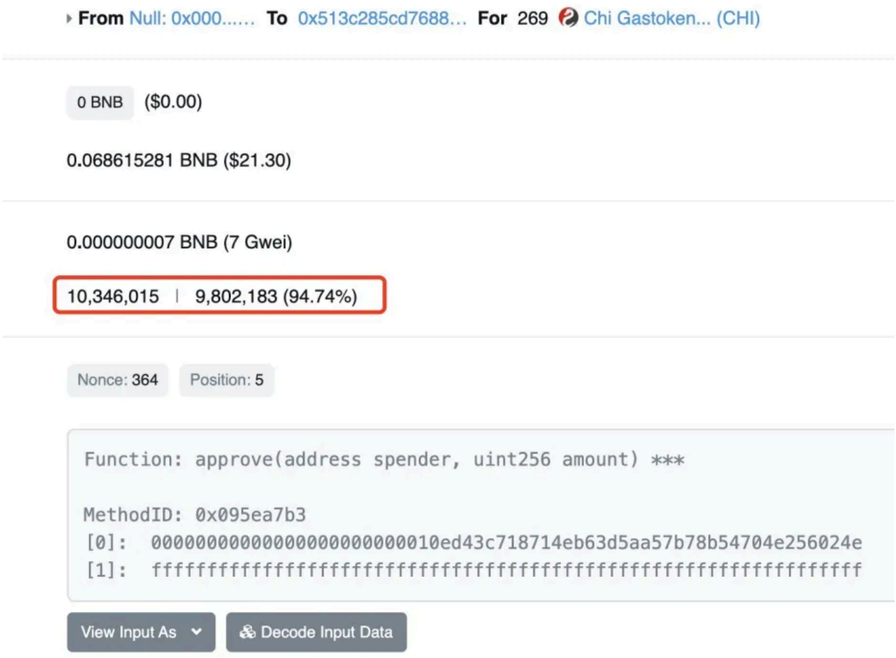
- Stealing Tokens Through Approve Authorizations or Permit Signatures

Hackers gain access to approved tokens, allowing them to transfer funds without further user interaction.

- Draining Native Assets

Hackers directly transfer native assets from the user's wallet. Additionally, hackers can cleverly design malicious smart contracts to steal users' gas fees. For example, a malicious contract named GPT was deployed on the Binance Smart Chain (BSC) (contract address: 0x513C285CD76884acC377a63DC63A4e83D7D21fb5), using airdropped tokens to lure users into interacting with it.

When users interact with this malicious contract, they are prompted to approve the contract to access tokens in their wallet. If the user grants approval, the malicious contract dynamically increases the gas limit based on the user's wallet balance, causing subsequent transactions to consume significantly more gas. The malicious contract then utilizes the excess gas to mint CHI tokens (CHI tokens can be used for gas fee reimbursement). Once the contract accumulates a substantial amount of CHI tokens, the hacker burns the CHI tokens to receive a gas refund upon contract destruction. This tactic allows hackers to profit from users' gas fees without their knowledge. Users may mistakenly believe they can profit by selling the airdropped tokens, only to realize their native assets have been stolen in the process.



From Null: 0x000...... To 0x513c285cd7688... For 269 Chi Gastoken... (CHI)

0 BNB ($0.00)

0.068615281 BNB ($21.30)

0.000000007 BNB (7 Gwei)

10,346,015 | 9,802,183 (94.74%)

Nonce: 364 Position: 5

```
Function: approve(address spender, uint256 amount) ***

MethodID: 0x095ea7b3
[0]:  00000000000000000000000010ed43c718714eb63d5aa57b78b54704e256024e
[1]:  ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

(3) Backdoor Tools

During the process of claiming airdrops, some users are required to download plugins for tasks like translation or token rarity analysis. These plugins often have questionable security, and many users inadvertently download them from unofficial sources, significantly increasing the risk of downloading plugins embedded with backdoors.

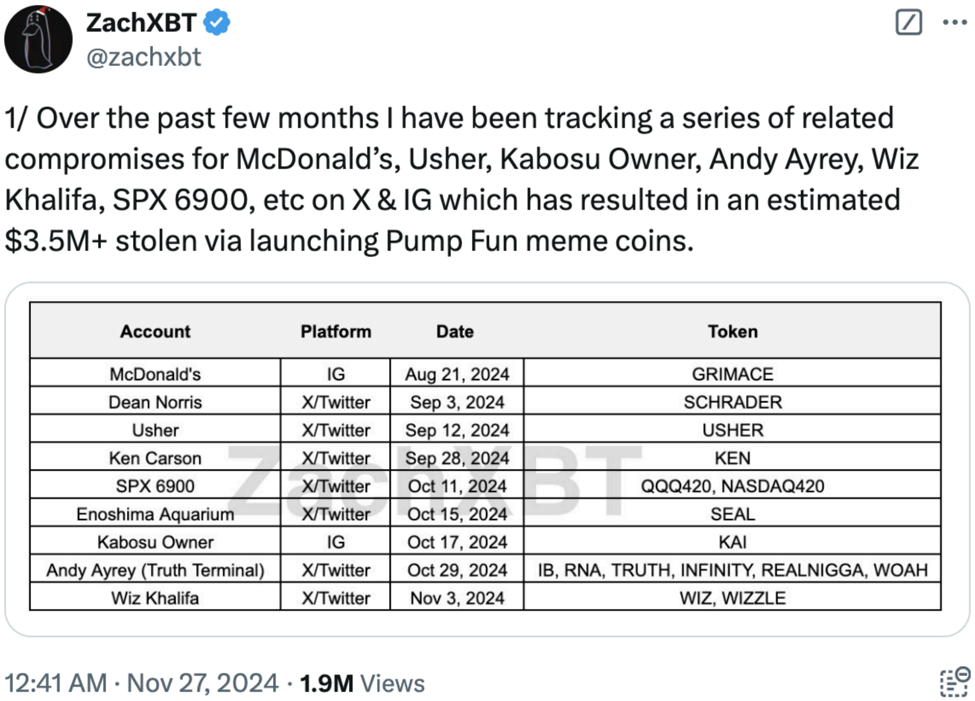
Additionally, services selling airdrop scripts have surfaced online, claiming to enable automatic bulk interactions through script execution. While this may sound efficient, downloading unverified and unaudited scripts poses a significant risk. These scripts may contain malicious code capable of stealing private keys, mnemonic phrases, or performing unauthorized operations. Worse still, some users carry out these risky operations without antivirus software installed or with it disabled, leaving their devices vulnerable to Trojan infections that can cause significant harm.

2.5.4 X Account Compromise

As Web3 continues to attract new users, often driven by FOMO (fear of missing out), account compromise incidents have surged. Many inexperienced or security-conscious users have suffered losses as a result. Hackers exploit the influence of well-known accounts and celebrities to spread misinformation, including false claims about token price manipulation, phishing links, or promotions for fake tokens. Once users click on phishing links or interact with fraudulent tokens promoted by hackers, they are often victimized. According to SlowMist’s security team, there were 94 account compromise incidents in 2024, accounting for 22.9% of all reported security incidents.

Notably, hackers have expanded their targets beyond well-known blockchain projects and members to include prominent brands in traditional industries and reputable official institutions. For instance, in January 2024, the U.S. Securities and Exchange Commission's (SEC) X account was unauthorizedly taken over. Hackers posted fake news allegedly from the SEC Chair, claiming that a Bitcoin ETF had been approved, which caused Bitcoin (BTC) prices to temporarily surge by $1,000. Additionally, meme coins have been particularly active during this bull market, drawing numerous Web2 celebrities into participation. On November 27, 2024, blockchain investigator ZachXBT reported on X: "Over the past few months, I’ve been tracking a series of attacks targeting McDonald’s, Usher, Kabosu’s Owner, Andy Ayrey, Wiz Khalifa, SPX 6900, and others through X and

Instagram. These attacks, involving the launch of Pump.Fun meme coins, have resulted in over $3.5 million in stolen funds."



ZachXBT
@zachxbt

1/ Over the past few months I have been tracking a series of related compromises for McDonald's, Usher, Kabosu Owner, Andy Ayrey, Wiz Khalifa, SPX 6900, etc on X & IG which has resulted in an estimated $3.5M+ stolen via launching Pump Fun meme coins.

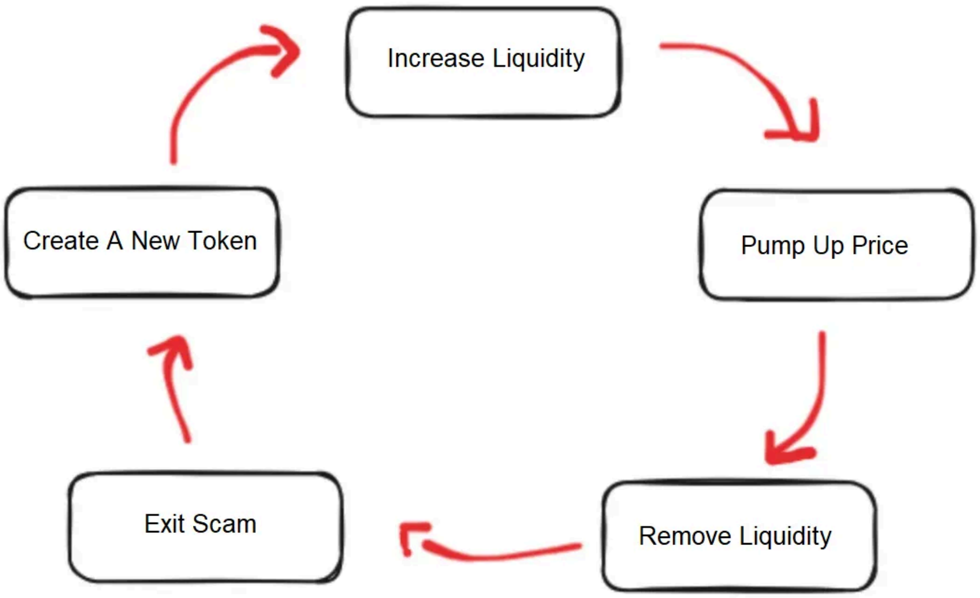
Account	Platform	Date	Token
McDonald's	IG	Aug 21, 2024	GRIMACE
Dean Norris	X/Twitter	Sep 3, 2024	SCHRADER
Usher	X/Twitter	Sep 12, 2024	USHER
Ken Carson	X/Twitter	Sep 28, 2024	KEN
SPX 6900	X/Twitter	Oct 11, 2024	QQQ420, NASDAQ420
Enoshima Aquarium	X/Twitter	Oct 15, 2024	SEAL
Kabosu Owner	IG	Oct 17, 2024	KAI
Andy Ayrey (Truth Terminal)	X/Twitter	Oct 29, 2024	IB, RNA, TRUTH, INFINITY, REALNIGGA, WOAH
Wiz Khalifa	X/Twitter	Nov 3, 2024	WIZ, WIZZLE

12:41 AM · Nov 27, 2024 · **1.9M** Views

(https://x.com/zachxbt/status/1861450263925559399)

2.5.5 Honeypot Scams

In these scams, users purchase scam tokens and often see the token value rapidly increase, leading them to hold onto the tokens in hopes of even greater gains. However, the smart contract is designed to restrict selling in various ways—such as blacklisting buyer addresses, altering token balances in wallets, or setting excessively strict selling conditions. Ultimately, users find themselves unable to sell the tokens, leaving their funds trapped.



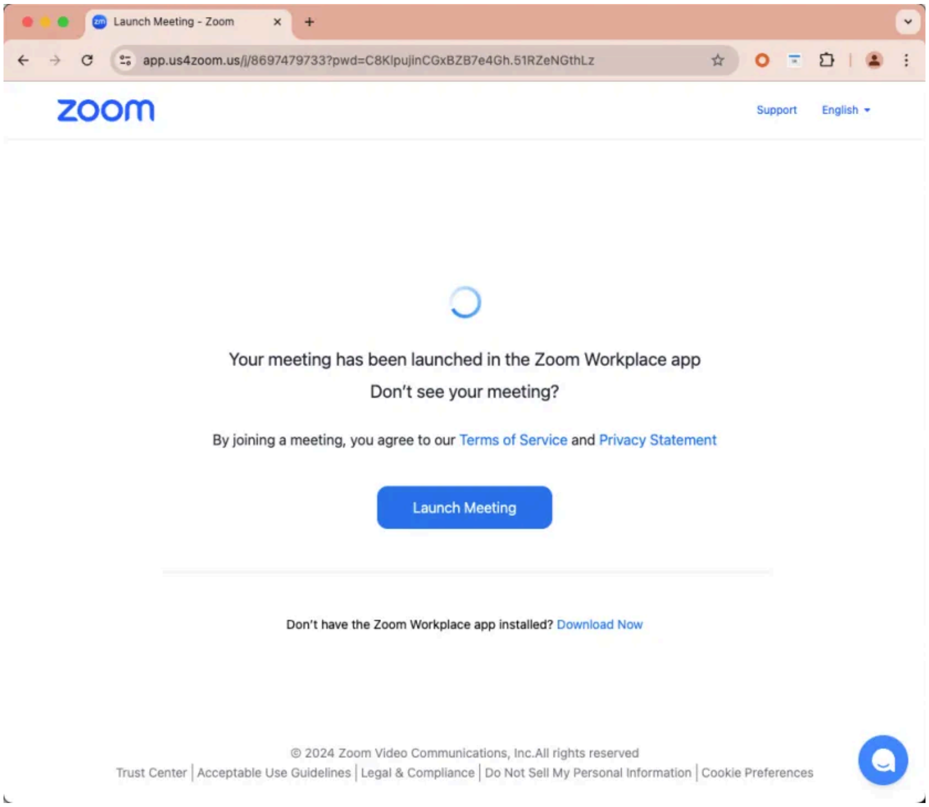
Common Reasons Users Fall into a Honeypot Scam:

- Imitation Tokens: Just as counterfeit money exists in the real world, fake tokens exist in the crypto space. Some fraudulent projects mimic the names and branding of well-known projects, creating token contracts with identical names. Users who fail to verify the token contract address carefully may unknowingly purchase these imitation tokens, only to find themselves unable to sell them later.
- "Race-to-Exit" Mentality: Some users knowingly participate in dubious projects, even after spotting warning signs (such as a candlestick chart showing continuous green candles). They gamble on the idea that they can exit quickly before the scheme collapses. The assumption is simple: buy during an upward trend and sell at the right time for a guaranteed profit. However, when they attempt to sell, they often find they cannot perform the transaction or can only sell a tiny fraction of their tokens.
- Induced by Scammers: Another common scenario involves users falling for scammers' persuasive pitches, leading them to invest in honeypot scams.

2.5.6 Trojan Attacks

In 2024, multiple users reported a phishing attack disguised as a Zoom meeting link. In one incident, a victim clicked on a malicious Zoom link and unknowingly installed malware, resulting in the theft of cryptocurrency assets worth millions of dollars. The malware is capable of collecting system information, stealing browser data, and accessing cryptocurrency wallet details. It then transmits the stolen data to a hacker-controlled server. These attacks often combine social engineering tactics with Trojan-based techniques, making it easy for unsuspecting users to fall victim.

According to analysis by the SlowMist security team, hackers used domains such as "app[.]us4zoom[.]us" to mimic legitimate Zoom meeting links. These pages closely resemble genuine Zoom interfaces. When users click the "Start Meeting" button, instead of launching the local Zoom client, they download a malicious installation package.


Launch Meeting - Zoom
app.us4zoom.us/j/8697479733?pwd=C8KlpujinCGxBZB7e4Gh.51RZeNGthLz
zoom
Support
English
Launch Meeting

Your meeting has been launched in the Zoom Workplace app

Don't see your meeting?

By joining a meeting, you agree to our Terms of Service and Privacy Statement

Don't have the Zoom Workplace app installed? Download Now

© 2024 Zoom Video Communications, Inc.All rights reserved

Trust Center | Acceptable Use Guidelines | Legal & Compliance | Do Not Sell My Personal Information | Cookie Preferences

After malicious code collects system information, browser data, cryptocurrency wallet details, Telegram data, Notes entries, and Cookie data, it compresses and transmits this information to a hacker-controlled server. During its operation, the malicious program often tricks users into entering their passwords. Additionally, subsequent malicious scripts may access the computer's Keychain data, which could include various passwords stored on the device. Hackers then attempt to decrypt this data to obtain sensitive information, such as wallet seed phrases and private keys, enabling them to steal the user's assets. The SlowMist security team strongly advises users to exercise caution before clicking on meeting links, avoid executing software or commands from unverified sources, and ensure they have antivirus software installed and regularly updated.

III. Anti-Money Laundering(AML) Trends

3.1 AML and Regulatory Dynamics

In 2024, the regulatory landscape for cryptocurrencies experienced significant developments, highlighted by the European Union's implementation of the Markets in Crypto-Assets (MiCA) regulation and the United States advancing stablecoin legislation. These efforts were driven by growing concerns about fraud, money laundering, and terrorist financing activities in the rapidly evolving crypto sector. This year saw the introduction of more stringent measures worldwide to combat illicit activities, with notable advancements in stablecoin regulation, cross-border crypto policies, and enforcement actions targeting major players in the crypto space.

3.1.1 Stablecoin Regulation

As global financial authorities increasingly recognize the growing influence and risks of digital assets, stablecoin regulation became a central focus in 2024. The collapse of TerraUSD in 2022 served as a stark reminder of market vulnerabilities, prompting stricter and clearer regulatory frameworks worldwide. This year marked a turning point as regions enacted legislation and policies to address the unique challenges posed by stablecoins while fostering innovation in the digital economy.

- **China**: In its 2024 Financial Stability Report, the People's Bank of China provided a detailed analysis of global cryptocurrency regulatory trends, with a particular focus on Hong Kong's progress in crypto compliance. The report emphasized the need for strengthened oversight of crypto assets.
- **Hong Kong, China**: On December 6, 2024, the Hong Kong Monetary Authority (HKMA) and the Financial Services and Treasury Bureau introduced the Stablecoin Bill. This bill aims to establish a regulatory framework for fiat-backed stablecoin issuers and enhance oversight of virtual asset activities.

- **European Union**: The EU approved the Markets in Crypto-Assets (MiCA) regulation, creating the world's first comprehensive and transparent framework for virtual asset oversight. Set to take effect by the end of 2024, MiCA requires stablecoin issuers to obtain an electronic money license, maintain adequate reserves, and adhere to strict transaction standards. Tether Limited, the issuer of USDT, failed to meet these requirements, leading to USDT's removal from EU-compliant platforms starting December 30, 2024.
- **Brazil**: The Central Bank of Brazil (BCB) plans to regulate stablecoins and asset tokenization by 2025. In November 2024, the BCB proposed a regulation to prohibit users from withdrawing stablecoins from centralized exchanges to self-custody wallets. However, in December, the BCB suggested it might revoke this restriction if improvements in transaction transparency and other critical issues are achieved.
- **United States**: Stablecoin issuers in the U.S. are now required to maintain a 1:1 reserve ratio, a measure supported by ongoing legislative discussions.
- **Middle East**: The UAE introduced a dedicated stablecoin license under its Virtual Asset Regulatory Authority (VARA), signaling the region's intent to lead in regulatory transparency. Qatar also included stablecoins in its first digital asset framework, marking a significant step in crypto regulation.

3.1.2 SEC Enforcement Actions

In November, the U.S. Securities and Exchange Commission (SEC) released its enforcement results for fiscal year 2024. The report revealed a total of 583 enforcement actions, representing a 26% decrease compared to 2023. Despite fewer actions, the SEC imposed a record-breaking $8.2 billion in penalties. Among these cases, the SEC initiated 431 "standalone" enforcement actions, a 14% decrease from 2023. It also pursued 93 "follow-on" administrative proceedings, aimed at barring or suspending individuals from holding specific roles in the securities industry based on criminal convictions, civil injunctions, or other orders—down 43% from the previous year. Additionally, there were 59 cases against issuers for failing to file required documents with the SEC, a 51% decline from 2023. The $8.2 billion in monetary remedies included $6.1 billion in disgorgement and prejudgment interest, the highest amount ever recorded, and $2.1 billion in civil penalties, the second highest on record. Notably, approximately 56% of these financial remedies stemmed from jury verdicts in cases involving one of the largest securities frauds in U.S. history.

In 2024, the SEC also secured orders prohibiting 124 individuals from serving as officers or directors of public companies, the second-highest number in a decade. Furthermore, the SEC distributed $345 million to harmed investors during the fiscal year, bringing the total amount returned to investors since FY 2021 to over $2.7 billion. The SEC received a record-high 45,130 tips, complaints, and referrals in 2024, including more than 24,000 whistleblower tips. Over 14,000 of these tips were submitted by just two individuals. The Commission awarded $255 million in whistleblower rewards during the year. The SEC highlighted that its 2024 enforcement actions addressed emerging threats such as artificial intelligence-related misrepresentations and fraudsters exploiting social media for romance scams. Simultaneously, the agency maintained a focus on perennial investor risks, including material misstatements, inadequate internal controls, and significant gatekeeper failures.

Examples of SEC Enforcement Actions in the Crypto Ecosystem:

- Terraform Labs Settlement: Terraform Labs agreed to a $4.5 billion settlement with the U.S. Securities and Exchange Commission (SEC) over the collapse of their TerraUSD and Luna cryptocurrencies. The settlement includes $3.5 billion in disgorgement, $460 million in interest, $420 million in civil penalties, and a $200 million personal contribution from former CEO Do Kwon.
- Jump Trading Penalty: High-speed trading firm Jump Trading Group agreed to pay a $123 million settlement to the SEC for misleading investors about the stability of TerraUSD, a stablecoin that collapsed in 2022. The SEC alleged that Jump's unit, Tai Mo Shan, falsely assured investors about TerraUSD's stability, contributing to its downfall.
- SEC Lawsuit Against Cumberland DRW: The SEC sued Cumberland DRW, the cryptocurrency unit of high-speed trading firm DRW Holdings, for failing to register as a securities dealer. The lawsuit alleges that Cumberland accrued millions in profits by trading with hedge funds and large market players without proper registration.

3.1.3 Anti-Money Laundering Sanctions

- Hong Kong's Directive to Worldcoin (May 2024): The Hong Kong Office of the Privacy Commissioner for Personal Data issued an enforcement notice to the Worldcoin Foundation, ordering the suspension of all operations in the region due to privacy and personal data concerns. Worldcoin was directed to cease scanning and collecting iris and facial images from the public, reflecting Hong Kong's commitment to protecting personal data within the crypto space.

- Arrest of Two Chinese Nationals (May 2024): The U.S. Department of Justice arrested two Chinese nationals, Daren Li and Yicheng Zhang, for orchestrating a large-scale cryptocurrency scam known as a "pig-butchering" scheme. The scam involved laundering at least $73 million.
- U.S. Sanctions on Iranian Crypto Mining Activities (May 2024): The U.S. Treasury Department, through its Office of Foreign Assets Control (OFAC), expanded sanctions on Iranian cryptocurrency mining operations. These sanctions targeted individuals and entities using crypto mining to evade international sanctions.
- Seizure of Over $6 Million in Crypto Linked to a Scam (Sept 2024): The U.S. Department of Justice announced the seizure of more than $6 million in cryptocurrency held by Southeast Asian criminals. These individuals orchestrated fraudulent cryptocurrency investment schemes, commonly referred to as "pig-butchering" scams, targeting U.S. residents. The FBI traced victim funds on the blockchain, identifying multiple wallets containing illicit funds.
- U.S. Sanctions on Russian Cybercriminals (Sept 2024): The U.S. Treasury sanctioned Sergey Ivanov and Cryptex, accused of laundering money for cybercriminals and darknet vendors. Additionally, the Treasury's Financial Crimes Enforcement Network designated the Russian cryptocurrency exchange PM2BTC as a significant money laundering threat.
- Sanctions Against North Korea’s Crypto Laundering Network (Dec 2024): Under Executive Order 13382, the U.S. imposed sanctions on two individuals and one entity associated with laundering cryptocurrency for North Korea. The network was used to fund the Democratic People's Republic of Korea's illicit weapons of mass destruction and ballistic missile programs.
- Indictment of LockBit Ransomware Developer (Dec 2024): The U.S. charged Rostislav Panev, a dual citizen of Russia and Israel, with developing and maintaining the LockBit ransomware code. Panev allegedly received over $230,000 in cryptocurrency for his role. He was arrested in Israel and awaits extradition to the U.S.

3.1.4 Regulatory Policies

3.1.4.1 Asia-Pacific

- **China:** In December 2024, the People's Bank of China released the China Financial Stability Report (2024), highlighting global cryptocurrency regulatory developments and Hong Kong's progress in compliance. The report emphasized that cryptocurrencies pose potential spillover risks to financial stability, prompting regulators worldwide to intensify oversight. It noted that 51 countries and regions have implemented bans on crypto assets, and some economies have amended existing laws or introduced new legislation for regulation. Hong Kong actively explores licensing regimes, categorizing virtual assets into securitized and non-securitized financial assets and enforcing a dual-license system for virtual asset trading platform operators.
- **Hong Kong, China**: In April 2024, Hong Kong approved spot Bitcoin and Ethereum Exchange-Traded Funds (ETFs), offering investors new opportunities. The Securities and Futures Commission (SFC) licensed four additional virtual asset trading platforms, strengthening regulatory oversight. Hong Kong also introduced a stablecoin sandbox and related legislation to establish a clear regulatory framework for stablecoin issuance and use.
- **Japan:** Japan advanced crypto tax reforms, reducing transaction profit taxes to 20%, and emphasized stricter anti-money laundering (AML) and Know Your Customer (KYC) compliance for exchanges and issuers.
- **South Korea:** South Korea enacted the Virtual Asset User Protection Act to enhance investor safety and regulate cross-border crypto transactions.
- **Vietnam:** Vietnam announced its National Blockchain Development Strategy, aiming to become a regional leader by 2030. However, cryptocurrencies remain unclassified and prohibited as legal tender, underscoring efforts to balance innovation and crime prevention.
- **Singapore:** The Monetary Authority of Singapore (MAS) revised the Payment Services Act, expanding the scope of regulated payment activities to include digital payment token services. MAS has issued major payment institution licenses to at least 19 crypto service providers, allowing them to offer digital token services.

- **Malaysia:** The Securities Commission of Malaysia announced a list of six approved cryptocurrency exchanges. Unapproved entities were instructed to cease activities immediately and refund investors.

3.1.4.2 North America

- **United States**: The approval of Bitcoin and Ethereum ETFs marked a milestone in mainstream cryptocurrency adoption. On January 10, 2024, the SEC approved the first spot Bitcoin ETF, followed by Ethereum ETF approval on May 23. Ethereum spot ETFs began trading on July 23. As of this year, spot Bitcoin ETFs have a net asset value of $105.08 billion (5.7% of Bitcoin's market cap), while Ethereum spot ETFs total $12.05 billion (2.94% of Ethereum's market cap). The Financial Innovation and Technology for the 21st Century Act (FIT21) clarified cryptocurrency classification and retained existing crypto custody accounting standards by opposing SAB 121. The Trump administration's pro-innovation policies included appointing crypto advocates like Paul Atkins as SEC Chair, signaling strong industry support.
- **Canada**: Canada continued refining its crypto regulatory framework, emphasizing AML and KYC compliance for crypto exchanges and service providers. The Canadian Securities Administrators (CSA) enhanced oversight of crypto asset investment products to ensure greater transparency and investor protection.

3.1.4.3 Europe

- **Russia**: Russia accelerated cryptocurrency regulations in 2024 to mitigate the impact of Western sanctions, focusing on leveraging digital assets for international trade. President Vladimir Putin legalized crypto mining and permitted cross-border transactions using mined assets. Authorities explored stablecoins (particularly those pegged to the Chinese yuan or BRICS currencies) for cross-border payments and established two state-supervised crypto exchanges to facilitate international trade.
- **European Union**: The Markets in Crypto-Assets (MiCA) regulation took full effect across the EU on December 30, 2024, establishing Europe as the first region with a unified cryptocurrency regulatory framework. MiCA imposed strict requirements on stablecoin issuers, including reserve backing and operational standards, while enhancing consumer protection.

- **United Kingdom**: The Financial Conduct Authority (FCA) plans to introduce a comprehensive crypto regulatory regime by 2026, building on the EU's MiCA framework.

3.1.4.4 Middle East and Africa

- **United Arab Emirates**: The UAE, through its Virtual Assets Regulatory Authority (VARA), solidified its global leadership in crypto regulation by issuing 13 new licenses in 2024. It also introduced stablecoin-specific licensing to address evolving market demands.
- **Saudi Arabia**: Saudi Arabia emerged as the region's fastest-growing crypto economy, leveraging blockchain innovation and piloting a central bank digital currency (CBDC) initiative.
- **United Arab Emirates**: The UAE, through its Virtual Assets Regulatory Authority (VARA), solidified its global leadership in crypto regulation by issuing 13 new licenses in 2024. It also introduced stablecoin-specific licensing to address evolving market demands.

3.1.4.5 Latin America

- **Argentina**: Argentina adopted a compliance framework for Virtual Asset Service Providers (VASPs) and planned the free circulation of currencies, including Bitcoin.
- **Brazil**: Brazil advanced its CBDC (DREX) pilot, focusing on real-world asset (RWA) development to enhance financial inclusion.
- **El Salvador**: El Salvador expanded its Bitcoin legal tender policy and collaborated with Argentina to develop cross-border crypto solutions.

In summary, due to the complexity of cryptocurrencies, regulatory discussions encompass financial stability, consumer protection, and anti-money laundering efforts. As blockchain and cryptocurrency technologies gain wider adoption, more governments and institutions are stepping in, and regulatory frameworks are evolving toward greater specificity and global alignment.

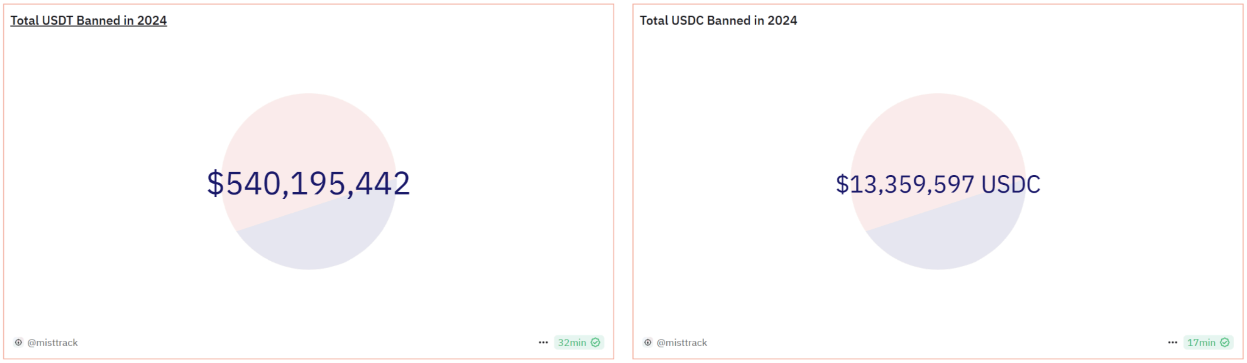
3.2 Anti-Money Laundering Data

3.2.1 Frozen Funds Data

3.2.1.1 SlowMist Assist Freezing

With significant support from partners in the InMist intelligence network, SlowMist assisted clients, partners, and public hacking incident victims in freezing over $112 million in 2024.

3.2.1.2 USDT and USDC Freezing



(https://dune.com/misttrack/2024)

In 2024, Tether froze $540,195,442 worth of USDT, while Circle froze $13,359,597 worth of USDC.

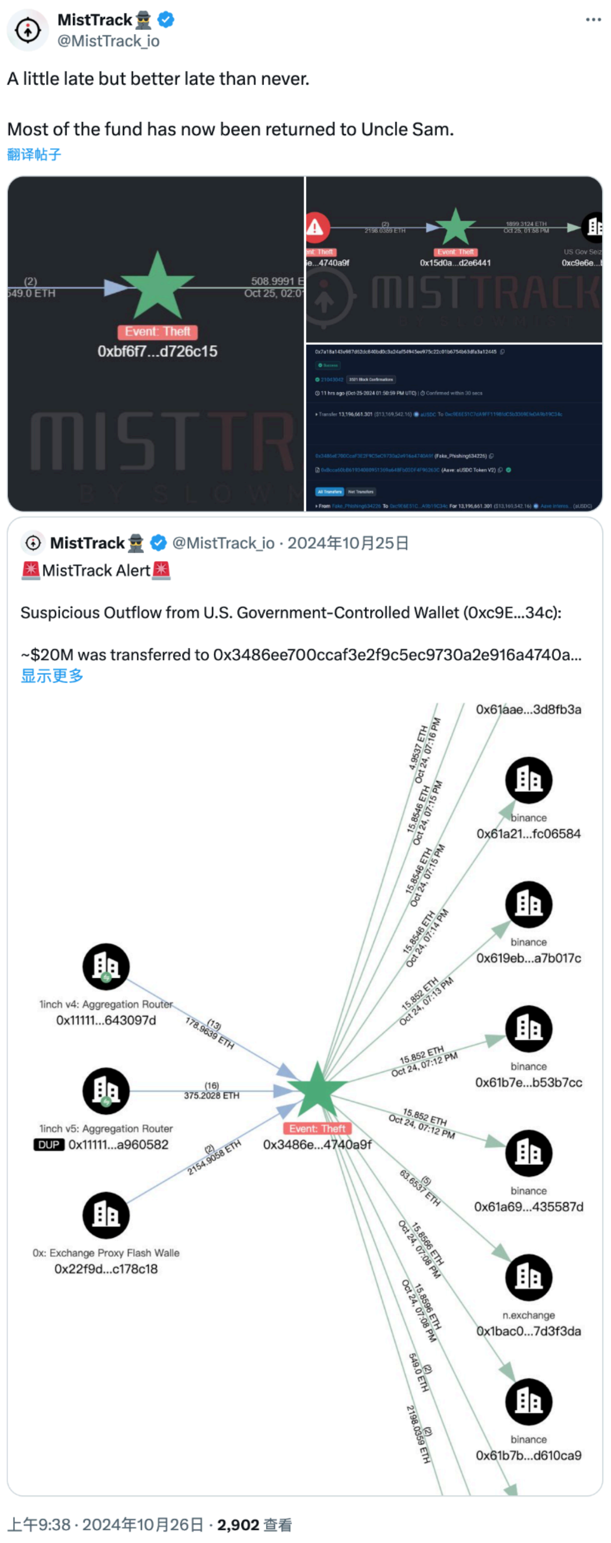
3.2.2 Fund Recovery Data

In 2024, there were 410 reported security incidents, with 24 cases successfully recovering all or part of the stolen funds. According to disclosed data, approximately $166 million was recovered, representing 8.25% of the total losses, which amounted to $2.013 billion.

A significant portion of the recovered funds—$62.5 million, or 37.65%—came from the Web3 gaming platform Munchables, operated by Blast. This case also highlighted the involvement of North Korean hackers. On March 27, 2024, Munchables suffered an attack, resulting in losses of approximately $62.5 million. It was revealed that the attackers, posing as developers, had infiltrated the project, gaining access to critical code and sensitive keys over an extended period. According to blockchain investigator ZachXBT, the Munchables team unknowingly hired four different developers, who were likely the same individual. Evidence included mutual recommendations for the role, regular fund transfers to two identical exchange deposit addresses, and shared wallet funding.

In a post on the X platform, Aavegotchi founder CoderDan disclosed that his team (@PixelcraftStuds) had tried this individual for game development in 2022. However, the person's behavior raised significant suspicions, reminiscent of North Korean hackers. They terminated the engagement within a month after the developer tried to recommend a "friend"—who was likely another hacker—for hire. Fortunately, under mounting pressure from the community and the Munchables team, the hackers eventually returned all stolen funds. Blast's founder Pacman announced via X: "Blast's core contributors successfully transferred $97 million into a multi-signature wallet. This required tremendous effort, but we are relieved that the former Munchables developer ultimately returned all the funds without requiring any ransom."

In addition to targeting DeFi projects and exchanges with large reserves, hackers have also aimed at government wallets. On October 25, 2024, a U.S. government-associated address (0xc9E6...C34c) was compromised, resulting in the transfer of approximately $20 million in cryptocurrencies to a hacker-controlled address (0x3486...0A9f). The compromised address had previously received funds from nine U.S. government-seized addresses related to the Bitfinex hack case. However, on the same day, the hackers began returning stolen funds to the U.S. government. They refunded approximately 13.19 million aUSDC and 2,408 ETH, valued at $19.3 million in total.



MistTrack🕵️ @MistTrack_io

A little late but better late than never.

Most of the fund has now been returned to Uncle Sam.

翻译帖子

MistTrack🕵️ @MistTrack_io · 2024年10月25日

🚨MistTrack Alert🚨

Suspicious Outflow from U.S. Government-Controlled Wallet (0xc9E...34c):

~$20M was transferred to 0x3486ee700ccaf3e2f9c5ec9730a2e916a4740a...

显示更多

上午9:38 · 2024年10月26日 · 2,902 查看

(https://x.com/MistTrack_io/status/1849989016755765702)

3.3 DPRK

In 2024, the Democratic People's Republic of Korea (DPRK) was implicated in a series of high-profile cyber heists, collectively stealing over hundreds of millions of dollars in cryptocurrency. The following is a chronological list of significant incidents attributed to DPRK-affiliated groups, with data from SlowMist Hacked:

Date	Target	Loss	Link
Sep, 2024	Linkedin Job Dev Scam	Unknown	Link
Apr-29, 2024	Rain	$14,800,000	Link
May-15, 2024	ALEX Labs	$4,300,000	Link
May-31, 2024	DMM Bitcoin	$305,000,000	Link
Jul-18, 2024	Wazirx	$230,000,000	Link
Sep-10, 2024	Indodax	$22,000,000	Link
Sep-19, 2024	BingX	$45,000,000	Link
Sep-25, 2024	Truflation	$5,600,000	Link
Oct-16, 2024	Radiant	$50,000,000	Link
	TOTAL	$676,700,000	

3.3.1 Methods of Attacks

Beyond technical exploits, many of these attacks relied heavily on social engineering to gain initial access or bypass security measures. For example, the DMM Bitcoin and Radiant breaches involved attackers building trust with targets through impersonation and phishing before deploying malware.

- Suspected North Korean Hackers Target Blockchain Community via Telegram

One prevalent tactic in 2024 involved phishing campaigns targeting blockchain and angel investing communities. In this campaign, attackers impersonated representatives of reputable investment firms on Telegram. They initiated conversations, scheduled fake meetings using platforms like Calendly, and convinced victims to download malicious App under the guise of resolving technical issues or sharing sensitive data.

- The Threat of DPRK IT Workers

Adding another dimension to DPRK's cyber operations is the deployment of IT workers into legitimate roles. According to Google's Threat Intelligence Group, North Korean operatives infiltrated IT, blockchain, and freelance platforms under false pretenses. These workers used falsified credentials and portfolios to secure positions, allowing them to compromise sensitive systems or facilitate broader attacks.

- Newer Variant of BeaRAT Malware

Researchers have identified a new variant of the BeaverTail malware, attributed to North Korean-affiliated attackers, that targets macOS users by masquerading as a legitimate browser-based video call application. The sophisticated malware is designed to exfiltrate sensitive information, including cryptocurrency wallet data and keychain files, from infected machines. The new version of BeaverTail is embedded in a macOS disk image mimicking the legitimate MiroTalk video call service, which is browser-based and requires no app download.

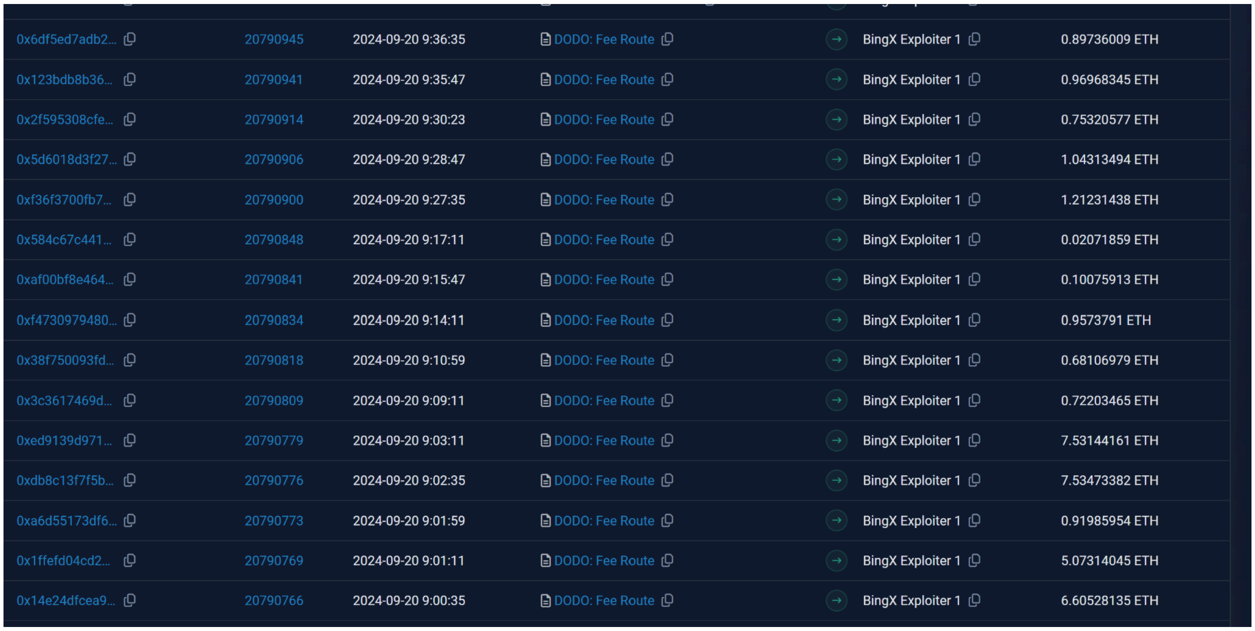
3.3.2 Methods of Laundering

While exploits on various blockchain networks have increased, Ethereum (ETH), Bitcoin (BTC), and TRON remain the primary networks for laundering stolen funds due to their high liquidity and extensive ecosystem support.

This subsection uses the BingX incident, tracked by SlowMist, as a case study. Our investigation highlights the basics of these methods without delving into advanced strategies for privacy reasons.

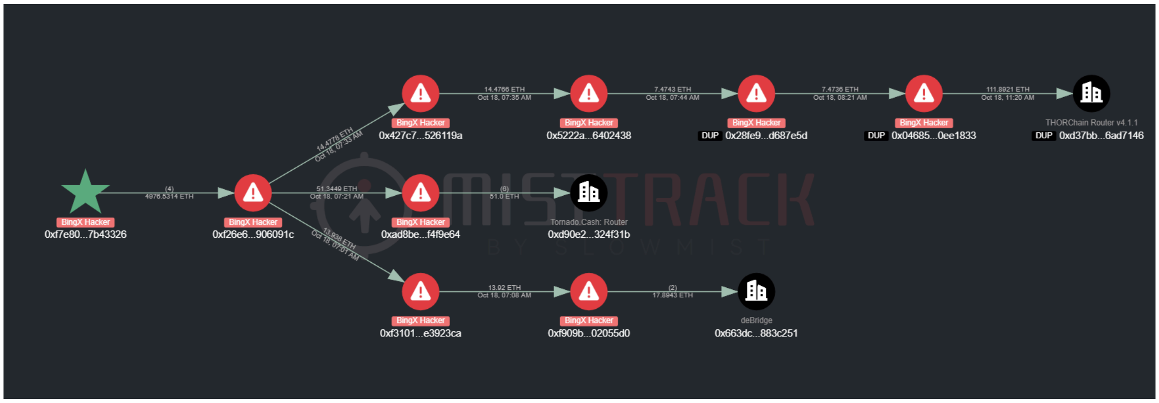
Path of Stolen Funds in the BingX Incident:

(1) Initial Conversion: The stolen funds were first transferred into a wallet controlled by the perpetrators, where they were converted from altcoins into Ethereum (ETH).

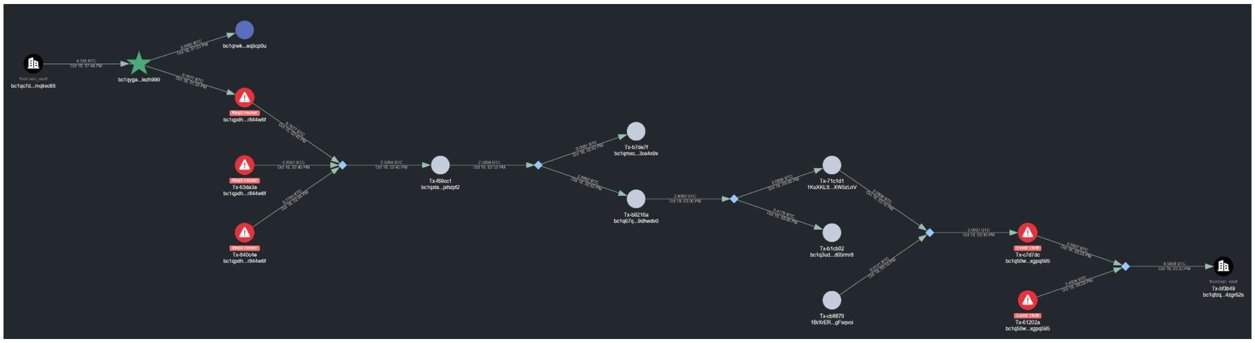


0x6df5ed7adb2...	20790945	2024-09-20 9:36:35	DODO: Fee Route	→	BingX Exploiter 1	0.89736009 ETH
0x123bdb8b36...	20790941	2024-09-20 9:35:47	DODO: Fee Route	→	BingX Exploiter 1	0.96968345 ETH
0x2f595308cfe...	20790914	2024-09-20 9:30:23	DODO: Fee Route	→	BingX Exploiter 1	0.75320577 ETH
0x5d6018d3f27...	20790906	2024-09-20 9:28:47	DODO: Fee Route	→	BingX Exploiter 1	1.04313494 ETH
0xf36f3700fb7...	20790900	2024-09-20 9:27:35	DODO: Fee Route	→	BingX Exploiter 1	1.21231438 ETH
0x584c67c441...	20790848	2024-09-20 9:17:11	DODO: Fee Route	→	BingX Exploiter 1	0.02071859 ETH
0xaf00bf8e464...	20790841	2024-09-20 9:15:47	DODO: Fee Route	→	BingX Exploiter 1	0.10075913 ETH
0xf4730979480...	20790834	2024-09-20 9:14:11	DODO: Fee Route	→	BingX Exploiter 1	0.9573791 ETH
0x38f750093fd...	20790818	2024-09-20 9:10:59	DODO: Fee Route	→	BingX Exploiter 1	0.68106979 ETH
0x3c3617469d...	20790809	2024-09-20 9:09:11	DODO: Fee Route	→	BingX Exploiter 1	0.72203465 ETH
0xed9139d971...	20790779	2024-09-20 9:03:11	DODO: Fee Route	→	BingX Exploiter 1	7.53144161 ETH
0xdb8c13f7f5b...	20790776	2024-09-20 9:02:35	DODO: Fee Route	→	BingX Exploiter 1	7.53473382 ETH
0xa6d55173df6...	20790773	2024-09-20 9:01:59	DODO: Fee Route	→	BingX Exploiter 1	0.91985954 ETH
0x1ffefd04cd2...	20790769	2024-09-20 9:01:11	DODO: Fee Route	→	BingX Exploiter 1	5.07314045 ETH
0x14e24dfcea9...	20790766	2024-09-20 9:00:35	DODO: Fee Route	→	BingX Exploiter 1	6.60528135 ETH

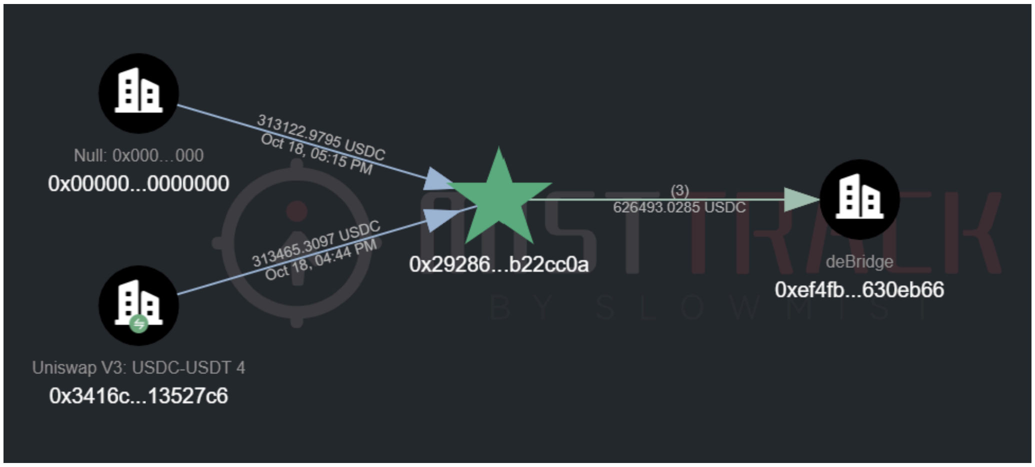
(2) Splitting and Deposits: The ETH was split across multiple wallet addresses and deposited into platforms such as Tornado Cash, Thorchain, and Debridge.



(3) After withdrawal on the Bitcoin network, the funds were fragmented and moved through several addresses before being consolidated again and bridged back to the Ethereum network as USDT.



(4) In this scenario the funds were bridge to the Solana network via Debrige as USDT but then it was swapped for USDC and then deposited into Debridge and withdrawn on the Solana network.



It's important to note that the Solana withdrawal was not the end of the investigation. This process of bridging and fragmenting funds repeated several more times before the funds were ultimately deposited into exchanges or moved to over-the-counter (OTC) markets on the TRON network.

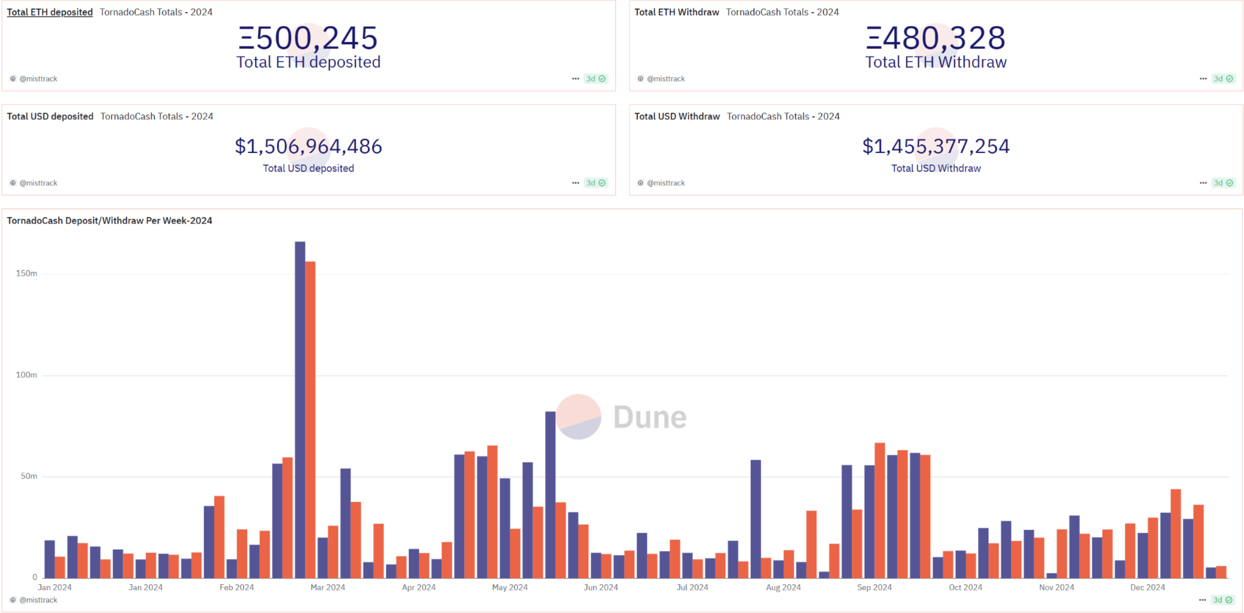
You might wonder why the attackers bridge funds across multiple networks. The primary reason is to test the anti-money laundering (AML) systems of various exchanges. While most exchanges enforce Know Your Transaction (KYT) protocols, automated systems can only handle so much. Complex laundering patterns, involving multiple hops and network bridges, often require manual intervention by services like ours to alert exchanges effectively. Mixers, in particular, add another layer of complexity. Demixing stolen funds often requires significant manual effort, and the difficulty increases with the volume of funds involved. The more hops and networks used, the harder it becomes to trace and block the stolen assets. This underscores the need for advanced tools and expertise to combat these evolving laundering techniques.

While OTC markets may appear to be a convenient option for trading cryptocurrency, they come with significant risks. Most OTC markets do not thoroughly vet for stolen funds, and users who engage with these markets could inadvertently find themselves in possession of illicit assets. In such cases, funds are often frozen or seized, leaving users as victims.

The BingX case demonstrates the increasing complexity of cryptocurrency investigations. From the moment the stolen funds landed in the hacker's wallet, they were swapped multiple times, moving from Altcoin to ETH, then to BTC, followed by USDT (on Ethereum), USDC (on Ethereum), and finally USDC (on Solana). Along the way, the funds passed through more than 12 different wallet addresses and were bridged across four blockchain networks. This intricate path represents only one branch of the investigation, which remains ongoing. As more users and companies adopt cryptocurrency, the frequency and complexity of such cases are expected to grow. This highlights the critical need for strong preventive measures, such as advanced anti-money laundering systems and proactive monitoring, to mitigate these challenges effectively.

3.4 Money Laundering Tools

3.4.1 Tornado Cash


Total ETH deposited TornadoCash Totals - 2024

Ξ500,245
Total ETH deposited

Total ETH Withdraw TornadoCash Totals - 2024

Ξ480,328
Total ETH Withdraw

Total USD deposited TornadoCash Totals - 2024

$1,506,964,486
Total USD deposited

Total USD Withdraw TornadoCash Totals - 2024

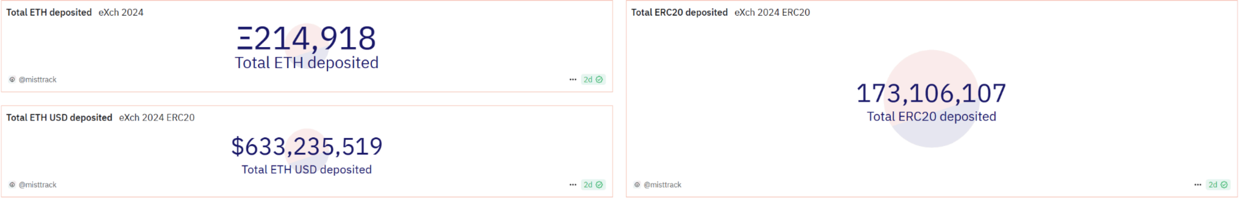
$1,455,377,254
Total USD Withdraw

TornadoCash Deposit/Withdraw Per Week-2024

(https://dune.com/misttrack/2024)

In 2024, users deposited a total of 500,245 ETH (approximately $1.506 billion) into Tornado.Cash, a year-on-year increase of 47%. A total of 480,328 ETH (approximately $1.455 billion) was withdrawn from Tornado.Cash, a year-on-year increase of 53%.

3.4.2 eXch


Total ETH deposited eXch 2024

Ξ214,918
Total ETH deposited

Total ETH USD deposited eXch 2024 ERC20

$633,235,519
Total ETH USD deposited

Total ERC20 deposited eXch 2024 ERC20

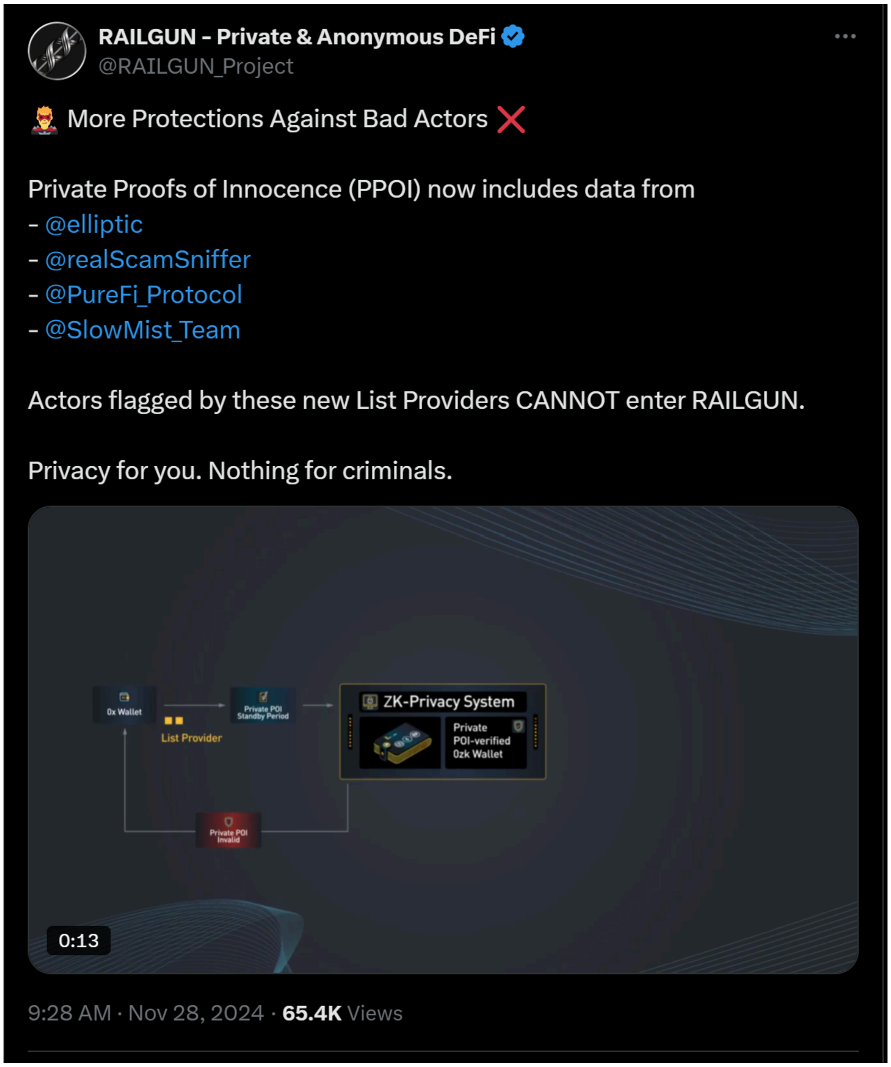
173,106,107
Total ERC20 deposited

(https://dune.com/misttrack/2024)

In 2024, users deposited a total of 214,918 ETH (approximately $633 million) into eXch, a year-on-year increase of 355%; a total of 173,106,107 ERC20s into eXch, a year-on-year increase of 579%.

The increase in eXch activity in 2024 is largely due to its growing use by malicious actors, including DPRK-affiliated entities. Unlike Tornado Cash, which can often be demixed for larger transactions, eXch is known for its lack of cooperation with law enforcement. This makes it a more attractive option for illicit activities, as it offers greater anonymity and less risk of asset recovery. These factors have positioned eXch as a preferred platform for bad actors, driving the significant growth in both ETH and ERC20 token deposits.

3.4.3 Railgun



RAILGUN - Private & Anonymous DeFi
@RAILGUN_Project

More Protections Against Bad Actors ❌

Private Proofs of Innocence (PPOI) now includes data from
- @elliptic
- @realScamSniffer
- @PureFi_Protocol
- @SlowMist_Team

Actors flagged by these new List Providers CANNOT enter RAILGUN.

Privacy for you. Nothing for criminals.

9:28 AM · Nov 28, 2024 · **65.4K** Views

(https://x.com/RAILGUN_Project/status/1862141642989539397)

Railgun has implemented Private Proofs of Innocence (PPOI), leveraging zero-knowledge proofs to ensure users can verify their funds are not linked to illicit activities without compromising privacy. This innovation strikes a crucial balance between privacy and compliance, making it harder for malicious actors to exploit the platform for laundering funds.

IV. Conclusion

In 2024, the blockchain industry continued to ride the wave of innovation and transformation, presenting both new opportunities and challenges. The numerous security incidents and anti-money laundering (AML) developments of the year serve as stark reminders of the importance of industry standards and robust technological safeguards. By analyzing blockchain security incidents and money laundering cases from 2024, we aim to raise awareness of the critical need for enhanced security across the ecosystem.

Looking ahead, as regulatory frameworks become more comprehensive and technological capabilities advance, there is every reason to believe the blockchain industry will progress toward greater safety, transparency, and compliance. We hope this report provides valuable insights, offering readers a clearer understanding of the current state of blockchain security and AML practices. Together, we can contribute to building a more secure, stable, and trustworthy blockchain ecosystem.

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 ScamSniffer

ScamSniffer is a security platform focused on Web3 anti-scam, providing real-time anti-scam protection by combining off-chain and on-chain monitoring data.

Our browser security extension helps users identify phishing websites and suspicious transactions, providing comprehensive protection for Web3 users.

Our security solutions have been adopted by wallets including Binance, Bybit, OneKey, Phantom, TokenPocket, and others, protecting millions of Web3 users monthly from phishing and fraud threats.

We are committed to building a safer Web3 ecosystem for the next billion users.

Website

https://www.scamsniffer.io/

X

https://x.com/realScamSniffer

Blog

https://drops.scamsniffer.io/

Email

b2b@scamsniffer.io

VII. About SlowMist

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

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

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

SlowMist Security Solutions

Security Services

Exchange Security Audits

For all types of exchanges, beyond the traditional network attack and defense of private key architecture security, business logic security and other comprehensive gray box security audit.

Wallet Security Audits

For all types of wallets, beyond the traditional network attack and defense of private key architecture security, business logic security and other comprehensive gray box security audit.

Blockchain Security Audits

For blockchain node configuration, node communication, consensus algorithm, contract virtual machine and other key modules, and solve the core security issues of the blockchain.

Smart Contract Audits

A comprehensive white-box security audit for source code for tokens, DApp contracts, etc.

Consortium Blockchain Security Solutions

The consortium blockchain full-cycle security construction solution proposed by SlowMist Technology is committed to improving the security and controllability of enterprises to the currently immature blockchain technology system, allowing the blockchain security system to be multi-leveled and standardized, thereby protecting the area blockchain applications can be implemented quickly and securely.

Red Teaming

Red Teaming will not be limited to traditional penetration testing and will focus more on attack assessments for real vulnerabilities such as enterprise personnel, enterprise business systems, enterprise supply chains, enterprise office systems, and enterprise physical security.

Security Monitoring

A dynamic security monitoring system that covers all possible vulnerabilities, and it continues to provide comprehensive security service.

Blockchain Threat Intelligence

By integrating threat intelligence, and the power of community partners, to build a joint defense system which integrated management under the chain.

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

Hacking time, hacking for fun, hacking for all.

Digital Asset Security Solution

Open source digital asset security solutions.

Security Products

SlowMist AML

Block risky cryptocurrencies and avoid risks.

MistTrack

A crypto tracking and compliance platform for everyone.

SlowMist Hack

Full summary of blockchain attack events.

False Top-up Vulnerability Scanner

A security weapon that allows the exchange to safely deposit and withdraw.

Website

https://slowmist.com

X

https://twitter.com/SlowMist_Team

Github

https://github.com/slowmist

Medium

https://slowmist.medium.com

Email

team@slowmist.com

Wechat

SLOWMIST

Focusing on Blockchain Ecosystem Security