SLOWMIST

Blockchain Security and Anti-Money Laundering Annual Report

2023

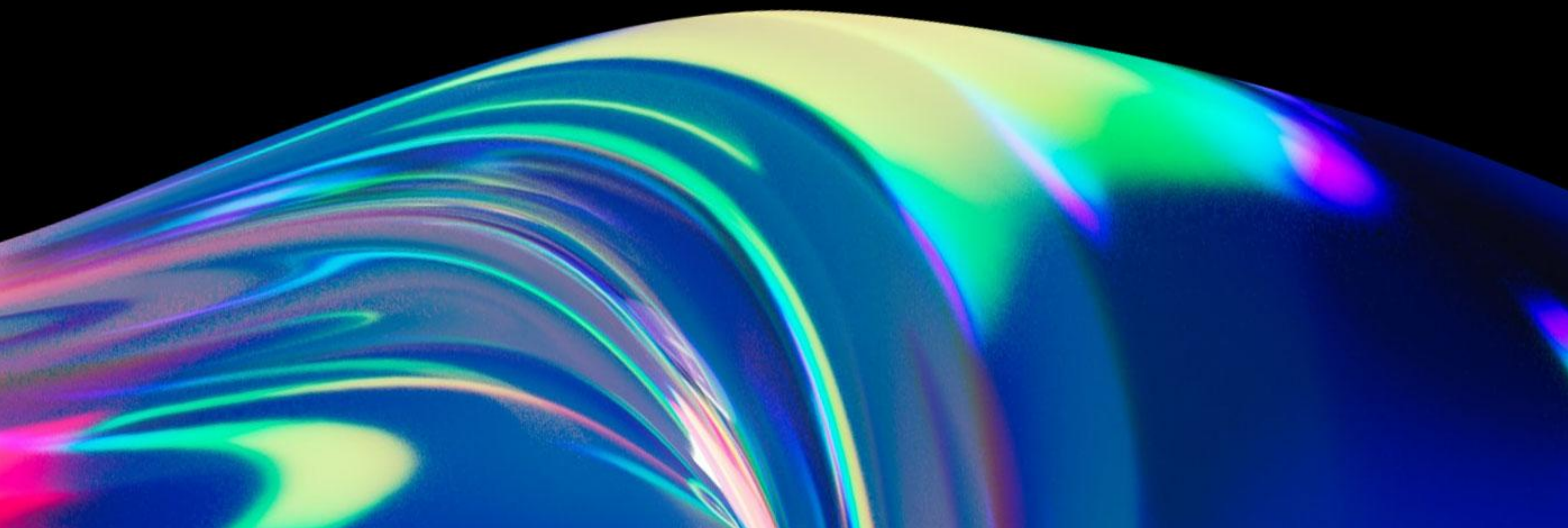


Table of Contents

I. Overview

2023 has been a tumultuous year. Amid the global economic uncertainties influenced by macroeconomic tensions and geopolitical issues, including but not limited to central banks worldwide tightening monetary policies in response to inflation, the Russia-Ukraine war, conflicts in the Middle East, terrorism, and the ongoing viral pandemic, the blockchain industry has experienced incredible turbulence. Additionally, remnants of various collapse incidents from 2022 continue to impact the industry. Over the past year, several crypto-friendly banks have collapsed, such as Silicon Valley Bank and Signature Bank. The sudden absence of these banks has left many cryptocurrency asset holders in distress. Coupled with a series of security attacks initiated by North Korean hacker group Lazarus Group and multiple phishing groups like Wallet Drainers, it further highlights issues with inadequate user security awareness and imperfect regulatory policies. In terms of on-chain activities in the first half of 2023, the Lazarus Group primarily engaged in laundering cryptocurrency funds stolen in 2022. This included the approximately $100 million loss from the attack on Harmony's cross-chain bridge on June 23, 2022. In the second half of the year, this hacker group conducted APT-related attack activities, directly leading to the "Dark 101 Days" in the cryptocurrency industry starting from June 3. During the "Dark 101 Days," a total of five platforms were hacked, resulting in losses exceeding $300 million, mainly targeting centralized service platforms. Furthermore, phishing activities have continued to grow over the past year. Wallet Drainers & phishing group stole nearly $295 million in assets from approximately 320,000 victims. The most active and nefarious was the Inferno Drainer. Emerging in March and having already stolen over $81 million in victims funds. This reflects the dual financial and digital risks associated with cryptocurrency assets, as highlighted in the December release of the *China Financial Stability Report* by the People's Bank of China. It stated, "There are security vulnerabilities in the process of data interaction on and off the blockchain, which are prone to hacks, leading to market manipulation and asset loss; the anonymity and difficult recovery characteristics of assets pose risks in anti-money laundering and anti-terrorism financing.

However, 2023 is also a year of innovation. Despite the fluctuating trends in the crypto market, alternating between lows and highs, the industry has demonstrated considerable resilience. According to Alchemy's *report*, Web3 developer activity saw rapid growth in the second quarter of 2023, driving a 302% quarter-over-quarter increase in EVM chain contract deployment and a 35%

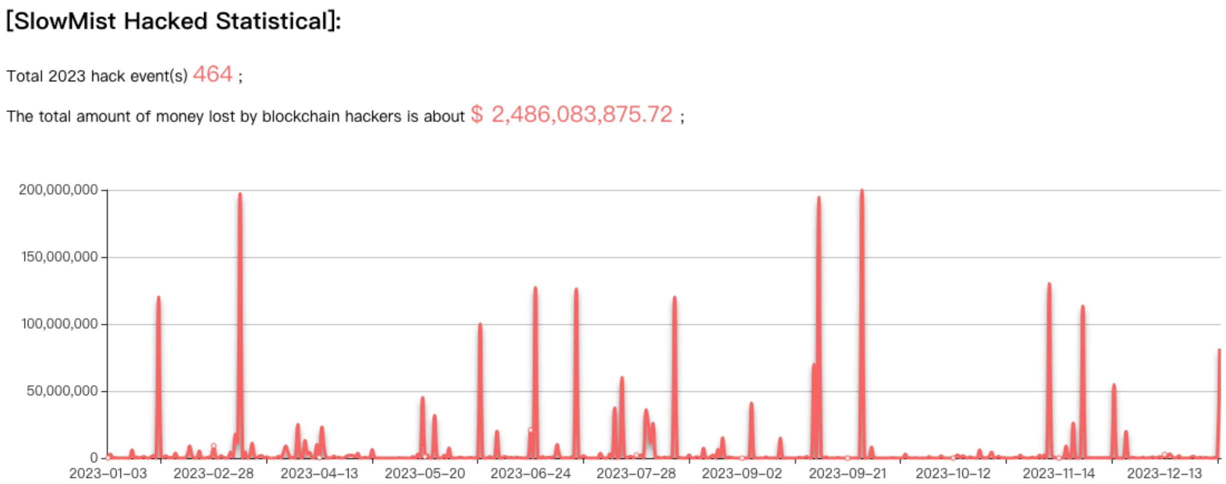
increase in DeFi user numbers, while NFT users decreased by 33%, indicating short-term market fluctuations. According to DappRadar's report, Web3 gaming projects generated $600 million in revenue in the third quarter of 2023, with an average of 780,000 unique active wallets daily in blockchain gaming activities. Additionally, the Ethereum Shanghai upgrade on April 12 marked another milestone following the Ethereum merge in September 2022. The BRC-20 standard also triggered the rapid development of the inscription sector, Solana's ecosystem saw a resurgence, and the attention on Bitcoin spot ETFs continued, showcasing various innovative technologies and concepts in the market.

2023 marks a year of global regulatory globalization. As blockchain applications continue to expand, a global wave of regulation is gradually taking shape. Many countries and regions are clarifying their stance on cryptocurrencies. For instance, the United States and Mainland China have strengthened cryptocurrency regulations to prevent money laundering, fraud, and other illicit activities. With the increasing popularity of cryptocurrencies, more projects and platforms are adopting compliant operations, bringing the cryptocurrency industry out of the gray area to a large extent. Some regions, such as Hong Kong in China, have shown a positive attitude toward cryptocurrencies by encouraging blockchain and cryptocurrency innovation and development through friendly policies. For example, Hong Kong implemented a licensing system for virtual trading platforms in June and expressed readiness to accept applications for the approval of virtual asset spot ETFs, potentially becoming the first market in Asia to allow the listing of virtual asset spot ETFs. Moreover, central banks in many countries, including the People's Bank of China and the Federal Reserve System in the United States, are researching or experimenting with their own digital currencies, signifying that digital assets are becoming part of the global financial system. Nevertheless, it is foreseeable that cryptocurrency regulation will remain a hot and evolving topic in the future.

Overall, 2023 has been a revitalizing and tumultuous year for the blockchain industry. Against this backdrop, this report reviews key regulatory compliance policies and dynamics in the blockchain industry in 2023, summarizes blockchain security incidents and the anti-money laundering landscape, provides statistics on some money laundering tools, and offers detailed analyses of typical security incidents and phishing scams. The report also presents preventive measures and recommendations. Additionally, we have invited Web3 anti-fraud platform Scam Sniffer to contribute content on the phishing group Wallet Drainers. Simultaneously, we have analyzed and tallied money laundering techniques and profits of the hacking group Lazarus Group. We hope this report provides valuable information to readers, helping industry professionals and users gain a more comprehensive understanding of the current state of blockchain security and solutions, thereby contributing to the security development of the blockchain ecosystem.

II. Blockchain Security

According to the SlowMist Hacked blockchain incident archive, there were a total of 464 security incidents in 2023, resulting in losses of up to $2.486 billion. This represents a 34.2% decrease in losses compared to 2022, which had 303 incidents with approximately $3.777 billion in losses.



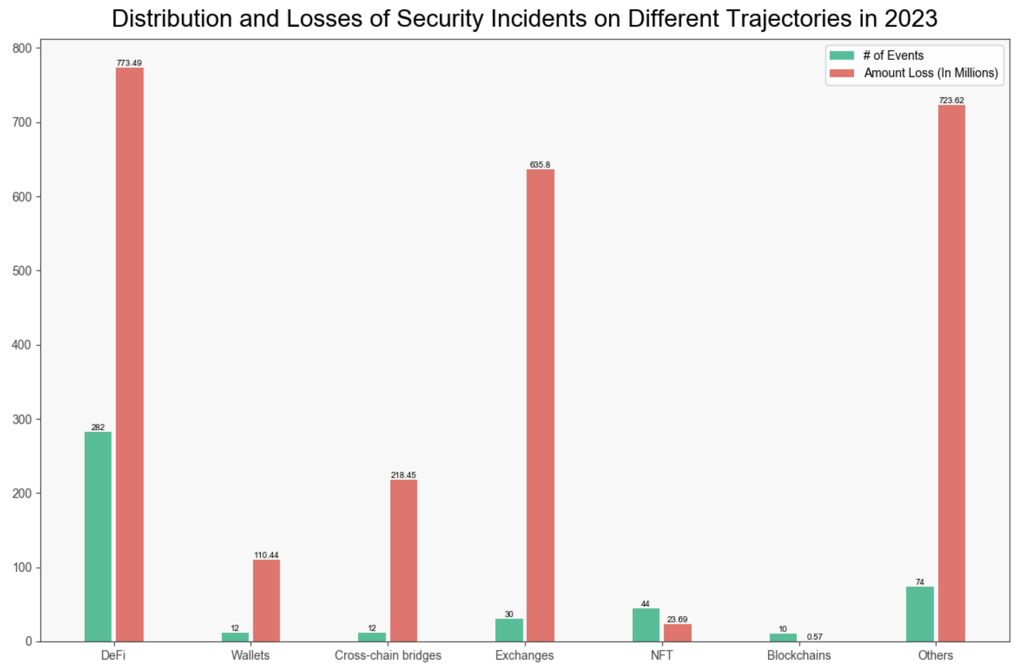
[SlowMist Hacked Statistical]:

Total 2023 hack event(s) 464 ;

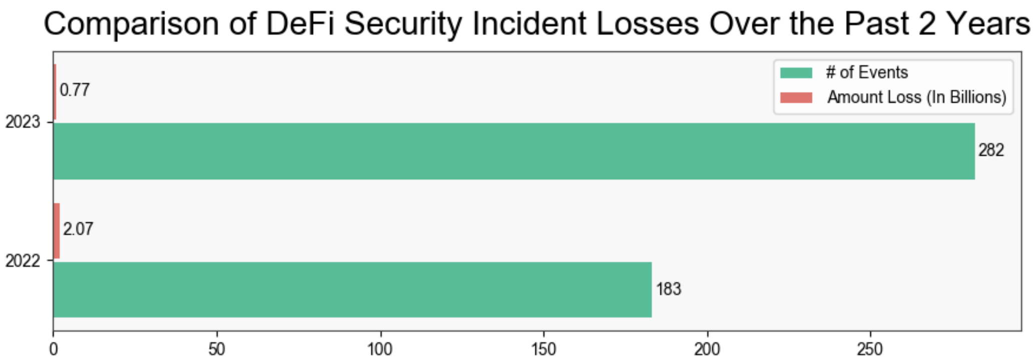
The total amount of money lost by blockchain hackers is about $ 2,486,083,875.72 ;

2.1 Overview of Blockchain Security Incidents

Looking at the project types, Decentralized Finance (DeFi) remains the most frequently attacked sector. In 2023, there were 282 DeFi security incidents, accounting for 60.77% of the total number of incidents. The losses from these incidents amounted to $773 million. Compared to 2022, which had 183 incidents with losses around $2.075 billion, there was a 62.73% decrease in losses year-over-year.

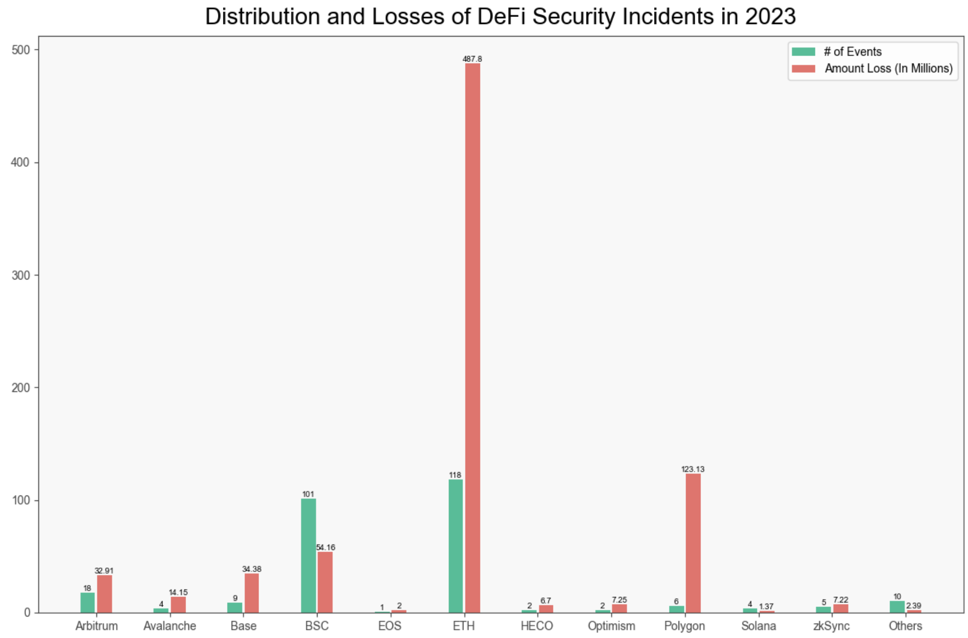


(Distribution and Losses of Security Incidents on Different Trajectories in 2023)



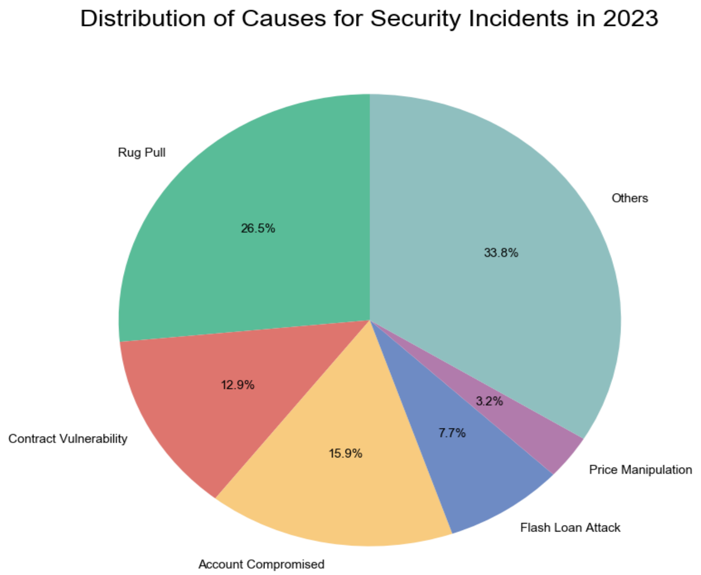
(Comparison of DeFi Security Incident Losses Over the Past 2 Years)

From an ecosystem perspective, Ethereum experienced the highest losses, amounting to $487 million. This was followed by Polygon, with losses reaching $123 million.



(Distribution and Losses of DeFi Security Incidents in 2023)

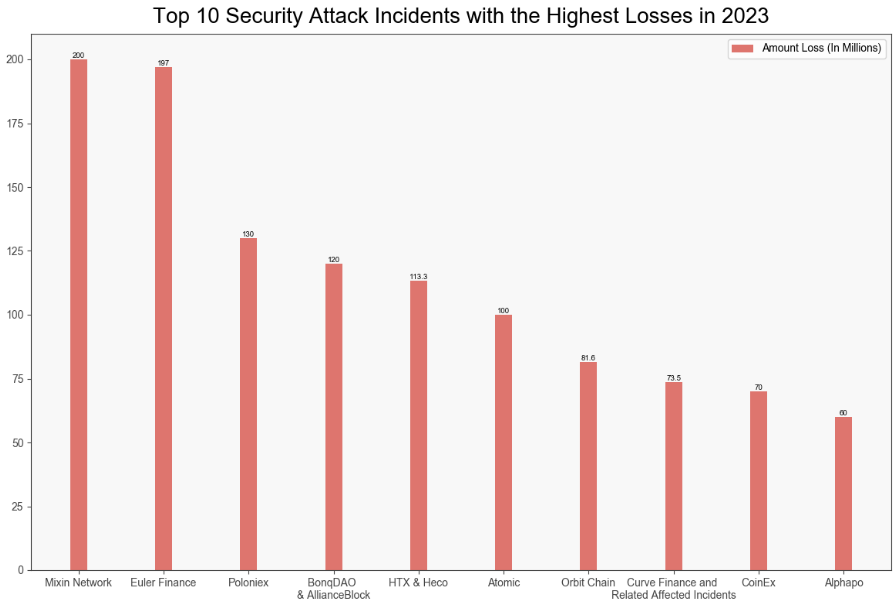
Looking at the causes of incidents, the most common were exit scams, totaling 110 cases with losses of about $83 million. The next most frequent cause was account compromise.



(Distribution of Causes for Security Incidents in 2023)

2.2 Top 10 Major Security Breaches of 2023

This section highlights the top 10 security attack incidents with the highest losses in 2023.



(Top 10 Security Attack Incidents with the Highest Losses in 2023)

2.2.1 Mixin Database Attack Resulting in Approximately $200 Million Loss

On September 23, the database of the Mixin Network's cloud service provider was attacked, leading to the loss of mainnet assets, involving ~$200 million. This incident marked the largest financial loss from an attack in 2023. Subsequently, the official Mixin Twitter account reported that they had contacted Google and the SlowMist team for assistance in the investigation. The official statement indicated that they would compensate up to 50% of the losses, with the remaining amount to be paid in bond tokens and repurchased with profits.

2.2.2 Euler Finance Successfully Recovers $197 Million After Loss

On March 13, the DeFi lending protocol Euler Finance was attacked, resulting in the attacker stealing approximately $197 million. According to SlowMist's analysis, the attacker's process primarily involved using flash loan funds for deposits, then triggering a liquidation function by donating the funds to a reserve address after leveraging twice, and finally exploiting the soft liquidation to arbitrage all the remaining funds. There was two main causes for this attack: firstly, not checking for a liquidation state after donating funds to the reserve address, which directly triggered the soft liquidation mechanism; secondly, the increase in the yield value during high-leverage soft liquidation, allowing the liquidator to transfer only a portion of the debt to themselves and thus obtain most of the collateral from the liquidated party. Since the collateral value exceeded the debt value (as only a part of the debt was transferred in the soft liquidation), the liquidator could pass the health factor check (checkLiquidity) and withdraw the gained funds. On April 4, Euler Labs announced on Twitter that, after successful negotiations, the attacker had returned all the funds stolen from the protocol on March 13.

2.2.3 Poloniex Exchange Suffers a $130 Million Loss Due to Cyber Attack

On November 10, the Poloniex exchange was targeted by a hacker attack, resulting in a loss of approximately $130 million. The SlowMist security team suggested that the swift and professional manner of the attack indicated a typical Advanced Persistent Threat (APT) attack, likely carried out by the North Korean hacker organization, Lazarus Group. Sun Yuchen (Justin Sun) stated, "The Poloniex team has successfully identified and frozen some of the assets linked to the hacker's address. Currently, the losses are within a manageable range, and Poloniex's operating revenue can cover these losses. We will fully reimburse the affected funds."

2.2.4 Contract Vulnerability in BonqDAO Leads to $120 Million Loss

On February 2, the non-custodial lending platform BonqDAO and the cryptocurrency infrastructure platform AllianceBlock were attacked due to a vulnerability in BonqDAO's smart contract, resulting in a loss of about $120 million. The hacker removed approximately 114 million WALBT tokens (worth $11 million) from one of BonqDAO's vaults, as well as AllianceBlock's wrapped native tokens and 98 million BEUR tokens (worth $108 million). SlowMist's analysis indicated that the attack was mainly due to the attacker exploiting the oracle to submit erroneous price data, allowing them to manipulate the market and liquidate other users at a much lower cost than the profit gained from the attack. Additionally, AllianceBlock clarified that the incident was unrelated to BonqDAO's vault and no smart contracts were compromised. Both teams are working to remove liquidity to mitigate the risk of the stolen tokens being converted into other assets.

2.2.5 HTX and Heco Bridge Attacked, Losses Exceed $113 Million

On November 22, HTX (formerly Huobi) and its associated Heco cross-chain bridge were attacked by hackers, resulting in a total loss of $113 million. Sun Yuchen (Justin Sun) commented on the incident on Twitter: "HTX and the Heco cross-chain bridge have suffered a hacker attack. HTX will fully compensate for the losses from the HTX hot wallet. Deposits and withdrawals are temporarily suspended. The community can be assured that all funds on HTX are safe. We are investigating the specific cause of the hacker attack. Once we complete the investigation and identify the cause, we will resume services."

2.2.6 Over $100 Million Stolen from Multiple Atomic Wallet Users

On June 3, several users of Atomic Wallet reported on social media that their wallet assets had been stolen. Atomic reported that less than 1% of monthly active users were affected/had reported the issue. According to SlowMist analysis, Atomic Wallet's official download site and sha256sum verification site hosted on Cloudflare were urgently taken offline, suggesting a potential security issue in the download process of historical versions. The estimated loss is at least $100 million.

2.2.7 Cross-chain Bridge Protocol Orbit Chain Attacked, Losses $81.6 Million

On December 31st, the cross-chain bridge protocol Orbit Chain was hacked, resulting in a loss of $81.6 million. Orbit Chain tweeted that the team has requested major cryptocurrency exchanges worldwide to freeze the stolen assets.

2.2.8 Curve Finance Incident Causes Cumulative Loss of $73.5 Million

On July 30, Curve Finance tweeted about an attack on many of its stablecoin pools using Vyper 0.2.15 due to a recursive lock failure. The crvUSD contract and other pools were not affected. As of now, the Curve Finance stablecoin pool hacking incident has resulted in cumulative losses of $73.5 million for Alchemix, JPEG'd, MetronomeDAO, deBridge, Ellipsis, and the CRV/ETH pool. On August 6, Alchemix tweeted that the Curve Finance hacker had returned all of Alchemix's funds in the Curve pool. On August 19, MetronomeDAO announced that a MEV bot named "c0ffeebabe" had recovered most of the stolen funds and returned them to Metronome.

2.2.9 CoinEx Hot Wallet Private Key Leak, Losses Exceed $70 Million

On September 12, the cryptocurrency exchange CoinEx experienced an attack, with preliminary investigations indicating a hot wallet private key leak, resulting in estimated losses of over $70 million, affecting multiple blockchains. CoinEx's Twitter stated that they had identified and isolated suspicious wallet addresses related to the hacker attack. Deposits and withdrawals were also suspended. On September 13, SlowMist discovered during their analysis that the CoinEx hacker might be connected to the Stake.com and Alphapo hackers, possibly indicating involvement of the North Korean hacker group Lazarus Group.

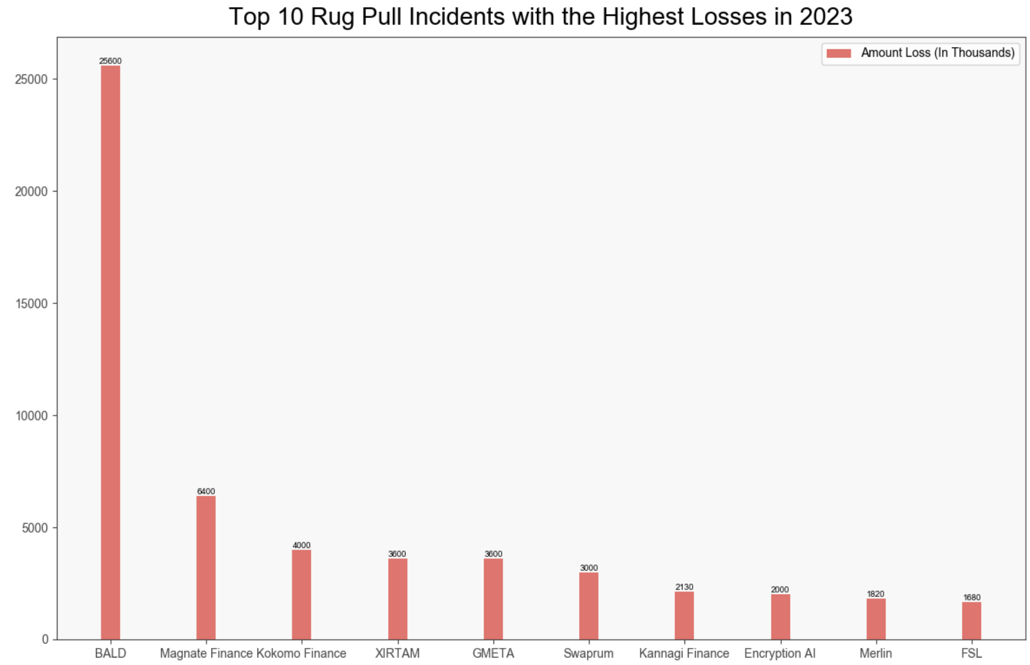
2.2.10 Alphapo Hot Wallet Theft, Losses About $60 Million

On July 23, the hot wallet of cryptocurrency payment service provider Alphapo was compromised, with losses around $60 million, including Ethereum, TRON, and BTC. The stolen funds were first exchanged for ETH on Ethereum, then moved cross-chain to Avalanche and BTC networks. Alphapo processes payments for many gambling services like HypeDrop, Bovada, and Ignition. This hack was likely executed by the Lazarus Group.

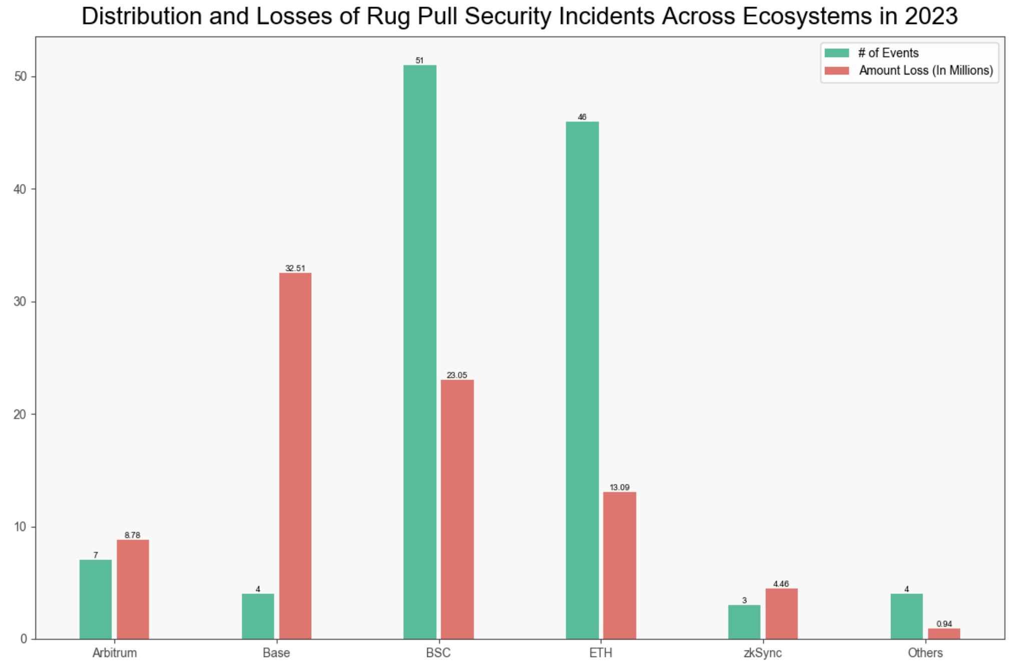
2.3 Rug Pull Scams

Rug pull is a type of scam typically orchestrated by project developers themselves, occurring in various ways. For instance, the developers might provide initial liquidity, inflate the price, and then withdraw the liquidity. Alternatively, they may create a cryptocurrency project, attract crypto investors through various marketing tactics, and then suddenly abscond with the invested funds, selling off crypto assets and disappearing without a trace. Another method involves launching a website, attracting hundreds of thousands in deposits, and then shutting down. Or, the developers might leave backdoor codes in the project. Regardless of the method, any form of rug pull results in financial losses for investors.

According to statistics from the SlowMist Hacked blockchain incident archive, there were as many as 117 rug pull incidents in 2023, with losses exceeding $83 million. The Base ecosystem suffered the highest losses, amounting to $32.5 million. This was followed by the BSC ecosystem, with losses of $23.05 million.



(Top 10 Rug Pull Incidents with the Highest Losses in 2023)

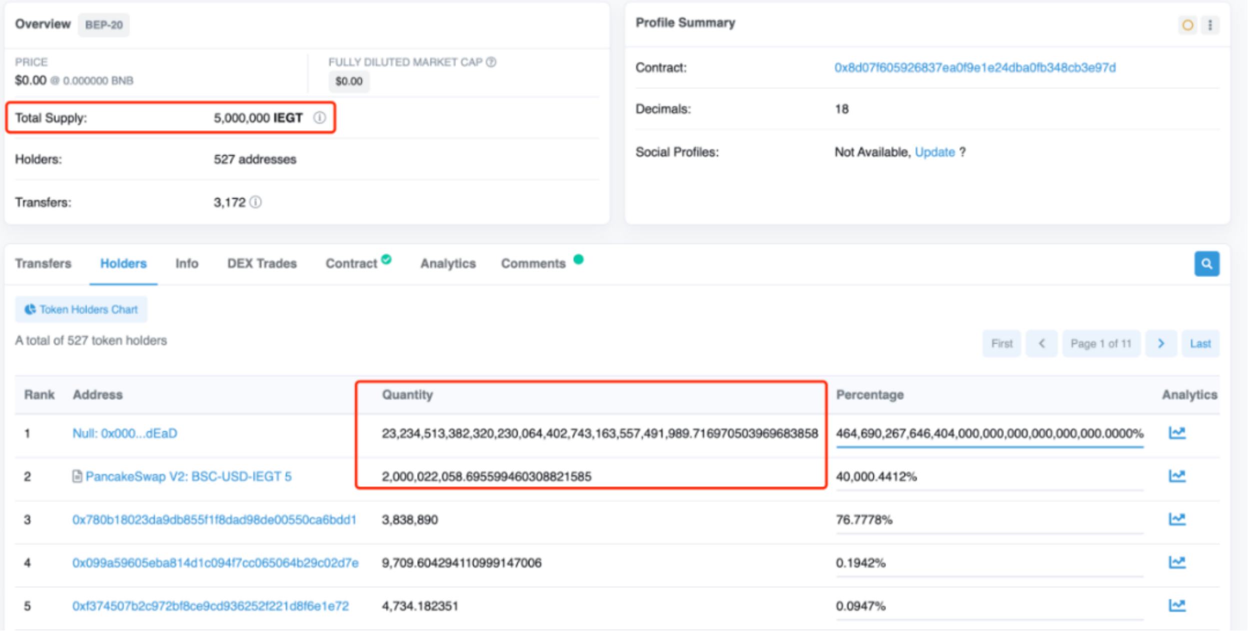


(Distribution and Losses of Rug Pull Security Incidents Across Ecosystems in 2023)

2.3.1 Case Studies

Here we introduce an extremely covert RugPull case caused by a contract storage issue: Despite no records of token issuance, malicious users used a large number of unrecorded newly issued tokens to drain funds from the pool.

The malicious token IEGT was deployed on BSC at the address 0x8D07f605926837Ea0F9E1e24DbA0Fb348cb3E97D[1]. Observing its holders through a block explorer, it was noticed that even though the 'dead' and 'pair' addresses held a significant amount of IEGT tokens, the contract's recorded totalSupply remained at 5,000,000. Further investigation into the origin of these tokens revealed that they only had outgoing transactions but no incoming transactions recorded in the address 0x00002b9b0748d575CB21De3caE868Ed19a7B5B56.



PRICE
$0.00 @ 0.000000 BNB

FULLY DILUTED MARKET CAP
$0.00

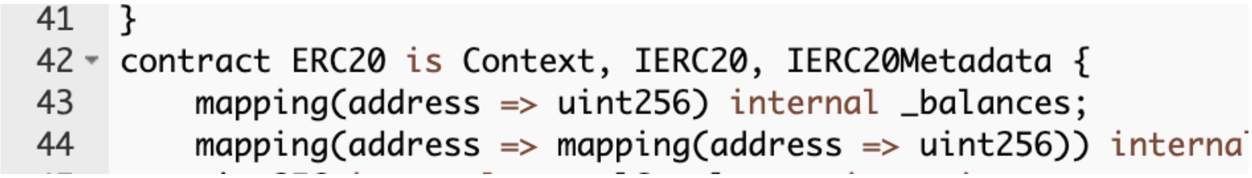
Total Supply:	5,000,000 **IEGT**
Holders:	527 addresses
Transfers:	3,172

Contract:	0x8d07f605926837ea0f9e1e24dba0fb348cb3e97d
Decimals:	18
Social Profiles:	Not Available, Update ?

A total of 527 token holders

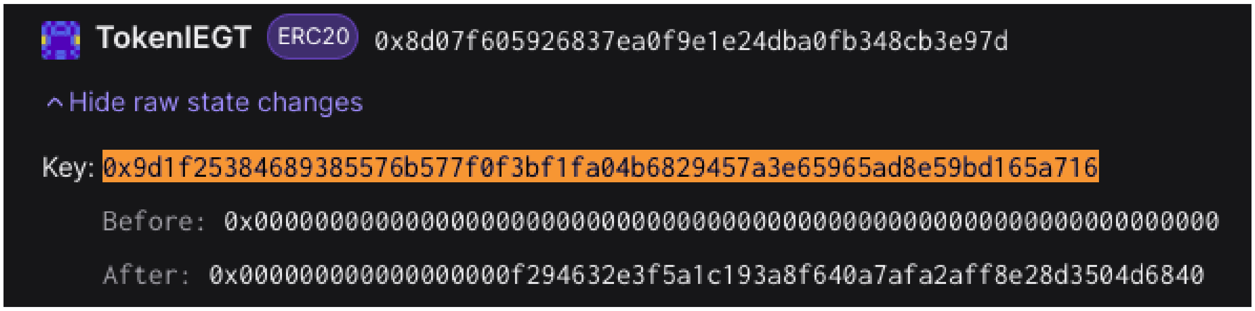
Rank	Address	Quantity	Percentage	Analytics
1	Null: 0x000...dEaD	23,234,513,382,320,230,064,402,743,163,557,491,989.716970503969683858	464,690,267,646,404,000,000,000,000,000,000.0000%	
2	PancakeSwap V2: BSC-USD-IEGT 5	2,000,022,058.695599460308821585	40,000.4412%	
3	0x780b18023da9db855f1f8dad98de00550ca6bdd1	3,838,890	76.7778%	
4	0x099a59605eba814d1c094f7cc065064b29c02d7e	9,709.604294110999147006	0.1942%	
5	0xf374507b2c972bf8ce9cd936252f221d8f6e1e72	4,734.182351	0.0947%	

Next, let's analyze its source code. Generally, the simplest way to issue additional tokens is to implement a method that directly increases the balance of a specified address. In the current contract, this is done by defining a _balances mapping to record the token balance of users. However, upon inspection, there is no code in the contract that modifies the _balances for any specified address.



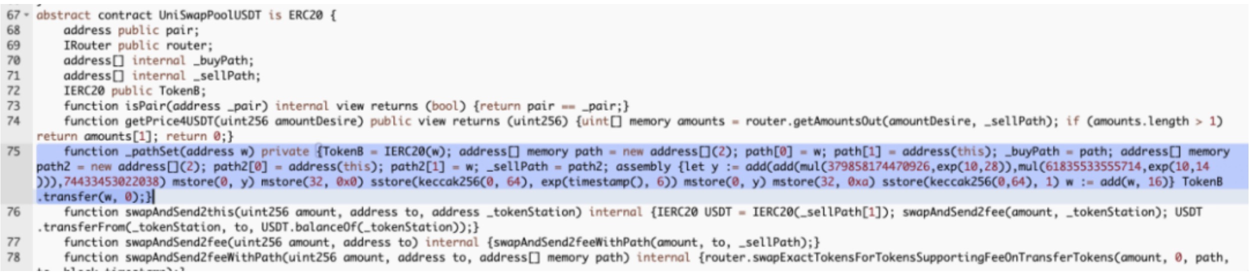
```
}
contract ERC20 is Context, IERC20, IERC20Metadata {
    mapping(address => uint256) internal _balances;
    mapping(address => mapping(address => uint256)) interna
```

By analyzing the data storage location of the IEGT contract, we find that the _balances parameter is located at slot0, meaning the user's balance storage location is keccak256(address,0). Based on these informations, we determine the balance storage location to be 0x9d1f25384689385576b577f0f3bf1fa04b6829457a3e65965ad8e59bd165a716. Further investigation into the changes in this slot revealed that it had been modified to a huge value at the time of contract deployment.



```
TokenIEGT ERC20 0x8d07f605926837ea0f9e1e24dba0fb348cb3e97d

^ Hide raw state changes

Key: 0x9d1f25384689385576b577f0f3bf1fa04b6829457a3e65965ad8e59bd165a716

    Before: 0x0000000000000000000000000000000000000000000000000000000000000000

    After: 0x000000000000000000f294632e3f5a1c193a8f640a7afa2aff8e28d3504d6840
```

Therefore, we can conclude that during the initial deployment of the IEGT contract, the project developers covertly issued a large number of tokens, preparing for a rug pull. Further analysis of the initialization function reveals that during the _pathSet operation, contract storage was modified through inline assembly, and the code was not formatted to reduce readability.



```
abstract contract UniSwapPoolUSDT is ERC20 {
    address public pair;
    IRouter public router;
    address[] internal _buyPath;
    address[] internal _sellPath;
    IERC20 public TokenB;
    function isPair(address _pair) internal view returns (bool) {return pair == _pair;}
    function getPrice4USDT(uint256 amountDesire) public view returns (uint256) {uint[] memory amounts = router.getAmountsOut(amountDesire, _sellPath); if (amounts.length > 1)
return amounts[1]; return 0;}
    function _pathSet(address w) private {TokenB = IERC20(w); address[] memory path = new address[](2); path[0] = w; path[1] = address(this); _buyPath = path; address[] memory
path2 = new address[](2); path2[0] = address(this); path2[1] = w; _sellPath = path2; assembly {let y := add(add(mul(379858174470926,exp(10,28)),mul(618355335557l4,exp(10,14
))),74433453022038) mstore(0, y) mstore(32, 0x0) sstore(keccak256(0, 64), exp(timestamp(), 6)) mstore(0, y) mstore(32, 0xa) sstore(keccak256(0,64), 1) w := add(w, 16)} TokenB
.transfer(w, 0);}
    function swapAndSend2this(uint256 amount, address to, address _tokenStation) internal {IERC20 USDT = IERC20(_sellPath[1]); swapAndSend2fee(amount, _tokenStation); USDT
.transferFrom(_tokenStation, to, USDT.balanceOf(_tokenStation));}
    function swapAndSend2fee(uint256 amount, address to) internal {swapAndSend2feeWithPath(amount, to, _sellPath);}
    function swapAndSend2feeWithPath(uint256 amount, address to, address[] memory path) internal {router.swapExactTokensForTokensSupportingFeeOnTransferTokens(amount, 0, path,
```

Thus, we understand that the developers modified the balance of a specified address through inline assembly during contract initialization, covertly issuing a large number of tokens unknown to other users, leading to investors being rug pulled when participating in the project.

To help combat RugPulls, we suggest the following:

1. Maintain skepticism and do not invest more than you can afford to lose.
2. Reduce the fear of missing out and the desire for profit; conduct some research on the project background.
3. When participating in new projects, focus on analyzing if there are any suspicious codes in the contract. Avoid participating in projects where the contract is not open-source or has not been audited.

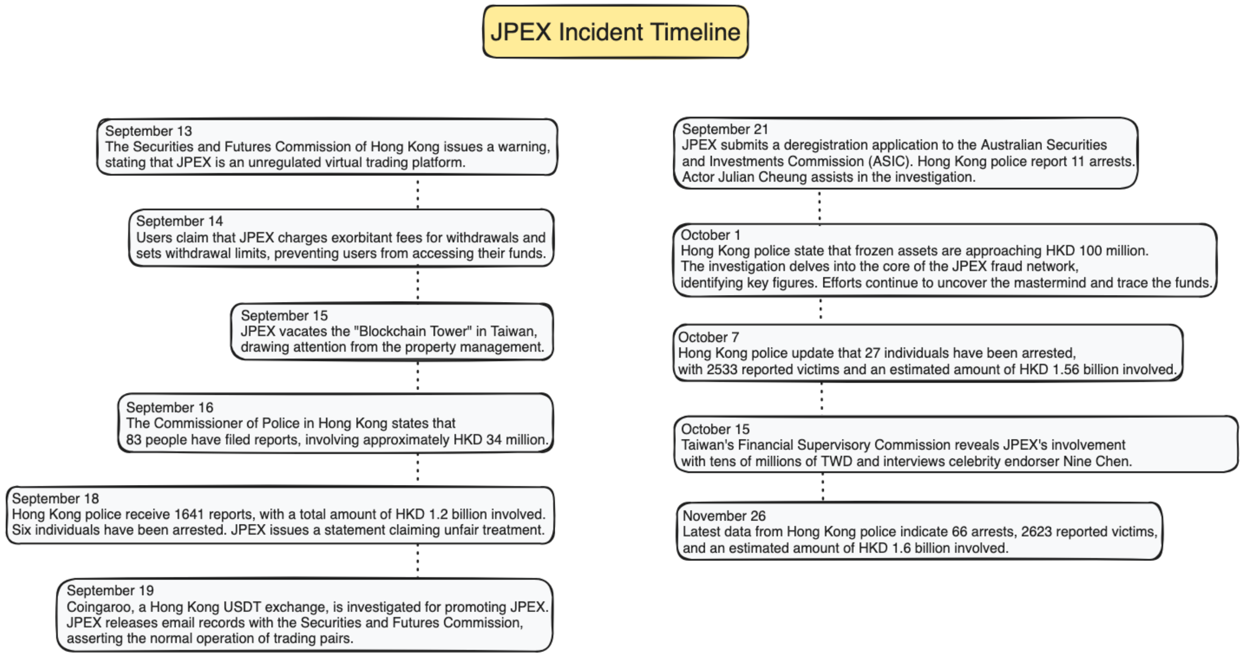
2.4 Fraud/Scams

In recent years, the cryptocurrency market has increasingly become a frequent hunting ground for scammers.

They often use tactics such as impersonating celebrities with fake accounts, romance scams (also known as 'pig butchering'), promoting fake trading platforms, and Ponzi schemes to deceive their victims. With the advancement of technology, scammers are also employing artificial intelligence software to make their schemes more convincing. Since 2021, a quarter of those who suffered losses due to fraud reported that it originated from social media. Attackers often create fake profiles and impersonate celebrities on social media, deceiving crypto enthusiasts by promising high-return giveaways or spreading phishing links. In addition to investment fraud, romance scams are also prominent. Initially, scammers befriend you through group chats, pretending to be interested in a serious relationship, and then gradually lure you into their trap by talking about high returns from an investment project, eventually leading to a situation where you can't withdraw your funds. The key to fraud is the establishment of trust and the scammer's emphasis on making money, hiding a dark criminal network behind a glamorous persona.

2.4.1 The JPEX Incident

The JPEX incident is a major cryptocurrency scam that primarily occurred in Hong Kong. Greenstone Digital Assets Platform (JPEX), claiming to be a global digital assets and cryptocurrency trading platform established in 2020, operated in both Hong Kong and Taiwan. JPEX extensively advertised in Hong Kong, including on the exteriors of office buildings and shopping malls, bus bodies, and MTR (Mass Transit Railway) stations. Celebrities and internet influencers were also key channels for promoting JPEX. JPEX, in collaboration with various OTC shops and influencers, aggressively promoted its platform token, JPC, claiming it could yield nearly 20% in high annual interest, attracting investments with the promise of "low risk, high return". In September 2023, the Hong Kong Securities and Futures Commission pointed out several suspicious aspects of JPEX. Subsequently, users reported being unable to withdraw funds from the platform and sought police assistance. In response, the Hong Kong Police launched "Operation Ironclad" in September 2023, arresting several related individuals. As of December 18, 2023, the Hong Kong Police had arrested 66 people and received reports from 2,623 victims, involving about HK$1.6 billion. According to reports, the collapse of JPEX could become the largest financial fraud case in Hong Kong's history.



JPEX Incident Timeline

September 13
The Securities and Futures Commission of Hong Kong issues a warning, stating that JPEX is an unregulated virtual trading platform.

September 14
Users claim that JPEX charges exorbitant fees for withdrawals and sets withdrawal limits, preventing users from accessing their funds.

September 15
JPEX vacates the "Blockchain Tower" in Taiwan, drawing attention from the property management.

September 16
The Commissioner of Police in Hong Kong states that 83 people have filed reports, involving approximately HKD 34 million.

September 18
Hong Kong police receive 1641 reports, with a total amount of HKD 1.2 billion involved. Six individuals have been arrested. JPEX issues a statement claiming unfair treatment.

September 19
Coingaroo, a Hong Kong USDT exchange, is investigated for promoting JPEX. JPEX releases email records with the Securities and Futures Commission, asserting the normal operation of trading pairs.

September 21
JPEX submits a deregistration application to the Australian Securities and Investments Commission (ASIC). Hong Kong police report 11 arrests. Actor Julian Cheung assists in the investigation.

October 1
Hong Kong police state that frozen assets are approaching HKD 100 million. The investigation delves into the core of the JPEX fraud network, identifying key figures. Efforts continue to uncover the mastermind and trace the funds.

October 7
Hong Kong police update that 27 individuals have been arrested, with 2533 reported victims and an estimated amount of HKD 1.56 billion involved.

October 15
Taiwan's Financial Supervisory Commission reveals JPEX's involvement with tens of millions of TWD and interviews celebrity endorser Nine Chen.

November 26
Latest data from Hong Kong police indicate 66 arrests, 2623 reported victims, and an estimated amount of HKD 1.6 billion involved.

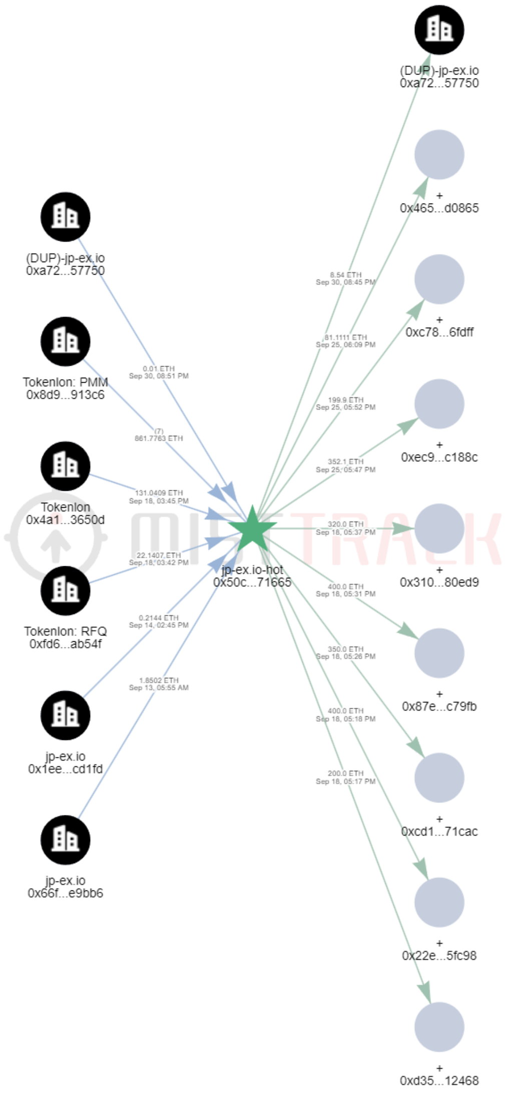
(JPEX Incident Timeline Chart)

We used MistTrack to analyzed some addresses associated with JPEX, here’s what we found::

【Ethereum】

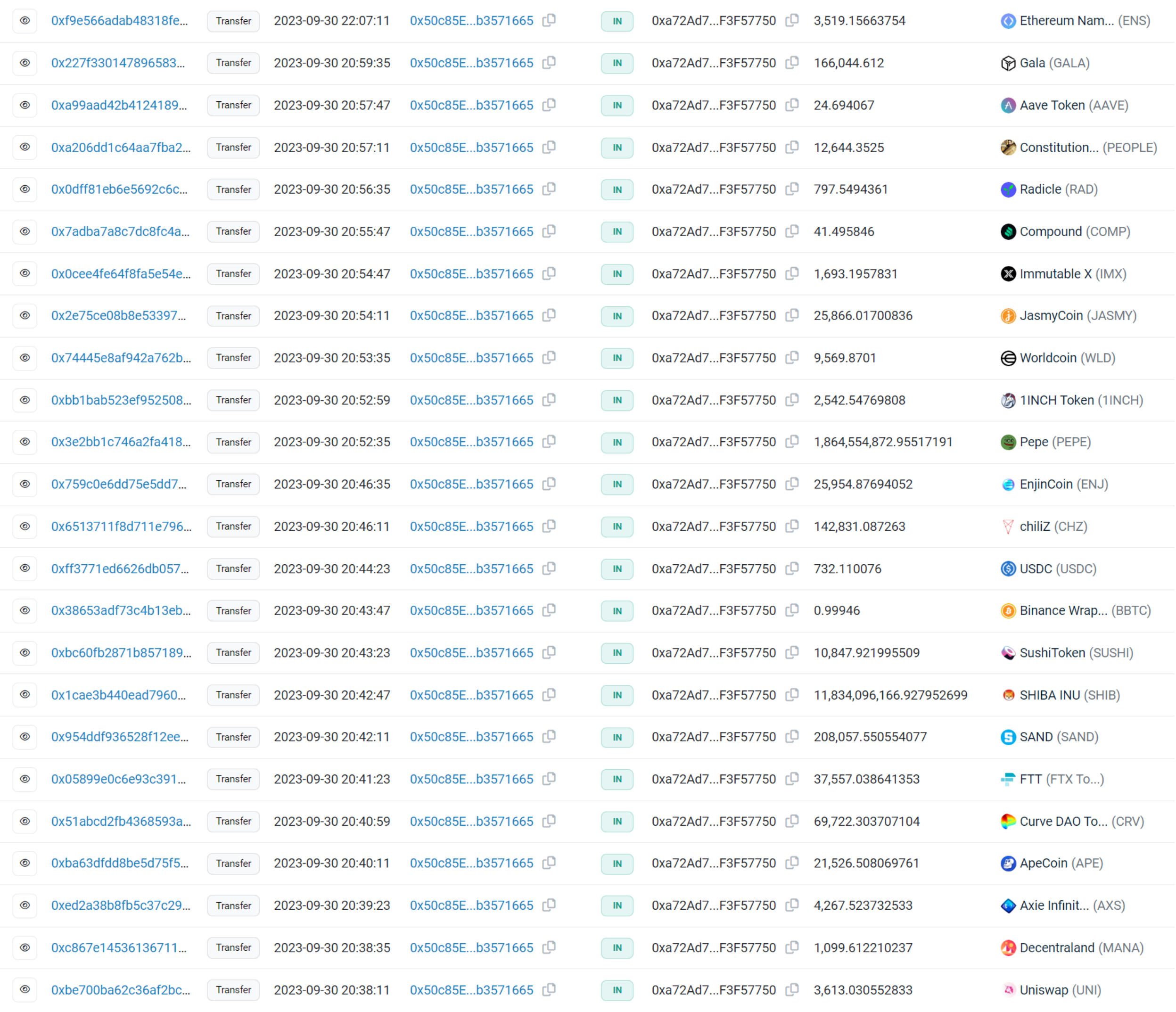
1. Starting September 18, the JPEX deposit collection hot wallet address 0x50c85e5587d5611cf5cdfba23640bc18b3571665 began exchanging most of its USDT for ETH, with subsequent transfers of ETH on September 18, 25, and 30:

- On September 18, 1,670 ETH were transferred to five different addresses, with no further movements as of yet.
- On September 25, 633.11 ETH were moved to three different addresses, also with no further movements to date.
- On September 30, 8.54 ETH were transferred to the JPEX Deposit address 0xa72ad701807e5902f458e1844d560128f3f57750.



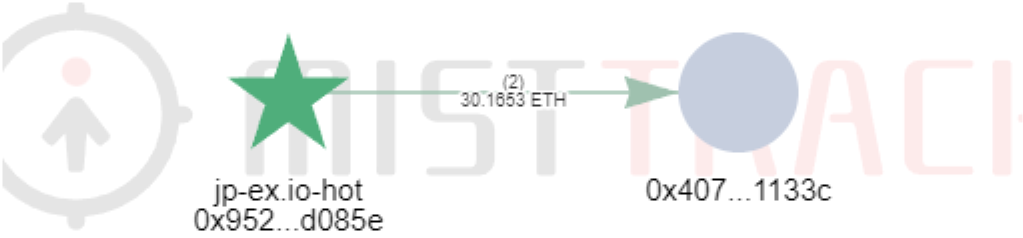
Additionally, on September 30, the address 0x50c8 transferred several ERC20 tokens (such as GALA, COMP, PEPE) to the JPEX Deposit address

0xa72Ad701807e5902F458e1844D560128F3F57750, with no further movements as of yet.

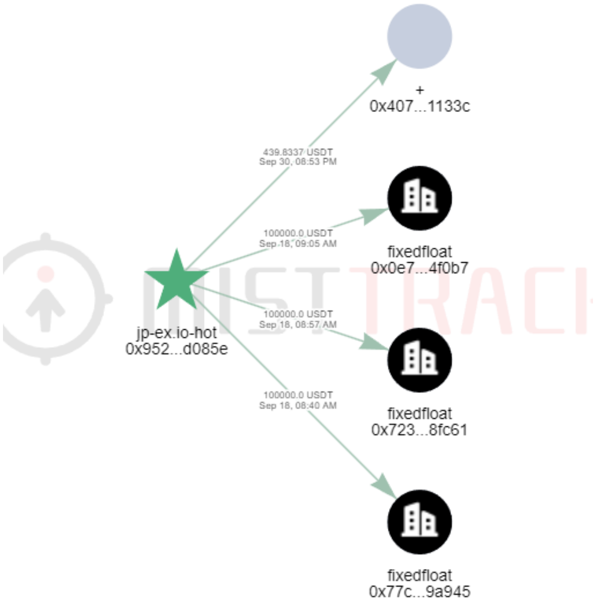


0xf9e566adab48318fe...	Transfer	2023-09-30 22:07:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	3,519.15663754	Ethereum Nam... (ENS)
0x227f330147896583...	Transfer	2023-09-30 20:59:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	166,044.612	Gala (GALA)
0xa99aad42b4124189...	Transfer	2023-09-30 20:57:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	24.694067	Aave Token (AAVE)
0xa206dd1c64aa7fba2...	Transfer	2023-09-30 20:57:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	12,644.3525	Constitution... (PEOPLE)
0x0dff81eb6e5692c6c...	Transfer	2023-09-30 20:56:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	797.5494361	Radicle (RAD)
0x7adba7a8c7dc8fc4a...	Transfer	2023-09-30 20:55:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	41.495846	Compound (COMP)
0x0cee4fe64f8fa5e54e...	Transfer	2023-09-30 20:54:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,693.1957831	Immutable X (IMX)
0x2e75ce08b8e53397...	Transfer	2023-09-30 20:54:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	25,866.01700836	JasmyCoin (JASMY)
0x74445e8af942a762b...	Transfer	2023-09-30 20:53:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	9,569.8701	Worldcoin (WLD)
0xbb1bab523ef952508...	Transfer	2023-09-30 20:52:59	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	2,542.54769808	1INCH Token (1INCH)
0x3e2bb1c746a2fa418...	Transfer	2023-09-30 20:52:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,864,554,872.95517191	Pepe (PEPE)
0x759c0e6dd75e5dd7...	Transfer	2023-09-30 20:46:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	25,954.87694052	EnjinCoin (ENJ)
0x6513711f8d711e796...	Transfer	2023-09-30 20:46:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	142,831.087263	chiliZ (CHZ)
0xff3771ed6626db057...	Transfer	2023-09-30 20:44:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	732.110076	USDC (USDC)
0x38653adf73c4b13eb...	Transfer	2023-09-30 20:43:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	0.99946	Binance Wrap... (BBTC)
0xbc60fb2871b857189...	Transfer	2023-09-30 20:43:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	10,847.921995509	SushiToken (SUSHI)
0x1cae3b440ead7960...	Transfer	2023-09-30 20:42:47	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	11,834,096,166.927952699	SHIBA INU (SHIB)
0x954ddf936528f12ee...	Transfer	2023-09-30 20:42:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	208,057.550554077	SAND (SAND)
0x05899e0c6e93c391...	Transfer	2023-09-30 20:41:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	37,557.038641353	FTT (FTX To...)
0x51abcd2fb4368593a...	Transfer	2023-09-30 20:40:59	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	69,722.303707104	Curve DAO To... (CRV)
0xba63dfdd8be5d75f5...	Transfer	2023-09-30 20:40:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	21,526.508069761	ApeCoin (APE)
0xed2a38b8fb5c37c29...	Transfer	2023-09-30 20:39:23	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	4,267.523732533	Axie Infinit... (AXS)
0xc867e14536136711...	Transfer	2023-09-30 20:38:35	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	1,099.612210237	Decentraland (MANA)
0xbe700ba62c36af2bc...	Transfer	2023-09-30 20:38:11	0x50c85E...b3571665	IN	0xa72Ad7...F3F57750	3,613.030552833	Uniswap (UNI)

2. The JPEX hot wallet address 0x9528043b8fc2a68380f1583c389a94dcd50d085e transferred 30.1653 ETH on September 30 to the address 0x4071b1fbe9d83acef3fc9c780122e6c0e611133c, which has not been moved since.

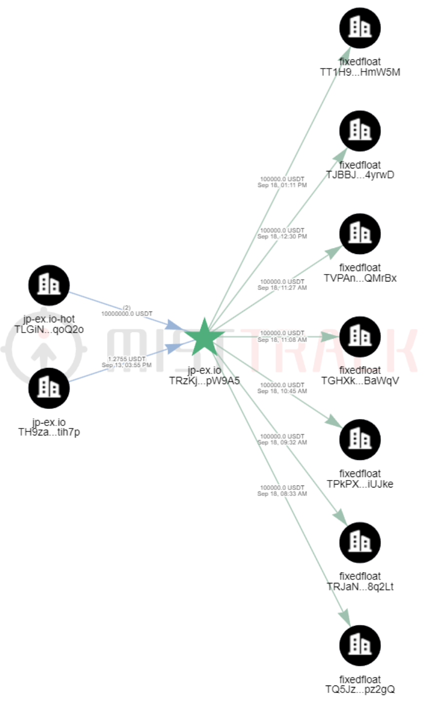


The same hot wallet address 0x952 transferred 300,000 USDT on September 18 to three FixedFloat deposit addresses, and on September 30, it transferred 439.83 USDT to the address 0x4071b1fbe9d83acef3fc9c780122e6c0e611133c, with no further transfers noted.



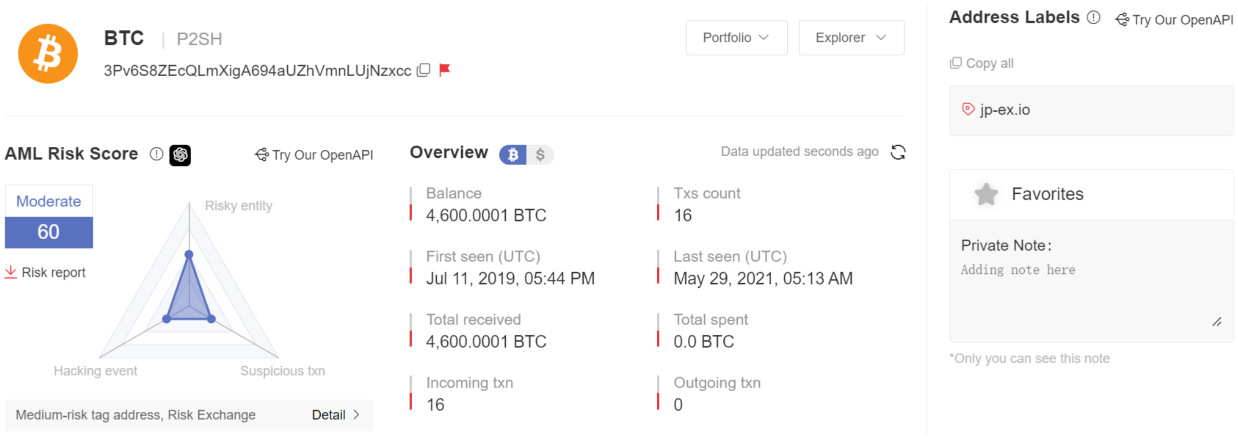
【TRON】

On September 18, the JPEX cold wallet address TRzKj5d8Mk3LVEbLrEey7myHy59cSpW9A5 transferred 700,000 USDT to seven FixedFloat deposit addresses:



【BTC】

1. The 4,600 BTC in address 3Pv6S8ZEcQLmXigA694aUZhVmnLUjNzxcc remains unmoved.



BTC | P2SH

3Pv6S8ZEcQLmXigA694aUZhVmnLUjNzxcc

AML Risk Score

Moderate
60

Medium-risk tag address, Risk Exchange

Overview

Data updated seconds ago

Balance 4,600.0001 BTC	Txs count 16
First seen (UTC) Jul 11, 2019, 05:44 PM	Last seen (UTC) May 29, 2021, 05:13 AM
Total received 4,600.0001 BTC	Total spent 0.0 BTC
Incoming txn 16	Outgoing txn 0

Address Labels

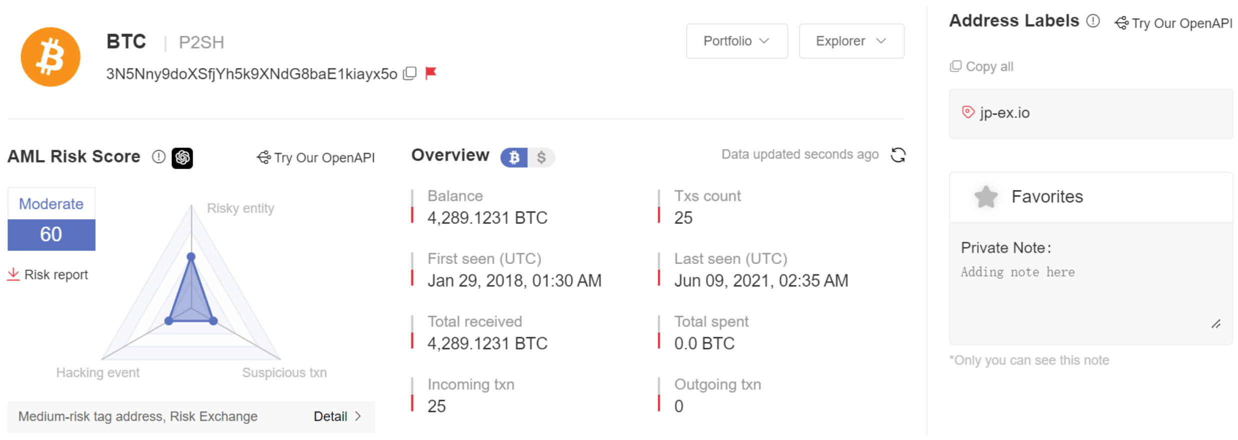
jp-ex.io

Private Note：

Adding note here

*Only you can see this note

2. The 4,289 BTC in address 3N5Nny9doXSfjYh5k9XNdG8baE1kiayx5o also remains unmoved.



BTC | P2SH

3N5Nny9doXSfjYh5k9XNdG8baE1kiayx5o

Address Labels

jp-ex.io

AML Risk Score

Moderate

60

Medium-risk tag address, Risk Exchange

Overview

Data updated seconds ago

Balance
4,289.1231 BTC

Txs count
25

First seen (UTC)
Jan 29, 2018, 01:30 AM

Last seen (UTC)
Jun 09, 2021, 02:35 AM

Total received
4,289.1231 BTC

Total spent
0.0 BTC

Incoming txn
25

Outgoing txn
0

Private Note:
Adding note here

*Only you can see this note

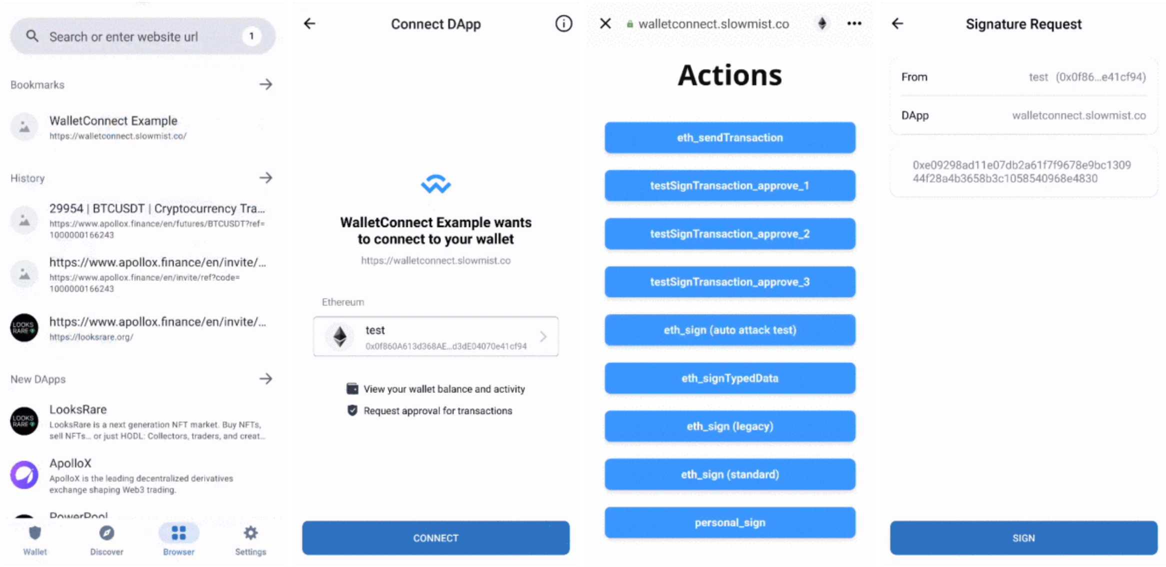
Following the incident, the Hong Kong Special Administrative Region Government and the Securities and Futures Commission acted promptly, demonstrating their commitment and serious attention to the matter. As stated by the Chief Executive of the Hong Kong Special Administrative Region, Lee Ka-chiu, "The JPEX incident reflects the importance of regulation and the necessity to invest in regulated platforms, as well as the importance of individual understanding of virtual assets." The CEO of the Hong Kong Securities and Futures Commission, Julia Leung Fung-yee, also commented, "The JPEX incident further highlights the importance of regulation, emphasizing that Hong Kong's direction in developing the Web3 ecosystem will not change. Virtual asset trading is an important part of the Web3 ecosystem, and the underlying technologies used in digital finance and virtual asset activities can bring benefits to the financial market." As we have seen, although this incident has posed short-term challenges for retail investors and related trading platforms, the market sentiment is expected to improve over time with the refinement of regulations. Regulatory bodies will likely enforce stricter and more comprehensive oversight of emerging financial services.

2.5 Phishing/Scam Techniques

This section highlights some of the phishing/scam techniques disclosed in 2023.

2.5.1 WalletConnect Phishing Incident

On January 30, 2023, the SlowMist security team identified a potential phishing risk associated with improper use of WalletConnect on Web3 wallets. This issue arises in scenarios where mobile wallet apps use an in-built DApp Browser in conjunction with WalletConnect. Some Web3 wallets, when providing support for WalletConnect, do not restrict where the WalletConnect transaction pop-up should appear. As a result, the sign-in request pop-up could appear on any interface of the wallet. When a user leaves the DApp Browser interface and switches to other wallet interfaces, such as Wallet or Discover, the WalletConnect connection remains active to avoid disrupting the user experience and to prevent repeated authorization. However, this can lead to unintended consequences if a malicious DApp suddenly triggers a sign-in request pop-up, potentially leading users to inadvertently perform actions that result in asset transfers through phishing.



WalletConnect Example
https://walletconnect.slowmist.co/

29954 | BTCUSDT | Cryptocurrency Tra...
https://www.apollox.finance/en/futures/BTCUSDT?ref=1000000166243

https://www.apollox.finance/en/invite/...
https://www.apollox.finance/en/invite/ref?code=1000000166243

https://www.apollox.finance/en/invite/...
https://looksrare.org/

LooksRare
LooksRare is a next generation NFT market. Buy NFTs, sell NFTs... or just HODL: Collectors, traders, and creat...

ApolloX
ApolloX is the leading decentralized derivatives exchange shaping Web3 trading.

PowerPool

WalletConnect Example wants to connect to your wallet
https://walletconnect.slowmist.co

test
0x0f860A613d368AE...d3dE04070e41cf94

View your wallet balance and activity
Request approval for transactions

walletconnect.slowmist.co

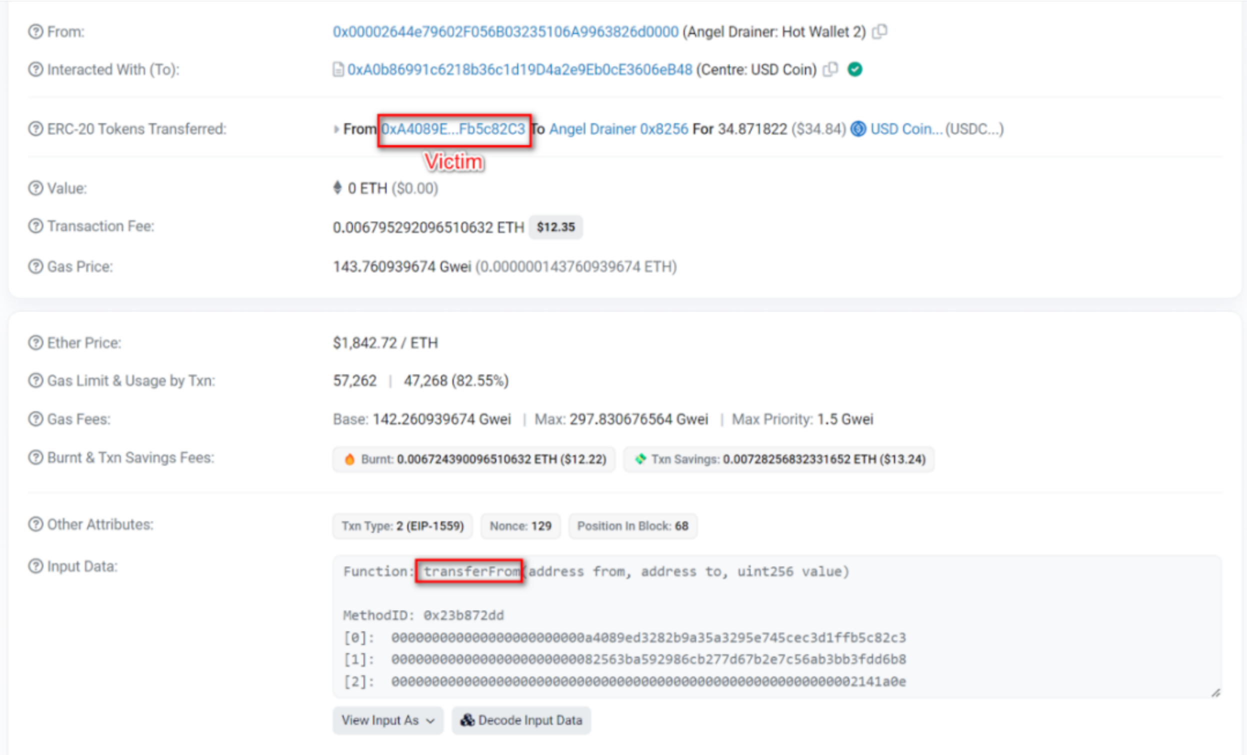
From test (0x0f86...e41cf94)
DApp walletconnect.slowmist.co

0xe09298ad11e07db2a61f7f9678e9bc1309
44f28a4b3658b3c1058540968e4830

Attackers use malicious DApp phishing sites to guide users to connect with WalletConnect. Once connected, they persistently send malicious sign-in requests (like eth_sign). If users recognize the potential risks of eth_sign and refuse to sign, the phishing page, due to WalletConnect's use of WebSocket Secure (wss) connections, continues to send malicious eth_sign sign-in pop-up requests. When using the wallet, users may mistakenly click the sign button, leading to asset theft. The main risks for individual users lies in two key areas: "domain and signature." This phishing method via WalletConnect has long been employed by many malicious websites, so users must remain highly vigilant when using it. For wallet developers, the first step is to conduct comprehensive security audits, particularly improving the user interaction security aspect. Strengthening the 'what you see is what you sign' mechanism can help reduce the risk of users falling for phishing attacks.

2.5.2 Permit Signature Phishing

Example of a victim's stolen transaction below:



From: 0x00002644e79602F056B03235106A9963826d0000 (Angel Drainer: Hot Wallet 2)

Interacted With (To): 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48 (Centre: USD Coin)

ERC-20 Tokens Transferred: From 0xA4089E...Fb5c82C3 To Angel Drainer 0x8256 For 34.871822 ($34.84) USD Coin... (USDC...)

Victim

Value: 0 ETH ($0.00)

Transaction Fee: 0.006795292096510632 ETH $12.35

Gas Price: 143.760939674 Gwei (0.000000143760939674 ETH)

Ether Price: $1,842.72 / ETH

Gas Limit & Usage by Txn: 57,262 | 47,268 (82.55%)

Gas Fees: Base: 142.260939674 Gwei | Max: 297.830676564 Gwei | Max Priority: 1.5 Gwei

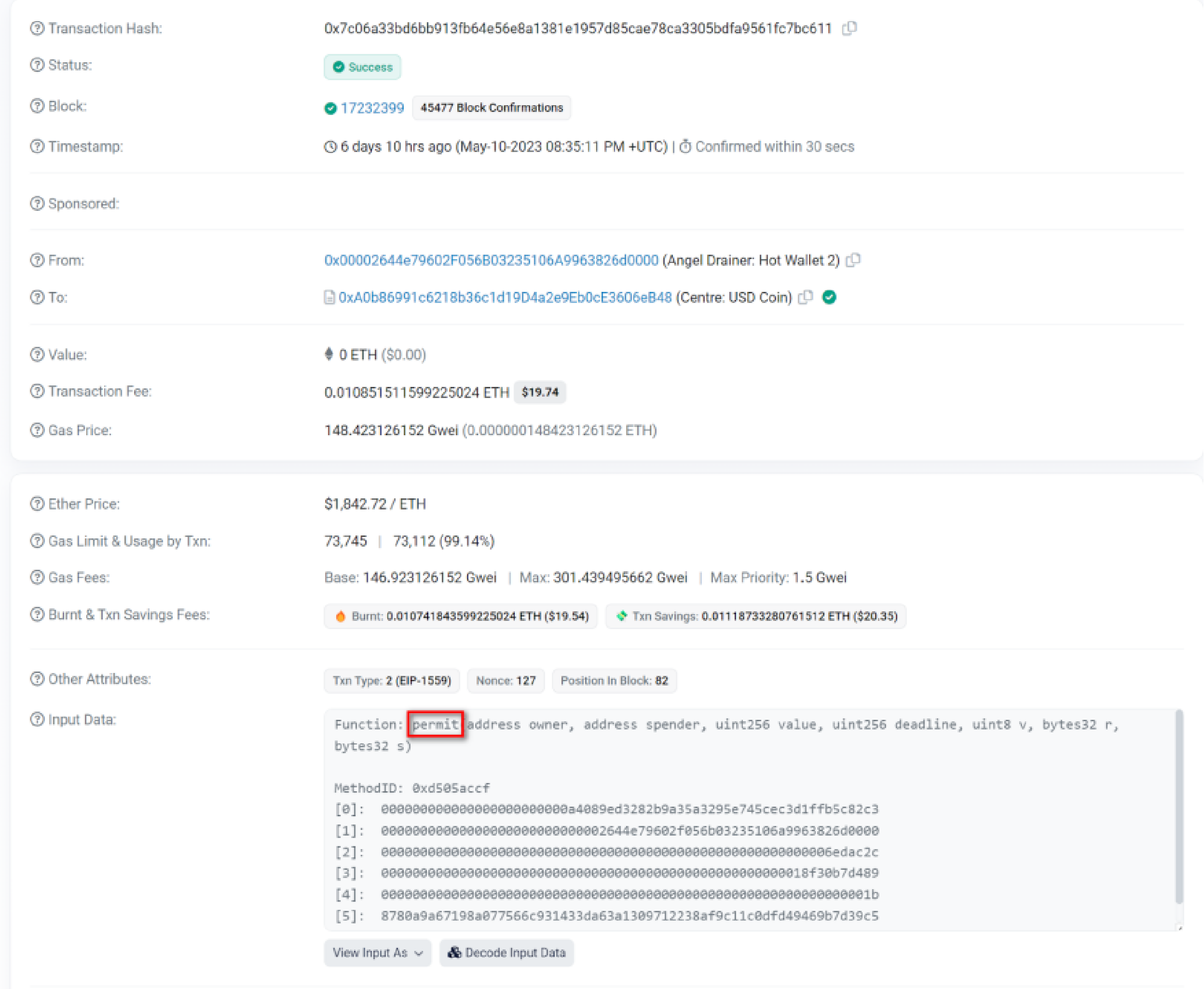
Burnt & Txn Savings Fees: Burnt: 0.006724390096510632 ETH ($12.22) Txn Savings: 0.007282568323331652 ETH ($13.24)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 129 Position In Block: 68

Input Data:

```
Function: transferFrom(address from, address to, uint256 value)

MethodID: 0x23b872dd
[0]:  000000000000000000000000a4089ed3282b9a35a3295e745cec3d1ffb5c82c3
[1]:  00000000000000000000000082563ba592986cb277d67b2e7c56ab3bb3fdd6b8
[2]:  0000000000000000000000000000000000000000000000000000000002141a0e
```

Analyzing this transaction, the contract initiator (0x00002...d0000) used the TransferFrom function to transfer 34.87 USDC from the victim's address (0xA4089...82C3) to another address (0x8256...D6B8). The TransferFrom function, upon a cursory inspection, appears straightforward: it allows a third party to initiate a transaction, transferring digital assets from the owner's account to the recipient's account. However, a deeper examination of the contract initiator's address (0x00002...d0000) reveals an additional permit operation, which is notably absent in the victim's transaction record.



Transaction Hash: 0x7c06a33bd6bb913fb64e56e8a1381e1957d85cae78ca3305bdfa9561fc7bc611

Status: Success

Block: 17232399 45477 Block Confirmations

Timestamp: 6 days 10 hrs ago (May-10-2023 08:35:11 PM +UTC) | Confirmed within 30 secs

Sponsored:

From: 0x00002644e79602F056B03235106A9963826d0000 (Angel Drainer: Hot Wallet 2)

To: 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48 (Centre: USD Coin)

Value: 0 ETH ($0.00)

Transaction Fee: 0.010851511599225024 ETH $19.74

Gas Price: 148.423126152 Gwei (0.000000148423126152 ETH)

Ether Price: $1,842.72 / ETH

Gas Limit & Usage by Txn: 73,745 | 73,112 (99.14%)

Gas Fees: Base: 146.923126152 Gwei | Max: 301.439495662 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees: Burnt: 0.010741843599225024 ETH ($19.54) Txn Savings: 0.01118733280761512 ETH ($20.35)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 127 Position In Block: 82

Input Data:

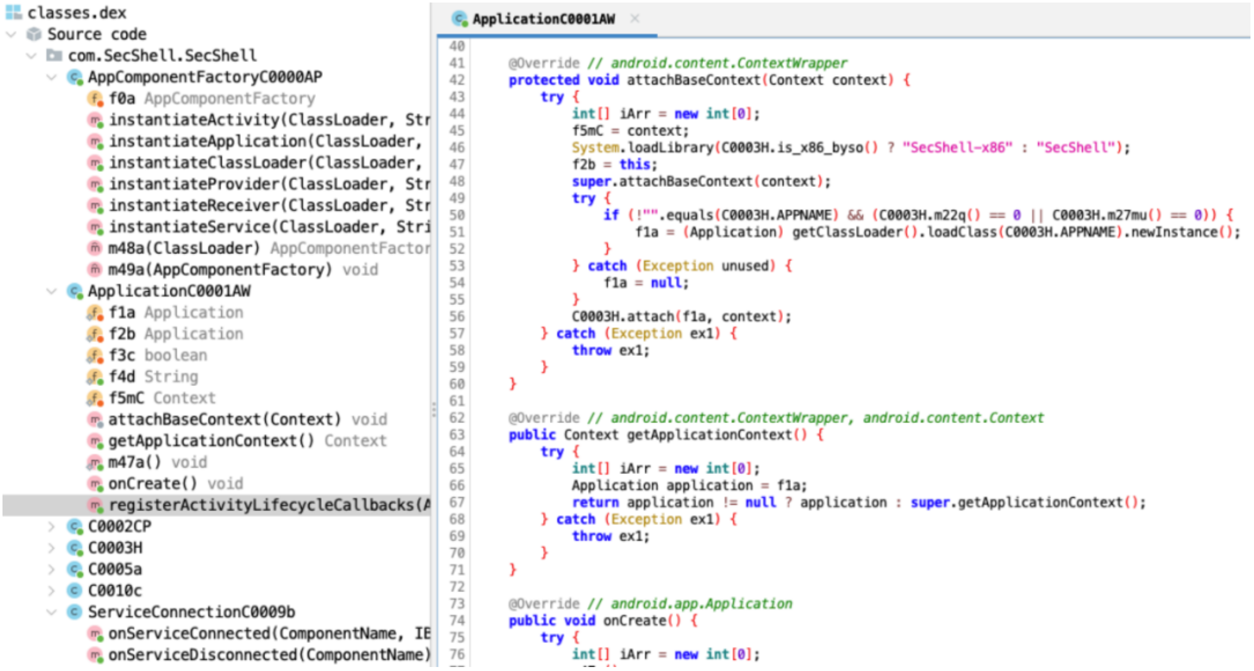
```
Function: permit address owner, address spender, uint256 value, uint256 deadline, uint8 v, bytes32 r,
bytes32 s)

MethodID: 0xd505accf
[0]:  000000000000000000000000a4089ed3282b9a35a3295e745cec3d1ffb5c82c3
[1]:  00000000000000000000000000002644e79602f056b03235106a9963826d0000
[2]:  00000000000000000000000000000000000000000000000000000000006edac2c
[3]:  000000000000000000000000000000000000000000000000000000018f30b7d489
[4]:  000000000000000000000000000000000000000000000000000000000000001b
[5]:  8780a9a67198a077566c931433da63a1309712238af9c11c0dfd49469b7d39c5
```

Official sources state that the 'permit' function was incorporated into the ERC20 protocol with EIP-2612, allowing users to interact with application contracts without prior authorization by attaching an authorization signature (permit). Specifically, in ERC20 token transactions, user A can authorize user B by using the approve function, granting B permission to operate a specified amount of A's tokens, and this function can only be called by the account owner. The role of the permit function is that A can sign the authorization off-chain in advance, informing B of this signature. Then B can use this signature to call permit, executing A's authorization actions (gaining allowance to use transferFrom for transfers), enabling A to transfer specified tokens without initiating a transaction, regardless of whether they are the account owner.

Additionally, Uniswap has introduced a new Token authorization standard, Permit2, which has also been targeted by phishing attacks. SlowMist advises users to avoid accessing websites of unknown origin, to carefully control the amount of Tokens authorized to contracts when interacting with DApps, and to thoroughly check signature content. Users are recommended to periodically use authorization tools like RevokeCash to check for abnormal authorizations and to use specific authorization management tools for Uniswap Permit2. If any abnormal authorizations are found, they should be revoked promptly.

2.5.3 Phishing with Fake Skype Apps

The prevalence of fake apps online extends beyond wallet and exchange categories, with social media applications like Telegram, WhatsApp, and Skype also being major targets. Phishing groups often add an extra layer of protection to these fake apps to prevent analysis. Common behaviors of these fake apps include uploading files and images from phones and data that may contain sensitive user information. Malicious alterations to network transmissions, such as changing the destination address of wallet transfers, have become increasingly common in fake Telegram and exchange apps. Users need to be extra cautious when downloading and using apps, ensuring they are using official download channels to avoid inadvertently downloading malicious apps and suffering financial losses.



```
classes.dex
  Source code
    com.SecShell.SecShell
      AppComponentFactoryC0000AP
        f0a AppComponentFactory
        instantiateActivity(ClassLoader, Str
        instantiateApplication(ClassLoader,
        instantiateClassLoader(ClassLoader,
        instantiateProvider(ClassLoader, Str
        instantiateReceiver(ClassLoader, Str
        instantiateService(ClassLoader, Stri
        m48a(ClassLoader) AppComponentFactor
        m49a(AppComponentFactory) void
      ApplicationC0001AW
        f1a Application
        f2b Application
        f3c boolean
        f4d String
        f5mC Context
        attachBaseContext(Context) void
        getApplicationContext() Context
        m47a() void
        onCreate() void
        registerActivityLifecycleCallbacks(A
      C0002CP
      C0003H
      C0005a
      C0010c
      ServiceConnectionC0009b
        onServiceConnected(ComponentName, IE
        onServiceDisconnected(ComponentName)
```

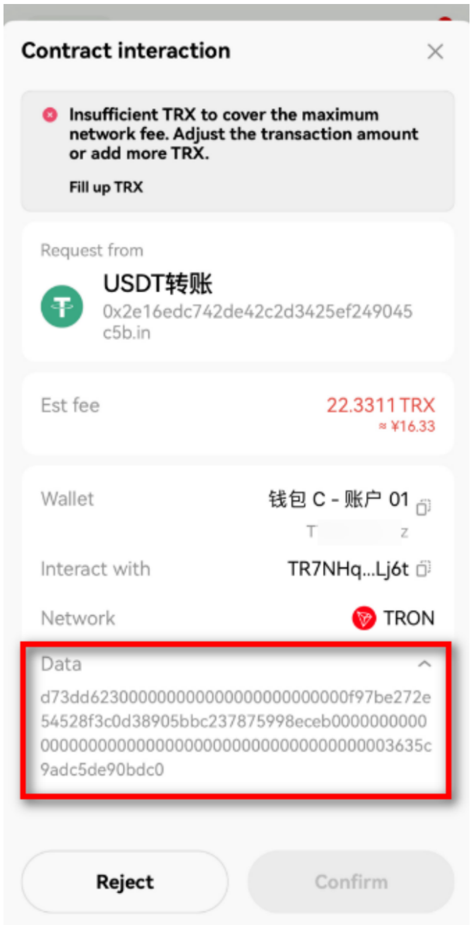
ApplicationC0001AW

```java

    @Override // android.content.ContextWrapper
    protected void attachBaseContext(Context context) {
        try {
            int[] iArr = new int[0];
            f5mC = context;
            System.loadLibrary(C0003H.is_x86_byso() ? "SecShell-x86" : "SecShell");
            f2b = this;
            super.attachBaseContext(context);
            try {
                if (!"".equals(C0003H.APPNAME) && (C0003H.m22q() == 0 || C0003H.m27mu() == 0)) {
                    f1a = (Application) getClassLoader().loadClass(C0003H.APPNAME).newInstance();
                }
            } catch (Exception unused) {
                f1a = null;
            }
            C0003H.attach(f1a, context);
        } catch (Exception ex1) {
            throw ex1;
        }
    }

    @Override // android.content.ContextWrapper, android.content.Context
    public Context getApplicationContext() {
        try {
            int[] iArr = new int[0];
            Application application = f1a;
            return application != null ? application : super.getApplicationContext();
        } catch (Exception ex1) {
            throw ex1;
        }
    }

    @Override // android.app.Application
    public void onCreate() {
        try {
            int[] iArr = new int[0];
```

2.5.4 Phishing Websites Disguised as Transfer Addresses

This type of scam often occurs in chat applications (like Telegram), beginning with over-the-counter (OTC) transactions. Before the actual transaction, scammers ask victims to transfer 0.1 USDT to "confirm whether their address poses any risk." They then provide the victim with a "public chain" address for the transaction, emphasizing that it must be entered into the wallet browser for the transfer to proceed. However, once the victim enters this “public chain” address into their browser, they find that all the tokens in their account have been stolen. The issue lies in this “public chain” address — 0x2e16edc742de42c2d3425ef249045c5b.in. Although it appears to be a TRON transaction with a 0x prefix, on closer inspection, it is actually a website URL ending in .in, not a blockchain address.

When searched in a wallet browser, this address only allows selections for the TRON network. After entering an amount and clicking next, the interaction is shown as a contract interaction (Contract interaction):



Contract interaction ✕

Insufficient TRX to cover the maximum network fee. Adjust the transaction amount or add more TRX.

Fill up TRX

Request from

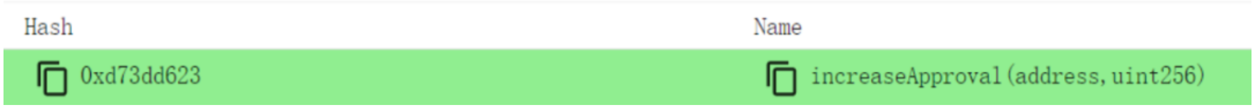
USDT转账
0x2e16edc742de42c2d3425ef249045c5b.in

Est fee	22.3311 TRX ≈ ¥16.33
Wallet	钱包 C - 账户 01 T [redacted] z
Interact with	TR7NHq...Lj6t
Network	TRON

Data

```
d73dd623000000000000000000000000f97be272e
54528f3c0d38905bbc237875998eceb0000000000
000000000000000000000000000000000003635c
9adc5de90bdc0
```

Decoding the Data section of the transaction, it's discovered that the scammer tricks the user into signing an increaseApproval action. Once the user clicks Confirm, the scammer is then able to steal the user's tokens using the transferFrom method.



Hash	Name
0xd73dd623	increaseApproval(address,uint256)

Given that blockchain technology is immutable and on-chain operations are irreversible, it is crucial to carefully verify addresses before performing any actions. Additionally, understanding the risk associated with a target address before conducting on-chain transactions is very important. For instance, entering the target address into tools like MistTrack to check its risk score and malicious tags can significantly help in avoiding financial losses.

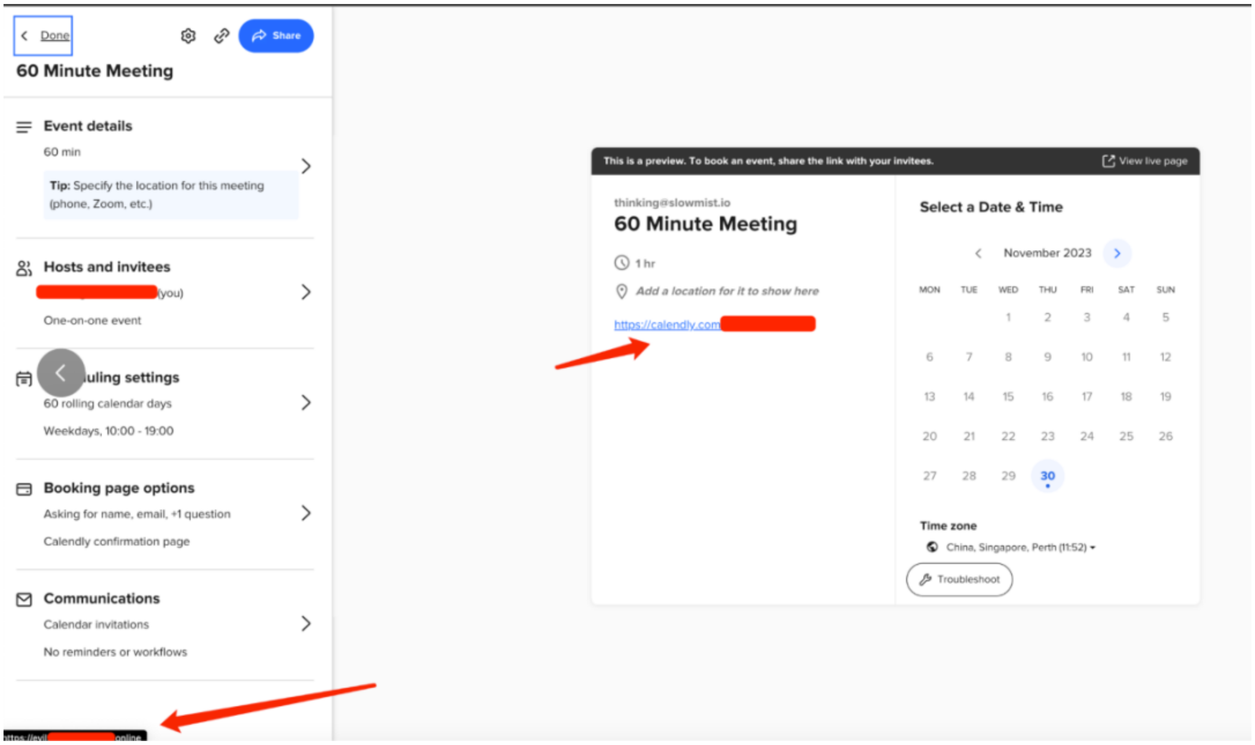
2.5.5 Targeted Attacks on Telegram

North Korean hackers impersonate well-known investment institutions to carry out phishing attacks against project teams, typically following these steps:

1. Select a Well-Known Investment Institution for Impersonation: They create fake Telegram accounts impersonating these institutions.
2. Identify Targets Among Prominent DeFi Projects: The fraudsters target well-known DeFi projects, initiating contact under the pretense of wanting to invest in them using these fake accounts.
3. Establish Contact and Build Trust: They start by engaging in conversations with the target to build a rapport. Once the trust of the project team is gained, they arrange meetings to carry out their scam. There are mainly two types of attack strategies used in these situations:

    - The fraudsters invite the project team to join meetings on websites like "***.group-meeting.team", pretending to schedule a face-to-face discussion and providing a malicious meeting link. When the project team clicks the link, they encounter a supposed regional access restriction. At this point, the North Korean hackers persuade the team to download and run a “location modifying” malicious script they provide. If the project team complies, their computers become controlled by the hackers, leading to the theft of funds.

- They also exploit the "Add Custom Link" feature of the Calendly meeting scheduling system to insert malicious links into event pages for phishing attacks. As Calendly seamlessly integrates into the routine work environment of most project teams, these malicious links are less likely to raise suspicion. Unsuspectingly, the project team may click on these links, download, and execute malicious code, allowing the North Korean hackers to gain access to or control over the project team's system.



60 Minute Meeting

Event details
60 min
Tip: Specify the location for this meeting (phone, Zoom, etc.)

Hosts and invitees
[redacted](you)
One-on-one event

uling settings
60 rolling calendar days
Weekdays, 10:00 - 19:00

Booking page options
Asking for name, email, +1 question
Calendly confirmation page

Communications
Calendar invitations
No reminders or workflows

https://evil[redacted]online

This is a preview. To book an event, share the link with your invitees.

thinking@slowmist.io
60 Minute Meeting
1 hr
Add a location for it to show here
https://calendly.com[redacted]

Select a Date & Time

November 2023

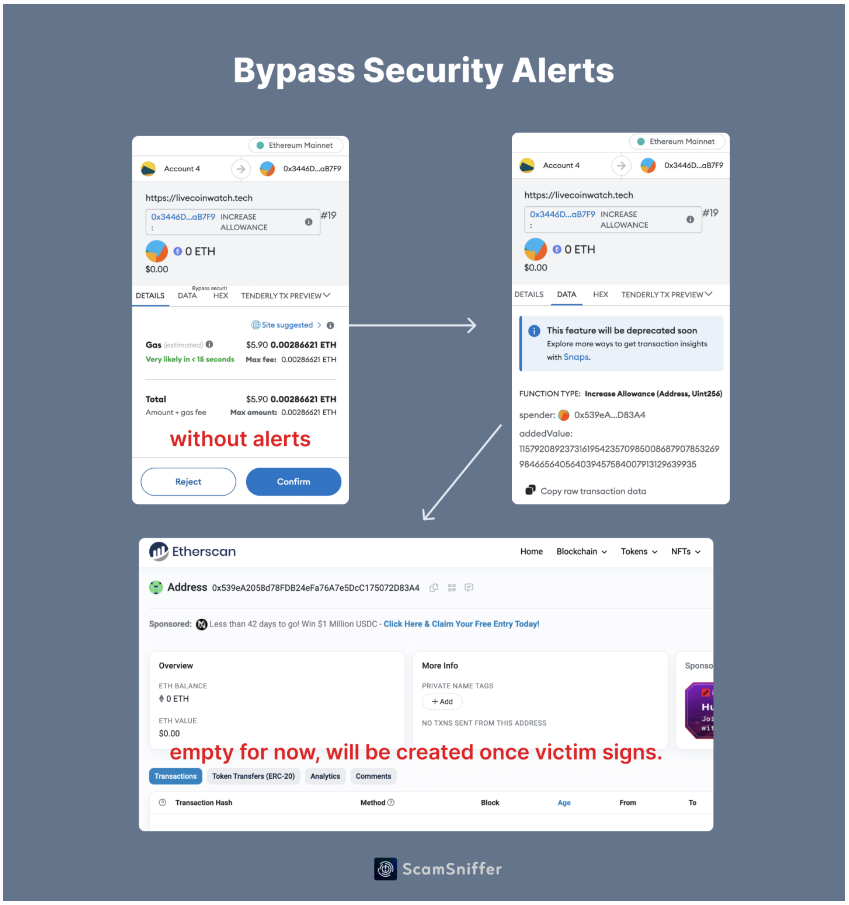
MON	TUE	WED	THU	FRI	SAT	SUN
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Time zone
China, Singapore, Perth (11:52)

Besides looking out for scams, users should also ensure the authenticity of contacts through dual-channel verification when adding new connections. Additionally, enabling two-factor authentication (2FA) on Telegram and staying vigilant about transaction security is vital to prevent financial losses. In the event of inadvertently running a related Trojan, it is imperative to immediately transfer funds to a secure location, disconnect from the internet and run antivirus software, and change all relevant account passwords and information on the affected computer, including those stored in the browser.

2.5.6 Create2 Phishing Risk

Attackers exploit the "create2" function to pre-calculate addresses where contracts will be deployed, then deceive users into granting permissions. These blank addresses can bypass blacklisting and security monitoring by security firms. Once the user grants permission, the attacker deploys the contract to that address and transfers out the user's assets. According to joint disclosures by ScamSniffer and SlowMist, since August, an organization has used this technique in address poisoning to steal $3 million from 11 victims, with one victim alone losing up to $1.6 million.



Bypass Security Alerts

Ethereum Mainnet
Account 4 → 0x3446D...aB7F9
https://livecoinwatch.tech
0x3446D...aB7F9 : INCREASE ALLOWANCE #19
0 ETH
$0.00
DETAILS | DATA | HEX | TENDERLY TX PREVIEW
Bypass securit
Site suggested
Gas (estimated): $5.90 0.00286621 ETH
Very likely in < 15 seconds
Max fee: 0.00286621 ETH
Total: $5.90 0.00286621 ETH
Amount + gas fee
Max amount: 0.00286621 ETH
without alerts
Reject | Confirm

Ethereum Mainnet
Account 4 → 0x3446D...aB7F9
https://livecoinwatch.tech
0x3446D...aB7F9 : INCREASE ALLOWANCE #19
0 ETH
$0.00
DETAILS | DATA | HEX | TENDERLY TX PREVIEW
This feature will be deprecated soon
Explore more ways to get transaction insights with Snaps.
FUNCTION TYPE: Increase Allowance (Address, Uint256)
spender: 0x539eA...D83A4
addedValue: 115792089237316195423570985008687907853269984665640564039457584007913129639935
Copy raw transaction data

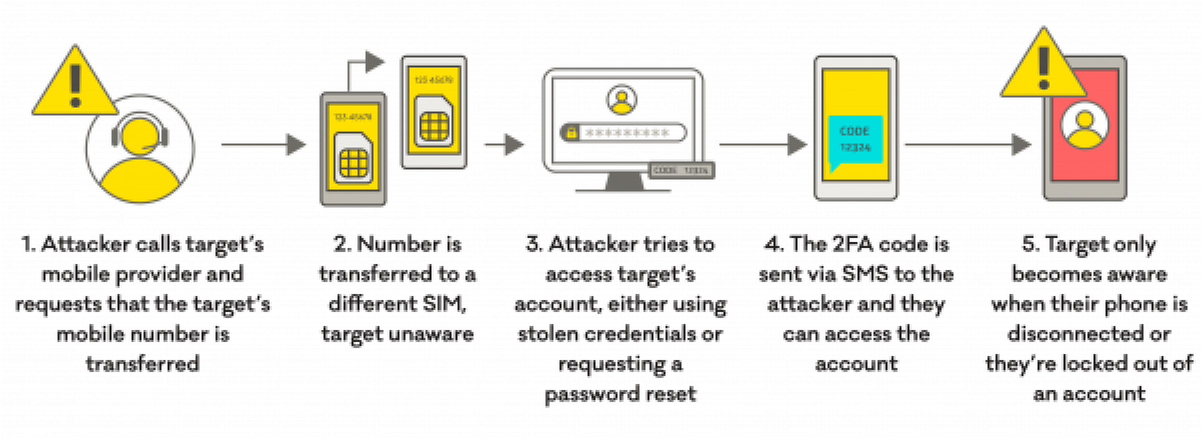
Etherscan
Home | Blockchain | Tokens | NFTs
Address 0x539eA2058d78FDB24eFa76A7e5DcC175072D83A4
Sponsored: Less than 42 days to go! Win $1 Million USDC - Click Here & Claim Your Free Entry Today!
Overview
ETH BALANCE: 0 ETH
ETH VALUE: $0.00
More Info
PRIVATE NAME TAGS: + Add
NO TXNS SENT FROM THIS ADDRESS
empty for now, will be created once victim signs.
Transactions | Token Transfers (ERC-20) | Analytics | Comments

Transaction Hash	Method	Block	Age	From	To

ScamSniffer

2.5.7 SIM Swap Attacks

In the cryptocurrency domain, attackers initiate SIM swap attacks with the goal of controlling the victim's phone number to bypass two-factor authentication, thereby gaining access to the victim's cryptocurrency accounts. With the rise of company data breaches and the sale of stolen personal information on the dark web, attackers obtain detailed personal data like identity cards from these leaks or through phishing. Armed with this information, they impersonate the victim to commence SIM swap attacks, gaining control over the victim's mobile communication and potentially their crypto assets.


1. Attacker calls target's mobile provider and requests that the target's mobile number is transferred
2. Number is transferred to a different SIM, target unaware
3. Attacker tries to access target's account, either using stolen credentials or requesting a password reset
4. The 2FA code is sent via SMS to the attacker and they can access the account
5. Target only becomes aware when their phone is disconnected or they're locked out of an account

On October 5, 2023, on-chain detective ZachXBT reported that a hacker, within the past 24 hours, executed SIM swap attacks against four different users of friend.tech, stealing 234 ETH (approximately $385,000).

In an interview with Cointelegraph, SlowMist CISO @23pds mentioned, "SIM Swap attacks are expected to intensify due to their low cost of execution. As Web3 becomes more popular and attracts more people to the industry, the likelihood of SIM swap attacks increases due to the relatively low technical requirements for conducting them."

The security of SIM cards depends on the security measures of the operators and is vulnerable to tactics like social engineering attacks. Therefore, it's advisable not to rely on authentication methods based solely on SIM cards. Users should enhance their account security by adding two-factor authentication, preferably using authenticators that support the TOTP algorithm.

III. Anti-Money Laundering(AML) Trends

3.1 AML and Regulatory Dynamics

In 2023, the world of cryptocurrencies continued to experience turmoil. During the previous crypto bull market, every move by industry giants SBF and CZ seemed to have a profound impact on the market. However, in November, a federal jury found SBF guilty on charges of fraud and conspiracy related to the collapse of FTX. Just weeks later, Binance accepted criminal charges and paid a fine of $4.3 billion, with CZ agreeing to relinquish control over Binance. As the crypto asset industry oscillates between a turbulent "crypto winter" and a bear market, governments and international organizations are adopting a more cautious approach. Regulatory policies concerning cryptocurrencies are still being progressively developed across various countries.

3.1.1 Stablecoin Regulation

The Navigating the Global Crypto Landscape with PwC: 2024 Outlook, released on December 19, reveals that in 2023, as many as 25 countries and regions have developed legislation or regulations for stablecoins. These include Austria, The Bahamas, Denmark, Estonia, Finland, France, Germany, Greece, Japan, Luxembourg, Portugal, Spain, Sweden, and Switzerland. The majority of these jurisdictions have also ensured or implemented all other scrutinized regulations, including a framework for cryptocurrency regulation, licensing or registration, and compliance with the Financial Action Task Force's (FATF) Travel Rule.

However, the report notes that some major countries like the United States, the United Kingdom, and Canada have not yet finalized legislation for stablecoins or established a comprehensive regulatory framework for cryptocurrencies. In contrast, crypto-friendly countries/regions like Singapore and the United Arab Emirates have adopted all cryptocurrency-related regulations except those pertaining to stablecoins.

Of the jurisdictions analyzed, about 18% or only 8 have not initiated any regulation for stablecoins. This group includes Bahrain, Brazil, India, Taiwan, Turkey, and others. Additionally, 23% of the reviewed jurisdictions, including Australia, Hong Kong, and Singapore, have commenced the regulatory process for stablecoins and are actively adopting relevant laws.

3.1.2 SEC Enforcement Actions

In November, the United States Securities and Exchange Commission (SEC) published the enforcement results for the fiscal year 2023. The report indicated that the SEC initiated 784 enforcement actions, a 3% increase from 2022. These actions resulted in penalties totaling $4.949 billion, the second-highest in history, only behind the $6.4 billion in 2022. The SEC noted that the fiscal year 2023 was a year of fruitful enforcement efforts, with key investigations involving areas such as cryptocurrencies, cybersecurity, false statements by publicly traded companies, and market manipulation.

Significant enforcement actions taken by the SEC in the crypto ecosystem included:

1. NFT Issuers Impact Theory and Stoner Cats: The SEC sued these NFT issuers under federal securities laws, marking an expansion in the SEC's regulatory scope. Both companies agreed to settlements with the SEC, paying approximately $6.1 million and $1 million, respectively, after being accused of selling unregistered securities.
2. Kraken Settlement: Kraken settled with the SEC for $30 million over its staking services, which were deemed unregistered securities, fitting the definition of an investment contract.
3. Linus Financial Agreement: The SEC reached a settlement with the Nashville-based crypto services company Linus Financial for allegedly offering and selling unregistered retail crypto lending products.
4. Coinbase Lawsuit: The SEC's lawsuit against Coinbase alleges that the exchange has been operating as an unregistered securities exchange, broker-dealer, and clearing agency. Coinbase has filed a motion to dismiss the lawsuit, with a decision expected in January of the following year.
5. Ripple and XRP: The SEC claims that Ripple's token XRP is a security. However, Judge Torres clarified in her ruling that XRP itself is not a security. Another judge, Rakoff, later overruled a motion that would have impacted the case, leaving the judgment still divided and undecided.
6. Bitcoin Spot ETF Applications: Despite numerous applicants and years of back-and-forth battles with the SEC, the commission has never approved a Bitcoin spot ETF. The latest

deadline for the SEC to respond to these applicants is between January 5th and 10th, 2024.

7. Civil Suit Against Binance: In June, the SEC filed a civil lawsuit against Binance, accusing the exchange of being unregistered and illegally supplying and selling securities to U.S. investors. The SEC has consistently refused Binance's requests to dismiss the lawsuit, and the legal battle is ongoing.

3.1.3 Anti-Money Laundering Sanctions

1. April 2nd: The United States Department of the Treasury sanctioned three North Koreans for providing money laundering support to the North Korean hacker group Lazarus Group.
2. May 25th: Binance assisted U.S. law enforcement in seizing $4.4 million and freezing accounts associated with organized crime in North Korea.
3. August 24th: As per the U.S. Treasury Department press release, the Justice Department charged Roman Semenov and Roman Storm, the co-founders of Tornado Cash, who were arrested by the FBI and IRS on charges of conspiring to launder money, operate an unlicensed money transmitting business, and violate sanctions regulations. The Treasury Department stated that despite knowing Lazarus Group was laundering hundreds of millions of dollars worth of stolen virtual currency for North Korean interests through its mixing service, Tornado Cash’s founders continued to develop and promote the service without meaningful measures to prevent its use for illegal purposes.
4. October 18th: The U.S. Department of the Treasury imposed sanctions on several individuals and entities, alleging support for Hamas's terrorist activities. This included a Gaza-based exchange and a business called "Buy Cash Money and Money Transfer Company." The Treasury stated that this business has a history of providing financial support to terrorist groups. Buy Cash was previously associated with wallets seized by the Israeli National Bureau for Counter Terror Financing in 2021, accused of "providing funds, material, technology, services, or support to Hamas," with transactions involving assets including Bitcoin.
5. October 31st: The Japanese government decided at a cabinet meeting to freeze assets of 9 Hamas members and a virtual currency trading company involved in funding the Palestinian armed political faction Hamas.

6. November 22nd: The U.S. Department of Justice announced that Binance and Changpeng Zhao pleaded guilty to federal charges in a $4 billion resolution. The U.S. Treasury's settlement announcement with Binance stated that the Financial Crimes Enforcement Network (FinCEN) would impose a $3.4 billion civil penalty on Binance, along with five years of regulation and significant compliance commitments, including ensuring Binance's full exit from the U.S.
7. November 29th: The U.S. Department of the Treasury sanctioned the cryptocurrency mixing service Sinbad for supporting transactions related to the North Korean hacker organization. Sinbad's website was also seized by the U.S. Federal Bureau of Investigation, the Dutch Financial Intelligence Unit, the Office of the Dutch Prosecutor, and the Finnish National Bureau of Investigation. Sinbad.io (Sinbad, also known as Sindbad) is a virtual currency mixer and a primary tool for laundering money for the Lazarus Group on behalf of North Korea. Sinbad facilitated the laundering of millions of dollars in stolen virtual currencies and was the mixer of choice for the Lazarus Group. Operating on the Bitcoin blockchain, Sinbad facilitated illegal transactions by obscuring their origins, destinations, and counterparties. Some industry experts believe Sinbad is another version of the Blender.io mixer.

3.1.4 Global Policy

- **China**

China has maintained a stringent policy towards cryptocurrencies. In 2021, China declared a complete ban on cryptocurrency trading and halted all business activities related to cryptocurrencies. On November 13th, the Financial Stability Bureau of the People's Bank of China published an article titled "Effectively Preventing and Resolving Financial Risks, Firmly Guarding Against Systemic Risks." The article highlighted that the rectification work in areas such as virtual currency trading was basically completed, with a firm stand against domestic cryptocurrency trading speculation. In December, the People's Bank of China released the *China Financial Stability Report (2023)*, which comprehensively assessed the soundness of China's financial system in 2022. The report addressed the risks associated with crypto assets and stated the continuation of rectifying illegal financial activities like virtual currency trading speculation. Additionally, the report summarized China's regulation of crypto assets and the global dynamics of crypto asset regulation, noting that "in recent years, many countries' regulatory authorities and international organizations have started assessing the risks of crypto assets, introducing regulatory policies and countermeasures, generally adhering to the principle of 'same business, same risk, same regulation,' regulating crypto asset operations commensurate with their risk levels, minimizing regulatory data gaps, reducing regulatory fragmentation, and eliminating regulatory arbitrage."

Despite China's strong containment of cryptocurrencies, the country continues to encourage the exploration and application of blockchain and digital currency-related technologies, responding and adjusting timely to emerging issues. Data shows that since the digital yuan was first introduced in January 2022, by the end of June, the transaction volume of the central bank's digital yuan was about 1.8 trillion yuan. On December 2nd, the People's Bank of China and the Central Bank of the United Arab Emirates renewed a 350 billion yuan/18 billion dirham (approximately $4.9 billion) currency swap agreement in Hong Kong, extending the bilateral currency swap agreement for five years to promote financial and economic ties. The two sides also signed a Memorandum of Understanding on Strengthening Cooperation in Central Bank Digital Currencies to enhance technical cooperation in the development of central bank digital currencies. On October 9th, six departments, including the Ministry of Industry and Information Technology, the Central Cyberspace Affairs Commission, the Ministry of Education, the National Health Commission, the People's Bank of China, and the State-owned Assets Supervision and Administration Commission, jointly issued the "High-Quality Development Action Plan for Computing Power Infrastructure." The plan proposes that by 2025, computing power will exceed 300 EFLOPS, with the proportion of intelligent computing power reaching 35%, and balanced development of computing power in the eastern and western regions. In December, the Ministry of Industry and Information Technology, in its response to Proposal No. 02969 of the First Session of the 14th National Committee of the Chinese People's Political Consultative Conference, stated that in addition to measures like "formulating a Web3.0 development strategy document suitable for China's national conditions" to improve top-level design, it will also strengthen research and regulation of Web3.0 technology, engage in international exchanges and cooperation on Web3.0, and increase technological promotion and dissemination.

- **Hong Kong SAR, China**

Hong Kong, as a regional financial center, is transforming itself into a cryptocurrency hub. On June 1st, Hong Kong's virtual currency licensing system officially opened, allowing platforms interested in virtual asset business to apply for a license and be regulated by the Hong Kong Securities and Futures Commission. On December 22nd, the Securities and Futures Commission issued *Circular on SFC-authorised funds with exposure to virtual assets*, replacing the previous *Circular on Virtual Asset Futures Exchange Traded Funds* issued on October 31, 2022. The notice stated that licensed institutions can issue and manage spot ETFs for virtual assets (like Bitcoin and Ethereum) that are permitted to trade on licensed trading platforms or recognized financial institutions, via both physical and cash subscription and redemption methods. In light of the JPEX incident, the CEO of the Securities and Futures Commission emphasized the importance of regulation, stating that Hong Kong's direction in developing the Web3 ecosystem will remain unchanged, and that virtual asset trading is an essential part of this ecosystem. The Commission and the Police Force have established a working group on virtual asset trading platforms, sharing information on suspicious activities and regulatory violations to jointly bring lawbreakers to justice. The Hong Kong Monetary Authority is also further strengthening cryptocurrency trading regulation to prevent money laundering and fraud, while the Securities and Futures Commission continues to review and enhance existing regulatory systems. On December 22, the Securities and Futures Commission (SFC) of Hong Kong issued *Joint circular on intermediaries' virtual asset-related activities* and *Circular on SFC-authorised funds with exposure to virtual assets*, stating that they are "ready to accept applications for the recognition of virtual asset spot exchange-traded funds (ETFs)."

- **United States**

The United States has a relatively flexible approach to cryptocurrencies. While regulatory policies are continually updated, there is no comprehensive ban on trading, purchasing, or selling cryptocurrencies. The U.S. is further enhancing its regulatory efforts to ensure the stability of the financial system and consumer protection.

- **European Union**

The European Union's regulatory policy on cryptocurrencies is still under discussion and revision, attempting to balance financial security with technological innovation. Notably, in December, the EU announced new sanctions against Russian-led cryptocurrency companies and projects, intensifying the crackdown on Russian crypto company executives.

- **Japan**

Japan is relatively open in its approach to cryptocurrencies, with established procedures and regulations to control and support the cryptocurrency market. In 2023, Japan's National Tax Agency released general guidelines on the taxation of NFTs, including examples of income tax collection and consumption tax situations. Additionally, the Bank of Japan stated it would make a final decision on issuing a CBDC before 2026.

- **South Korea**

South Korea has clear regulations on cryptocurrencies, including registration requirements, compliance audits, and financial consumer protection. South Korea is also promoting various blockchain-related innovation projects. In 2023, the Bank of Korea (BOK) announced details of its retail central bank digital currency (CBDC) pilot program, with 100,000 selected citizens to join in the fourth quarter of the next year. The Financial Services Commission (FSC) also announced legislative proposals and regulatory provisions for the *Virtual Asset User Protection Act* in December. The law aims to protect virtual asset users and establish a sound virtual asset market trading order. In response, the Financial Supervisory Service announced the establishment of a Virtual Asset Regulation Bureau and a Virtual Asset Investigation Bureau, in preparation for the implementation of the *Virtual Asset User Protection Act* in July of the following year.

- **Singapore**

Singapore has always been forward-looking in its legislation on cryptocurrencies. The Monetary Authority of Singapore (MAS) released a consultation paper on a crypto consumer protection handbook in 2023, which will be followed by final guidelines. Singapore actively participates in international financial cooperation, like the policymaker group Project Guardian, comprising Japan's FSA, the UK's FCA, and Switzerland's FINMA, to promote cross-border financial development and asset tokenization. MAS also launched pilot projects for digital assets and decentralized finance (DeFi) services in 2023.

In summary, due to the complexity of cryptocurrencies, regulatory policy has become a complex discussion involving financial stability, consumer protection, and anti-money laundering. However, as blockchain and cryptocurrency technologies become more widespread, more governments and institutions are getting involved, and regulatory policies are evolving towards more specific and global directions.

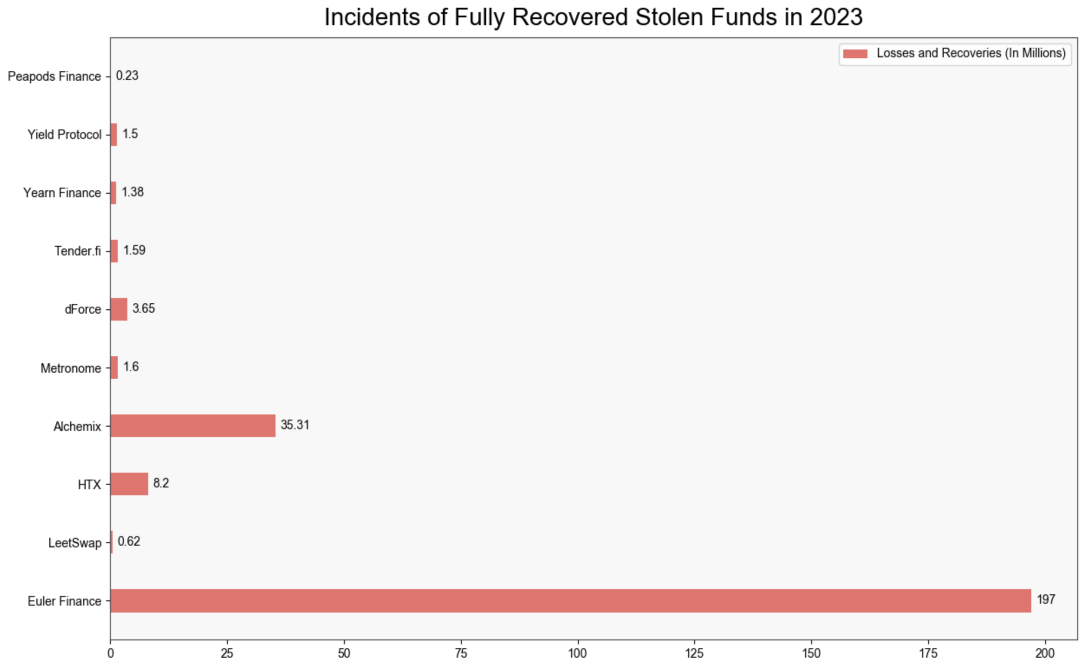
3.2 Anti-Money Laundering in Security Incidents

3.2.1 Frozen Funds Data

With substantial support from partners in the InMist Intelligence Network, SlowMist successfully assisted clients, partners, and publicly hacked entities in freezing over $12.5 million in funds in the year 2023.

3.2.2 Funds Recovery Data

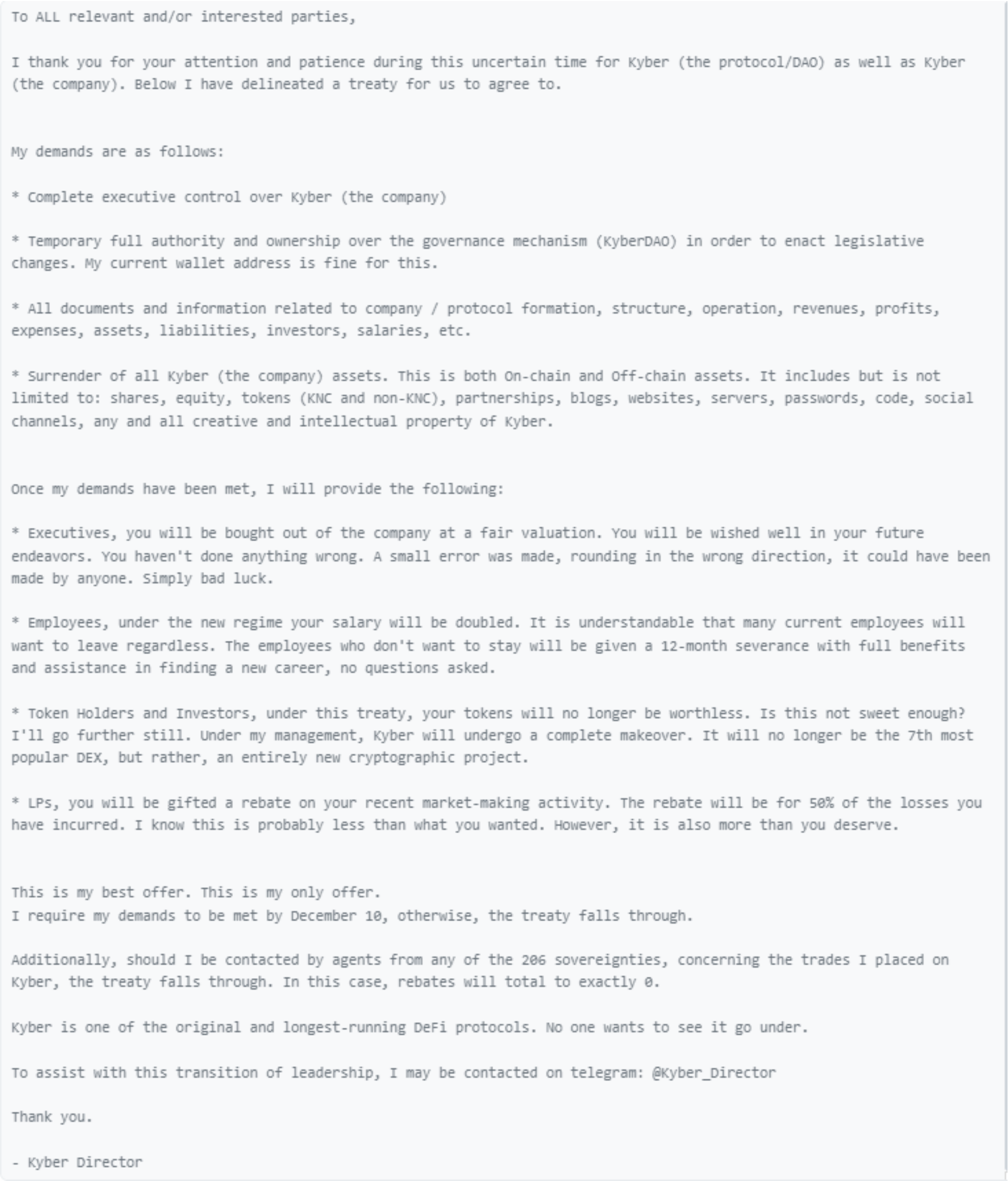
In 2023, there were 31 incidents where victims of attacks were able to recover all or part of their lost funds. In these 31 incidents, a total of approximately $384 million in stolen funds was involved, with about $297 million being returned, accounting for 77% of the stolen amount. Among these incidents, funds from 10 different protocols were fully recovered.



(Incidents of Fully Recovered Stolen Funds in 2023)

Whether it's through offering a bounty or negotiating for the return of stolen funds, there are mainly two ways of communication: one is making announcements on the project's media platforms, and the other is the attacker and the project team communicating through on-chain messages. Speaking of on-chain messaging, one must mention the most "absurd" and unprecedented on-chain negotiation case of the year — the KyberSwap Exploiter incident.

After the attack on November 23rd, the KyberSwap team engaged in negotiations with the hacker using on-chain messages. The KyberSwap team expressed willingness to pay a 10% white hat bounty. In response, the KyberSwap Exploiter issued a statement regarding the potential terms of the negotiation:



To ALL relevant and/or interested parties,

I thank you for your attention and patience during this uncertain time for Kyber (the protocol/DAO) as well as Kyber (the company). Below I have delineated a treaty for us to agree to.

My demands are as follows:

* Complete executive control over Kyber (the company)

* Temporary full authority and ownership over the governance mechanism (KyberDAO) in order to enact legislative changes. My current wallet address is fine for this.

* All documents and information related to company / protocol formation, structure, operation, revenues, profits, expenses, assets, liabilities, investors, salaries, etc.

* Surrender of all Kyber (the company) assets. This is both On-chain and Off-chain assets. It includes but is not limited to: shares, equity, tokens (KNC and non-KNC), partnerships, blogs, websites, servers, passwords, code, social channels, any and all creative and intellectual property of Kyber.

Once my demands have been met, I will provide the following:

* Executives, you will be bought out of the company at a fair valuation. You will be wished well in your future endeavors. You haven't done anything wrong. A small error was made, rounding in the wrong direction, it could have been made by anyone. Simply bad luck.

* Employees, under the new regime your salary will be doubled. It is understandable that many current employees will want to leave regardless. The employees who don't want to stay will be given a 12-month severance with full benefits and assistance in finding a new career, no questions asked.

* Token Holders and Investors, under this treaty, your tokens will no longer be worthless. Is this not sweet enough? I'll go further still. Under my management, Kyber will undergo a complete makeover. It will no longer be the 7th most popular DEX, but rather, an entirely new cryptographic project.

* LPs, you will be gifted a rebate on your recent market-making activity. The rebate will be for 50% of the losses you have incurred. I know this is probably less than what you wanted. However, it is also more than you deserve.

This is my best offer. This is my only offer.
I require my demands to be met by December 10, otherwise, the treaty falls through.

Additionally, should I be contacted by agents from any of the 206 sovereignties, concerning the trades I placed on Kyber, the treaty falls through. In this case, rebates will total to exactly 0.

Kyber is one of the original and longest-running DeFi protocols. No one wants to see it go under.

To assist with this transition of leadership, I may be contacted on telegram: @Kyber_Director

Thank you.

- Kyber Director

In this on-chain statement, the KyberSwap Exploiter proposed a series of settlement conditions. These included complete executive control over the Kyber company, temporary full control of KyberDAO's governance mechanism to implement legislative changes, and a demand for all documents and information related to the company/protocol. Additionally, the Kyber company was asked to hand over all on-chain and off-chain assets. The KyberSwap Exploiter promised a series of compensation measures for the company's executives, employees, token holders, and investors once the demands were met. This included providing a fair valuation buyout for senior executives, doubling employee salaries, offering 12 months of severance pay and comprehensive benefits for employees who chose not to stay, and guaranteeing the value of investors' tokens. The attacker emphasized that if their demands were not met by December 10th or if there was any contact from agents of sovereign states, the settlement agreement would be considered void. In the statement, the KyberSwap Exploiter also referred to themselves as the Kyber Director.

According to the latest updates from the KyberSwap team, they have contacted the controller of the frontrunning bots and negotiated the return of 90% of the funds obtained by the bots. So far, the KyberSwap team has received approximately $5.17 million worth of funds returned by the controller of the frontrunning bots.

To learn how to leave on-chain messages, you can refer to our article here.

3.3 Profile and Activities of Hacker Groups

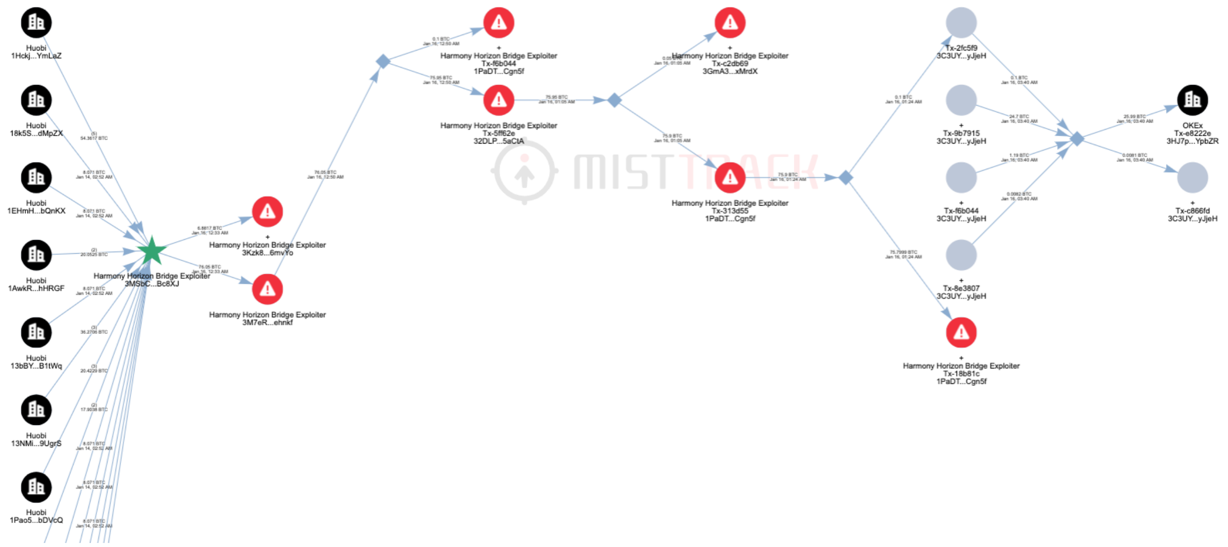
3.3.1 The Lazarus Group

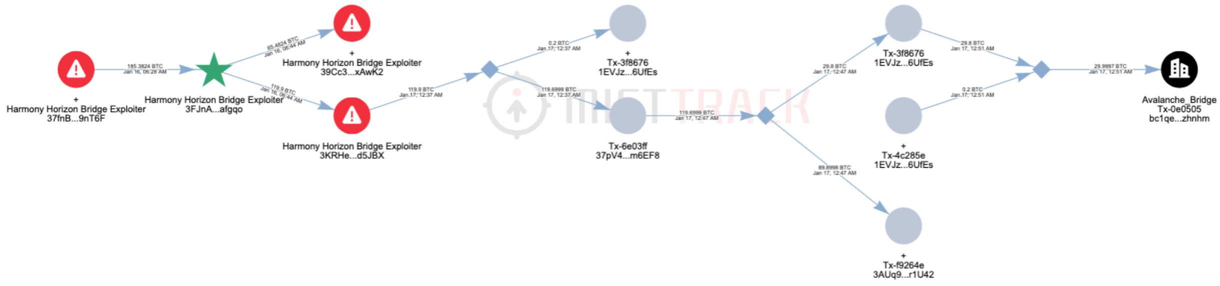
Based on public information available in 2023, as of June, no major cryptocurrency thefts had been attributed to the North Korean hacker group Lazarus Group for that year. Their activities, according to on-chain data, mainly involved laundering the cryptocurrencies stolen in 2022, including approximately $100 million taken in the Harmony cross-chain bridge attack on June 23, 2022.

Following the Harmony cross-chain bridge attack on June 23, 2022, the stolen funds were deposited directly into the Tornado Cash mixing protocol and then withdrawn to a batch of new addresses, with no further movement observed after that.

The Lazarus Group's activities in laundering the cryptocurrencies stolen from the Harmony cross-chain incident in 2022 are as follows:

- After a period of inactivity lasting nearly half a year, the hackers began withdrawing funds from Tornado Cash between January 13th and 16th, 2023. They conducted deposit and withdrawal operations within the privacy network Railgun, after which some of the funds were transferred to trading platforms and withdrawn to the BTC network.





- In the days following January 16th, the hackers further diversified the funds withdrawn to the BTC network through multiple layers of transfers. Some of the funds were again moved to various trading platforms, while others were transferred to the Avalanche chain via the Avalanche Bridge, eventually being converted into USDT/USDD, and then moved to mixing networks on the ETH/TRON chains.

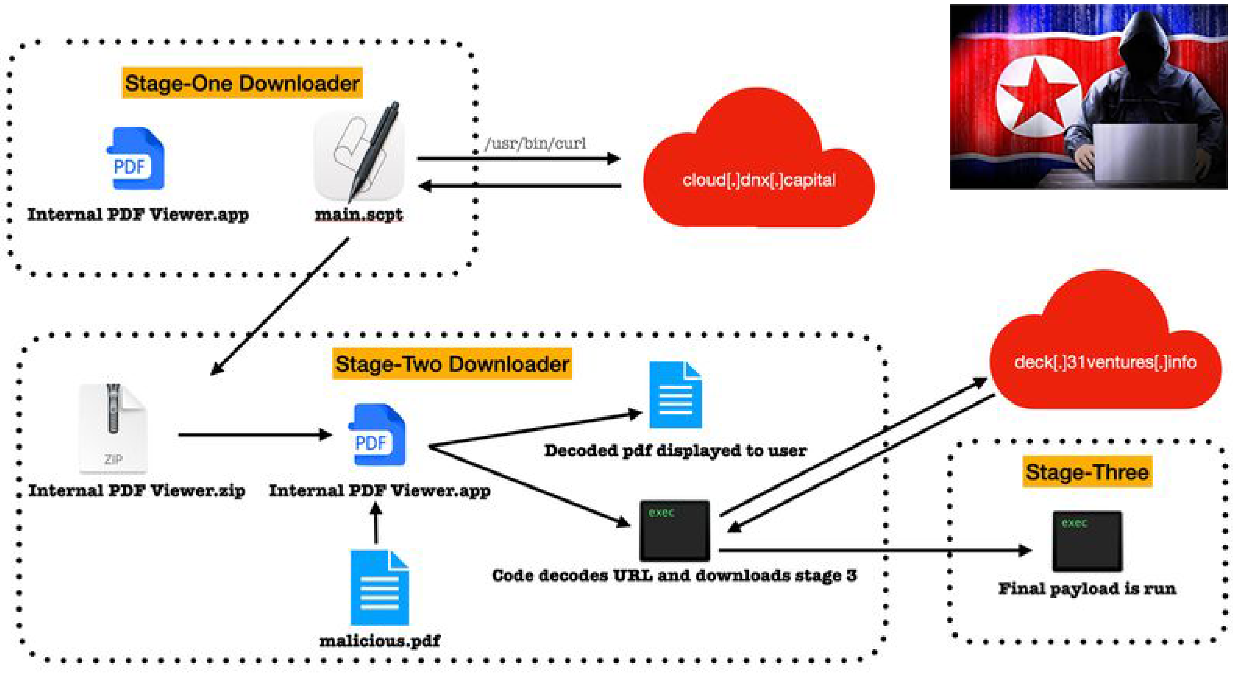
Subsequent events revealed that in addition to laundering the cryptocurrencies stolen in 2022, the North Korean hacker group Lazarus Group was also actively engaged in other activities, including carrying out Advanced Persistent Threat (APT) related attacks. These activities led to what the cryptocurrency industry refers to as the “Dark 101 Days” starting June 3rd.

During the "Dark 101 Days," a total of 5 platforms were compromised, with the stolen amount exceeding $300 million. Most of the targets were centralized service platforms.

Date	Event	Amont	Link
June 3rd	Atomic Wallet Hack	Over $100M USD	Link
July 22nd	Coinspaid Hot Wallet Breach	$37.3M USD	Link
July 23rd	Alphapo Hot Wallet Hacked	$60M USD	Link
Sept 4	Stake.com Incident	$41M USD	Link
Sept 12th	CoinEx Hot Wallet Private Key Leak	$70M USD	Link
	Total	$308.3M USD	

Around September 12, SlowMist, in collaboration with its partners, identified a large-scale Advanced Persistent Threat (APT) attack on the cryptocurrency industry, orchestrated by the hacker group Lazarus Group. The attack method was as follows:

Initially, the attackers impersonated legitimate identities, fooling the verification staff through real-person authentication to become bona fide customers, followed by authentic deposits. Utilizing this customer identity as a cover, the attackers targeted official personnel at specific communication intervals between various officials and customers (attackers). They then precisely deployed custom-made Trojans for Mac or Windows to these officials, gaining unauthorized access. Once access was secured, they moved laterally within the network, remaining undetected for extended periods, ultimately achieving their goal of stealing funds.



The United States Federal Bureau of Investigation (FBI) has been closely monitoring significant theft cases within the cryptocurrency ecosystem and has issued public press releases to attribute responsibility for these events to the North Korean hacker group Lazarus Group. Here are some key press releases by the FBI in 2023 regarding the Lazarus Group's involvement in major crypto thefts:

- January 23rd: FBI confirmed that the North Korean hacker group Lazarus Group was responsible for the Harmony Hack incident.
- August 22nd: FBI issued a notice stating that the North Korean hacker organization was involved in the hacking attacks on Atomic Wallet, Alphapo, and CoinsPaid, collectively stealing $197 million in cryptocurrencies.
- September 6th: FBI issued a press release confirming that the North Korean hacker group Lazarus Group was responsible for the theft of $41 million from Stake.com, a cryptocurrency gambling platform.

According to our analysis, the money laundering methods used by the North Korean hacker group Lazarus Group have been continuously evolving over time, with new techniques emerging periodically. The timeline for changes in their money laundering methods is detailed in the following table:

Timeline	Incident	New Methods of Money Laundering
January	Harmony Bridge Hack	ETH Chain: Stolen funds -> Tornado Cash -> Railgun -> Several exchanges (e.g., Binance, OKX, Huobi) -> BTC Chain: Withdrawal from exchanges -> Avalanche Bridge -> Avalanche Chain: After cross-chain transfer -> Convert to ETH Token using 1inch trading aggregator's limit order feature -> Bridge -> ETH Chain: 1. After cross-chain transfer -> Convert to USDT Token using 1inch trading aggregator's limit order feature -> ETH money laundering network 2. After cross-chain transfer -> Convert to USDD Token using 1inch trading aggregator's limit order feature -> BitTorrent Bridge -> Tron Chain: After cross-chain transfer -> Multiple transfers -> Tron money laundering network
June	Atomic Wallet Hack	ETH Chain: Stolen token funds -> MetaMask Swap -> ETH -> WETH -> Malicious contract -> ETH -> WETH -> Avalanche Bridge
July		ETH Chain: Stolen token funds -> Uniswap -> ETH -> WETH -> Avalanche Bridge ->

	Coinspaid Hot Wallet Breach	Avalanche Chain: Withdrawal from Avalanche Bridge -> 1inch -> BTC Token -> Bridge BTC Chain: Withdrawal from Bridge -> Sinbad Mixer
July	Alphapo Hot Wallet Hack	Tron Chain: Stolen token funds -> Sunswap -> TRX funds -> TransitSwap -> ETH Chain: Overlap of funds with (1) Stake.com crypto gambling platform theft and (2) CoinEx hot wallet private key leak across different chains
September	Stake.com Incident	BSC Chain: Stolen token funds -> 1inch / Biswap / Pancakeswap -> BNB -> Swft cross-chain -> Tron Chain: After Swft cross-chain, funds -> USDT-TRC20 -> Swft cross-chain -> BSC Chain: After Swft cross-chain, funds -> BNB -> BSC: Token Hub -> BNB Chain -> Thorchain -> BTC Network
September	CoinEx Hot Wallet Private Key Leak	Tron Chain: Stolen token funds -> Sunswap -> TRX -> Sunswap -> USDT -> Hieswap / BitTorrent -> BSC Chain: Withdrawal from Hieswap / BitTorrent -> USDT-BEP20 -> Stargate -> USDT-ERC20 -> Thorchain -> BTC Chain: Funds after Thorchain cross-chain -> BTC -> Swft and other cross-chain bridges Tron Chain: After Swft cross-chain, funds ->

		USDT-TRC20 -> Tron chain OTC addresses
September	Money Laundering Harmony cross-chain bridge attack incident	Funds transferred to a Russian exchange for laundering

Leveraging the extensive intelligence support from partners in the InMist Intelligence Network, the SlowMist AML (Anti-Money Laundering) team conducted follow-up analyses on the data related to theft incidents involving the hacker group Lazarus Group. This led to the partial profiling of the group, revealing key characteristics and information:

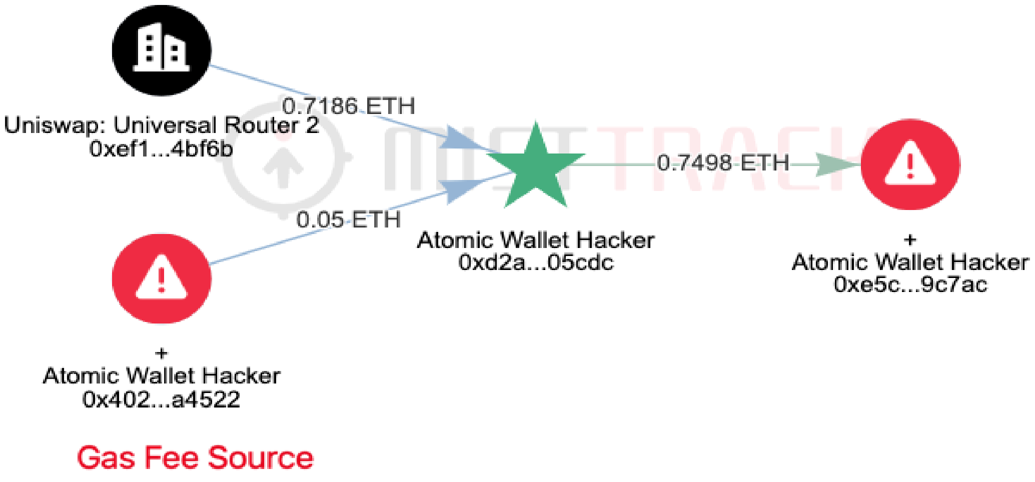
1. They often use European and Turkish identities for disguise.
2. The team has acquired several pieces of crucial information, including:
   - Dozens of IP addresses
   - Numerous email addresses
   - Partially anonymized identity information

The following are examples of the IP addresses linked to the Lazarus Group (note that the specific details are partially masked for security and privacy reasons):

- 111.*.*.49
- 103.*.*.162
- 103.*.*.205
- 210.*.*.9
- 103.*.*.29
- 103.*.*.163
- 154.*.*.10
- 185.*.*.217

Analysis and sharing of event details related to the hacker group Lazarus Group are as follows:

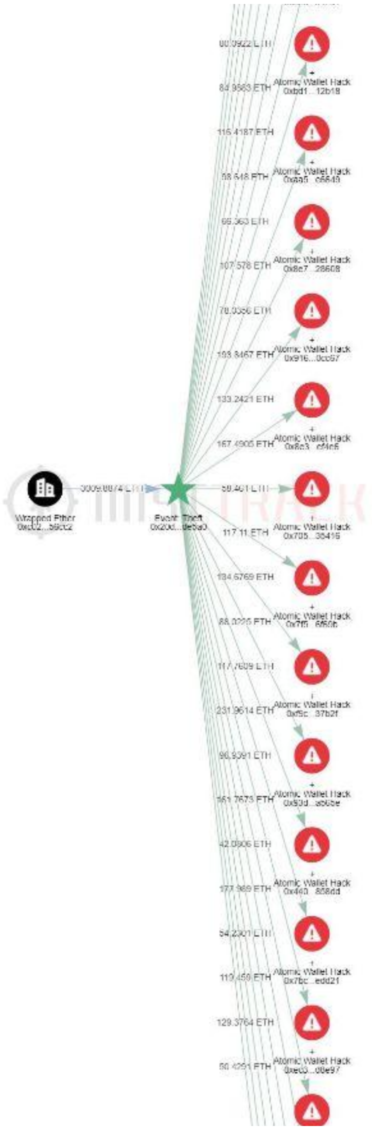
- Atomic Wallet Incident



On June 3, several users of Atomic Wallet reported on social media that their wallet assets had been stolen. It was estimated that the total amount stolen had reached $100 million. Investigations identified 142 new suspicious addresses linked to the hackers. By June 9, the investigation revealed a pattern in the funds transfer by the Atomic Wallet hackers that was similar to strategies previously used by the Lazarus Group. The pattern involved hackers transferring token-type funds from the stolen user addresses to new addresses, and then converting all token-type funds into the base asset of the chain (ETH for the Ethereum chain and TRX for the Tron chain), using platforms such as Uniswap, MetaMask Swap, and Sunswap.

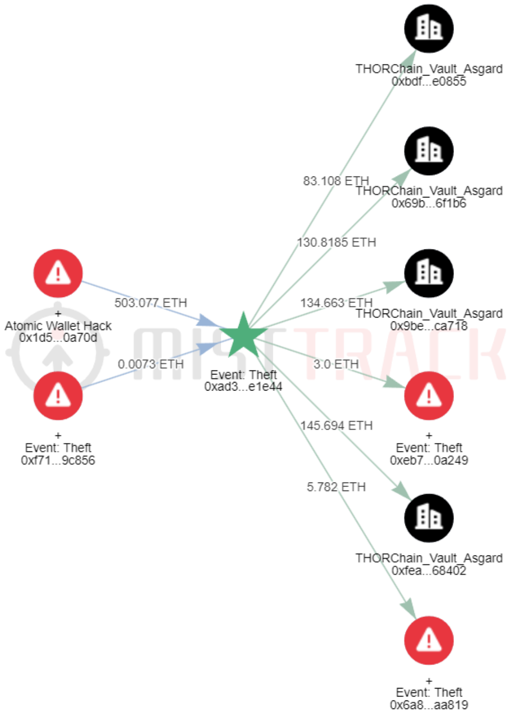
According to MistTrack, three primary money laundering methods were identified:

1. The hackers deployed two exchange contracts. The first one exchanged ETH for WETH, and the second exchanged WETH back to ETH. The converted ETH was then dispersed to multiple addresses, exchanged again for WETH, and transferred across chains to Avalanche. Finally, WETH was exchanged for BTC, and the funds were transferred from the Avalanche chain to the BTC network.

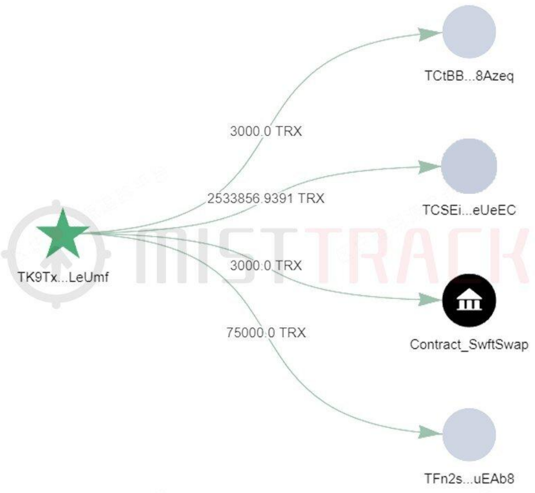


80.0922 ETH
Atomic Wallet Hack 0xbd1...12b18
84.9563 ETH
116.4187 ETH
Atomic Wallet Hack 0x8a5...c6649
58.648 ETH
66.363 ETH
Atomic Wallet Hack 0x8e7...28608
107.578 ETH
78.0356 ETH
Atomic Wallet Hack 0x916...0cc67
193.8467 ETH
133.2421 ETH
Atomic Wallet Hack 0x8c3...cf4c6
167.4905 ETH
Wrapped Ether 0xc02...56cc2
3009.8874 ETH
Event: Theft 0x20d...de5a0
59.461 ETH
Atomic Wallet Hack 0x705...35416
117.11 ETH
184.6769 ETH
Atomic Wallet Hack 0x7f5...6f60b
88.0226 ETH
117.7609 ETH
Atomic Wallet Hack 0xf5c...37b2f
231.9614 ETH
96.9391 ETH
Atomic Wallet Hack 0x93d...a565e
161.7673 ETH
42.0906 ETH
Atomic Wallet Hack 0x440...858dd
177.989 ETH
54.2301 ETH
Atomic Wallet Hack 0x7bc...edd21
119.459 ETH
129.3764 ETH
Atomic Wallet Hack 0xe03...d8e97
90.4291 ETH
MISTTRACK

2) ETH to THORChain Transfer and Conversion to BTC: Hackers transferred ETH to THORChain, where they exchanged it for BTC, and then moved the BTC to BTC addresses. Additionally, they used SwftSwap for cross-chain transactions.

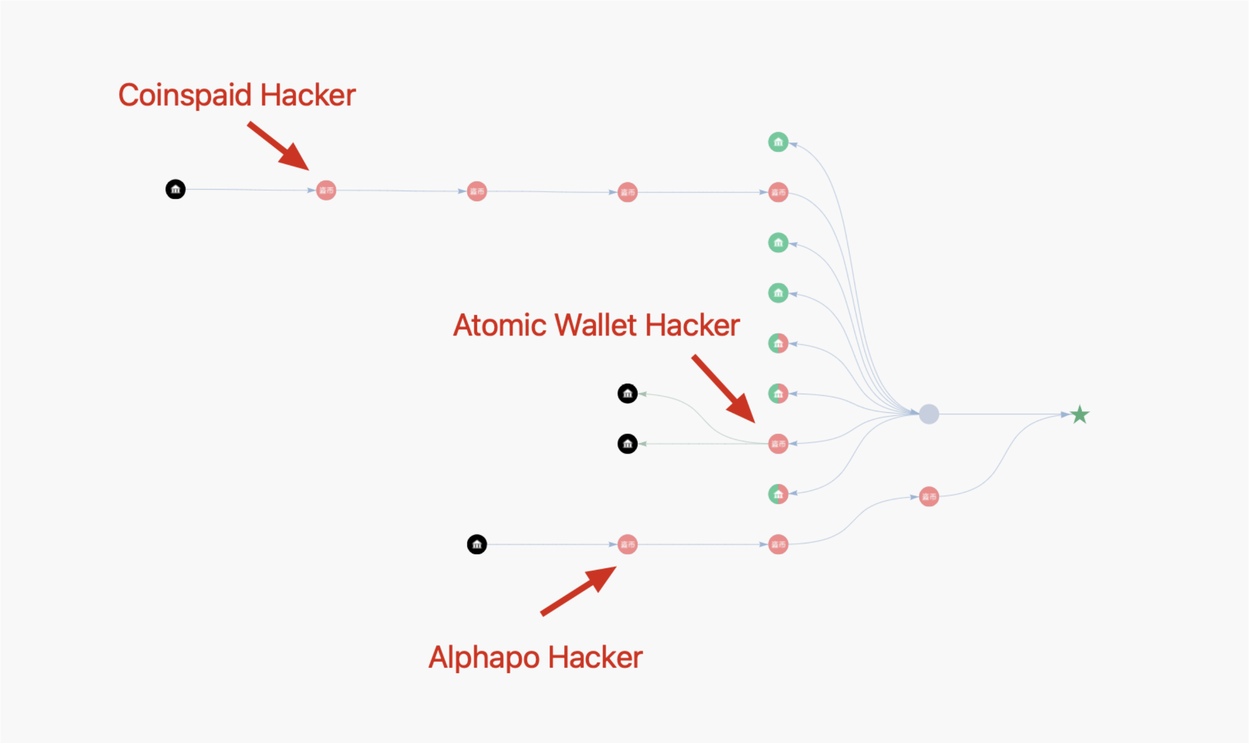


3) Swap and transfer of USDT through SunSwap: Hackers converted a majority of USDT into TRX using SunSwap and accumulated it at a specific TRON address. From there, the TRX was dispersed to multiple addresses, with most of it being transferred to exchange platforms for deposit. A portion of the TRX was exchanged back to USDT using SunSwap, with most of this USDT being dispersed to various trading platforms and some being transferred cross-chain using SwftSwap.



- Coinspaid Hot Wallet Unauthorized Withdrawals

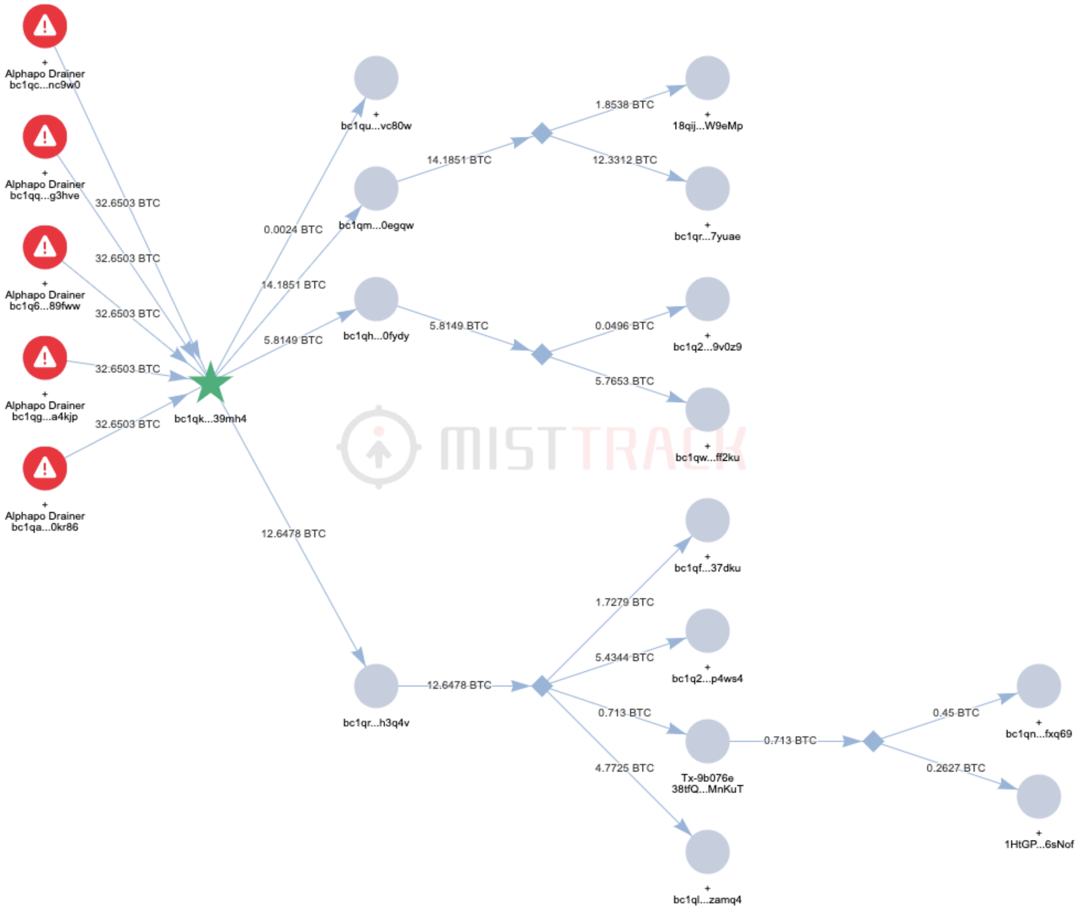
During the CoinsPaid attack on July 22, 2023, the suspected hacker group Lazarus Group impersonated recruiters and targeted CoinsPaid employees with recruitment emails and LinkedIn messages. CoinsPaid reported that the suspected Lazarus Group spent six months attempting to gain access to their network. The subsequent movement of stolen funds from Coinspaid's hot wallet showed overlaps with the funds from the theft of assets from multiple Atomic Wallet users and the theft from the Alphapo hot wallet.



- Alphapo Hot Wallet Hack

On July 23, following the theft of the Alphapo hot wallet, the hacker transferred the stolen funds through multiple cross-chain layers, eventually withdrawing them on the BTC network. The funds were then once again exchanged through a cross-chain bridge, converting BTC into USDT-TRC20 and withdrawing it on the TRON network. For instance, the path for converting stolen funds on the

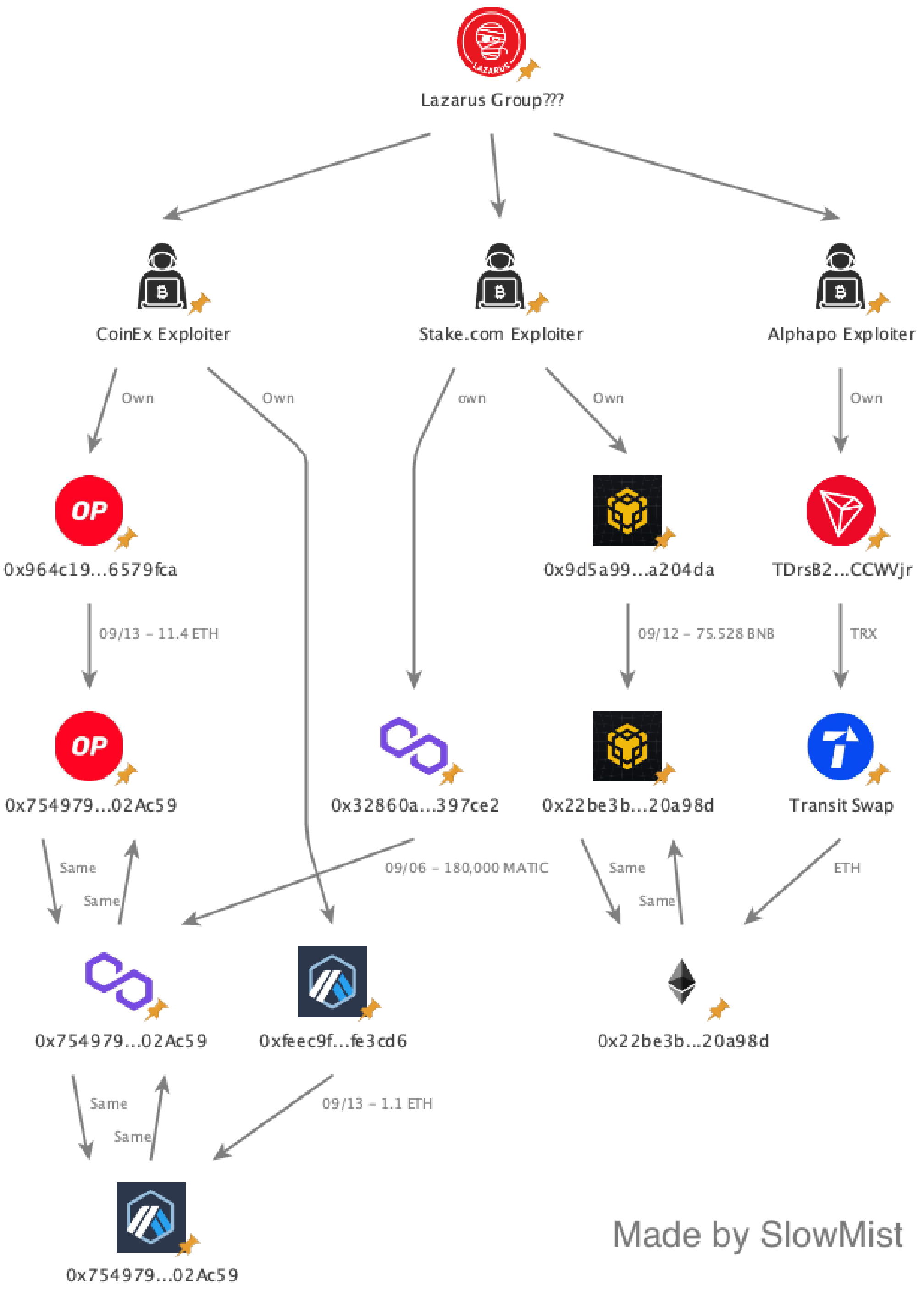
Ethereum chain was as follows: Ethereum Chain -[via Avalanche Bridge]-> Avalanche Chain -[via Avalanche Bridge]-> Bitcoin Network.



- Stake.com Hack

According to the analysis by our AML team, there are overlaps in the subsequent movement of stolen funds from Stake.com with the funds involved in the theft of the Alphapo hot wallet and the leak of the CoinEx hot wallet private keys.

Specifically, on the Binance Smart Chain (BSC), the stolen BNB funds from the Stake.com cryptocurrency gambling platform were transferred to several ChangeNOW deposit addresses. Later, a portion of these stolen funds was exchanged through cross-chain platforms such as TransitSwap and Swft, and then moved to exchanges like Mexc.



- CoinEx Hot Wallet Hack

The CoinEx exchange experienced a hot wallet private key leak incident on September 13. Based on the chain analysis, the movement of the stolen funds overlapped with those involved in the theft of the Alphapo hot wallet and the Stake.com cryptocurrency gambling platform heist. The FBI previously confirmed on August 22 and September 6 that the hacker group Lazarus Group was responsible for the Alphapo and Stake.com theft incidents.

The laundering of the stolen funds from the CoinEx hot wallet leak incident occurred in multiple phases and exhibited different laundering behaviors across various chains.

Phase One: Transferring Funds to the BTC Network
- Tron Chain Stolen Funds: Tron chain stolen Token assets -> Sunswap -> TRX -> SunSwap -> USDT-TRC20 -> HieSwap/BitTorrent cross-chain bridge -> BSC Chain -> USDT-BEP20 -> Stargate cross-chain bridge -> ETH Chain -> USDT-ERC20 -> ThorChain cross-chain bridge -> Bitcoin -> Sinbad mixer.
- BSC Chain Stolen Funds: BSC chain stolen Token assets -> Pancakeswap -> BNB -> BSC: Token Hub -> BNB Chain -> Thorchain -> Bitcoin
- Solana Chain Stolen Funds: SOL -> Wormhole Bridge -> ETH Chain -> ETH -> Exchanges like Kucoin.
- Funds from other chains were cross-chain exchanged through exchanges like ChangeNOW, FixedFloat, Simpleswap, letsexchange.

Phase Two: Transferring Funds from the BTC Network to the Tron Chain OTC
- BTC -> Swft/Other cross-chain platforms -> Tron Chain -> USDT-TRC20 -> Suspected OTC

Phase Three: Withdrawing from Sinbad Mixer -> BTC -> Thorchain -> ETH Chain.

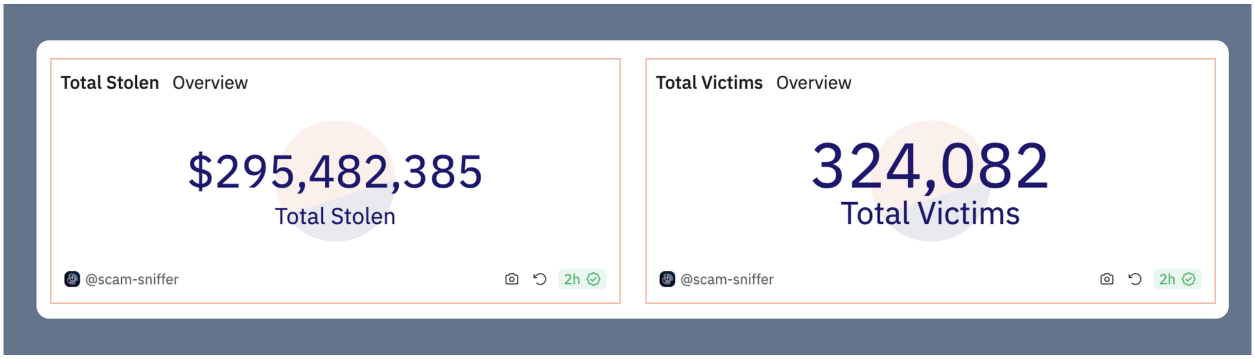
3.3.2 Phishing Groups: Wallet Drainers

Note: This section is written by the Scam Sniffer team.

- **Overview**

Wallet Drainers, a type of cryptocurrency-related malware, have achieved notable "success" in the past year. These software programs are deployed on phishing websites to deceive users into signing malicious transactions, thereby stealing assets from their cryptocurrency wallets. These phishing activities continuously target ordinary users in various forms, leading to significant financial losses for many who unwittingly sign these malicious transactions.

- **Stolen Fund Statistics**



Total Stolen Overview

$295,482,385

Total Stolen

@scam-sniffer

Total Victims Overview

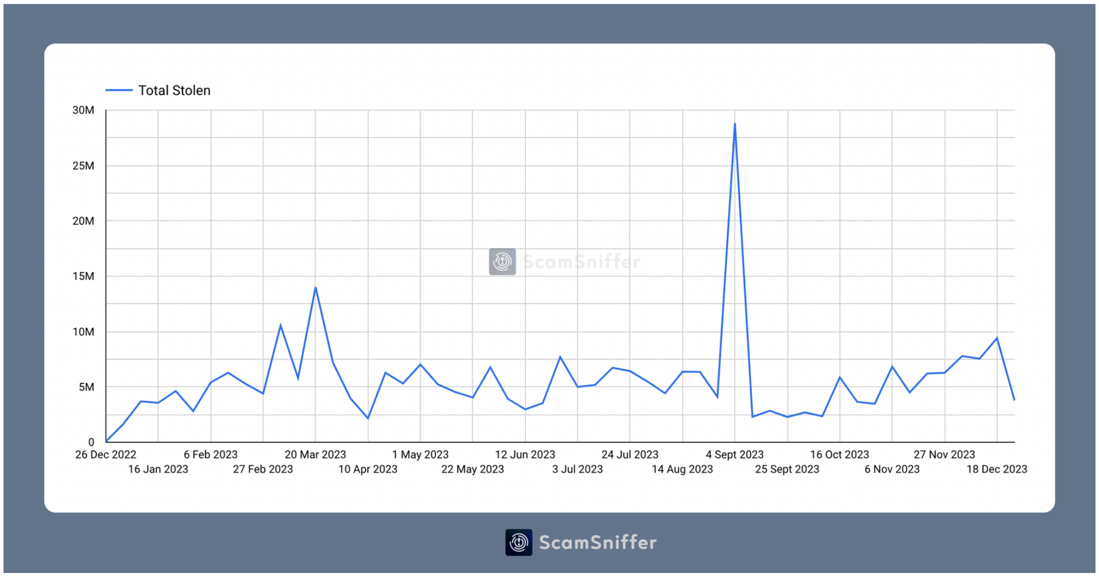
324,082

Total Victims

@scam-sniffer

Over the past year, Scam Sniffer has monitored these Wallet Drainers and identified that they have stolen nearly $295 million in assets from approximately 324K victims.

- **Trends**



Notably, on March 11, nearly $7 million was stolen, primarily due to fluctuations in the USDC exchange rate and phishing sites impersonating Circle. There was also a significant spike in thefts around March 24, coinciding with the compromise of Arbitrum's Discord and subsequent airdrop events.

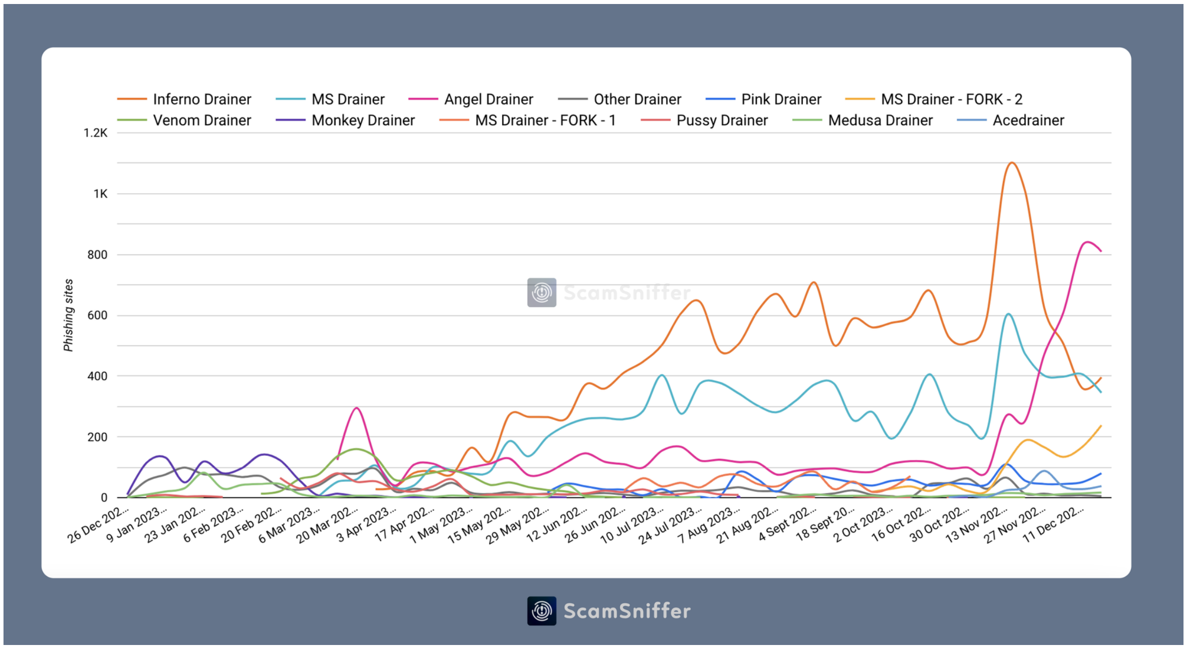
Each peak in thefts is associated with community-wide events, which could be airdrops or hacking incidents.

- **Noteworthy Wallet Drainers**

Drainer	Total Stolen	Victims	Source	Appeared time
Inferno Drainer	$81 million	134k	View	March, 2023
MS Drainer	$59 million	63k	View	March, 2023
Angel Drainer	$20 million	30k	View	March, 2023
Monkey Drainer	$16 million	18K	View	August, 2022
Venom Drainer	$27 million	15k	View	January, 2023
Pink Drainer	$18 million	9k	View	March, 2023
Pussy Drainer	$15 million	4k	View	January, 2023

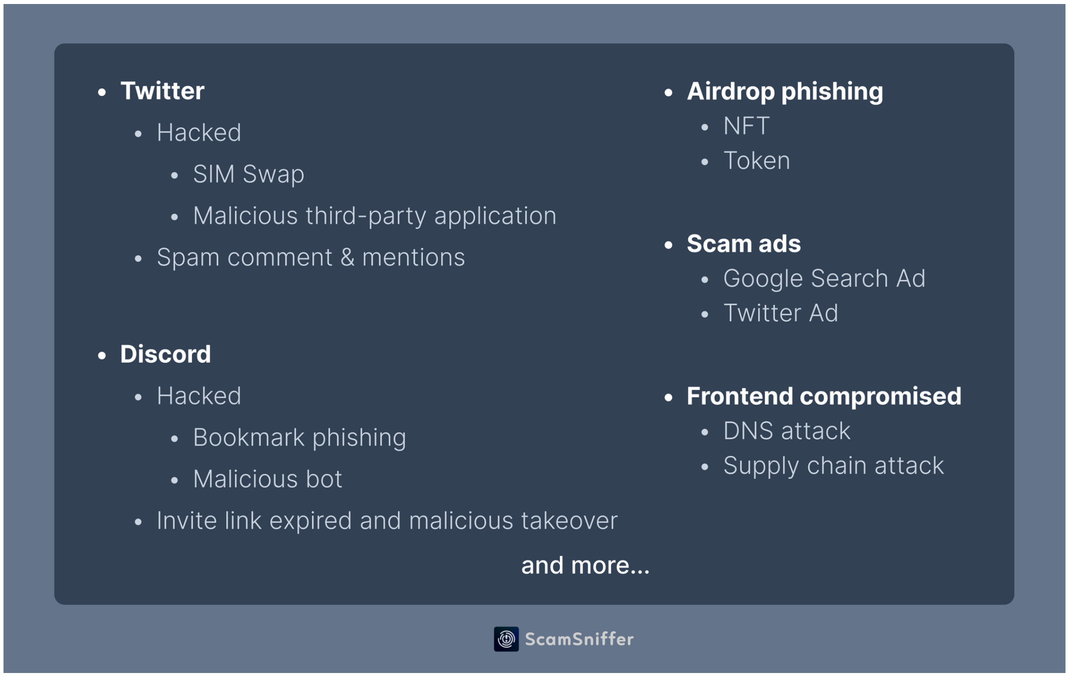
After ZachXBT exposed Monkey Drainer, they announced their exit after being active for 6 months. Venom then took over most of their clientele. Subsequently, MS, Inferno, Angel, and Pink emerged around March. With Venom ceasing operations around April, most phishing groups shifted to using other services. With a 20% Drainer fee, they made at least $47 million by selling these services.

- **Wallet Drainers Trends**



Analysis of the trend shows that phishing activities have been consistently growing. Moreover, each time a Drainer exits, a new one replaces it, such as Angel emerging as a replacement after Inferno announced its departure.

- **How do they initiate phishing activities?**



- **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
- **Frontend compromised**
  - DNS attack
  - Supply chain attack

and more...

ScamSniffer

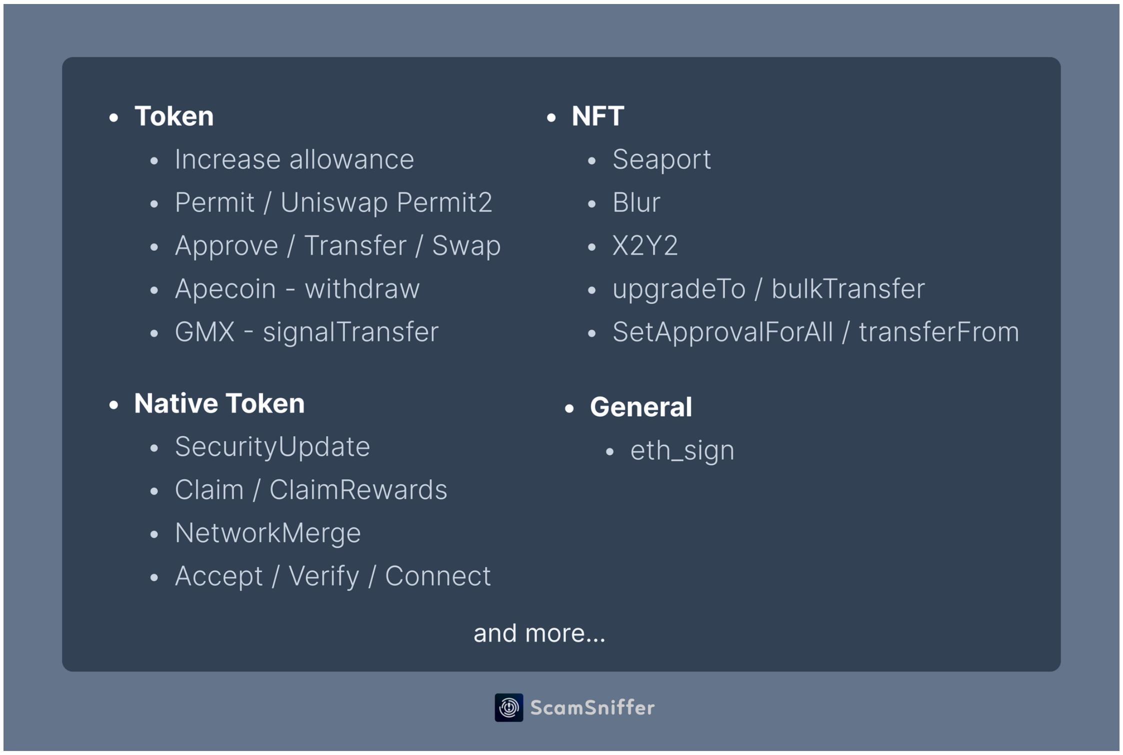
These phishing websites mainly acquire traffic through several methods:

- Hacker Attacks:
    - Official project Discord and Twitter accounts being hacked
    - Attacks on the front end of official projects or the libraries they use
- Organic Traffic
    - Airdropping NFTs or Tokens
    - Exploiting expired Discord links
    - Spam reminders and comments on Twitter
- Paid Traffic
    - Google ad search
    - Twitter ads

Although hacker attacks have a wide impact, the community often reacts promptly, typically within 10-50 minutes. In contrast, airdrops, organic traffic, paid advertising, and exploiting expired Discord links are less noticeable.

Additionally, there are more targeted phishing methods such as personal direct message phishing.

- **Common Phishing Signatures**



- **Token**
  - Increase allowance
  - Permit / Uniswap Permit2
  - Approve / Transfer / Swap
  - Apecoin - withdraw
  - GMX - signalTransfer
- **Native Token**
  - SecurityUpdate
  - Claim / ClaimRewards
  - NetworkMerge
  - Accept / Verify / Connect
- **NFT**
  - Seaport
  - Blur
  - X2Y2
  - upgradeTo / bulkTransfer
  - SetApprovalForAll / transferFrom
- **General**
  - eth_sign

and more...

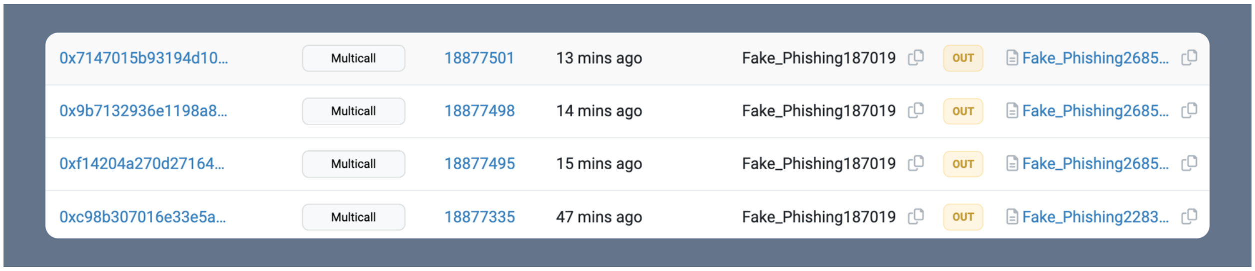
ScamSniffer

Different asset types are targeted with specific malicious phishing signature methods. The type of assets held in a victim's wallet determines the kind of phishing signature initiated.

For instance, from the case of exploiting GMX's signalTransfer to steal Reward LP tokens, it's evident that the phishing techniques have become highly sophisticated and tailored for specific assets.

- **Increase Use of Smart Contracts**

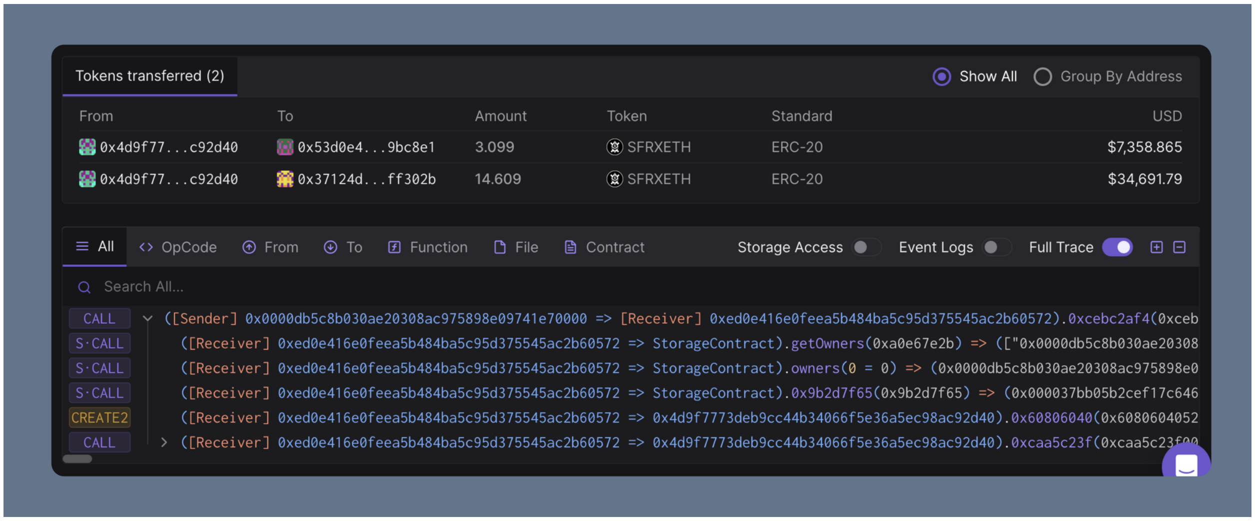
1) Multicall



0x7147015b93194d10...	Multicall	18877501	13 mins ago	Fake_Phishing187019	OUT	Fake_Phishing2685...
0x9b7132936e1198a8...	Multicall	18877498	14 mins ago	Fake_Phishing187019	OUT	Fake_Phishing2685...
0xf14204a270d27164...	Multicall	18877495	15 mins ago	Fake_Phishing187019	OUT	Fake_Phishing2685...
0xc98b307016e33e5a...	Multicall	18877335	47 mins ago	Fake_Phishing187019	OUT	Fake_Phishing2283...

Starting with Inferno, there has been an increased focus on using contract technology. For instance, in cases where splitting transaction fees requires two separate transactions, the process might not be fast enough. This could allow the victim to revoke authorization before the second transfer. To enhance efficiency, they began using multicall for more effective asset transfers.

2) CREATE2 & CREATE



Tokens transferred (2) ● Show All ○ Group By Address

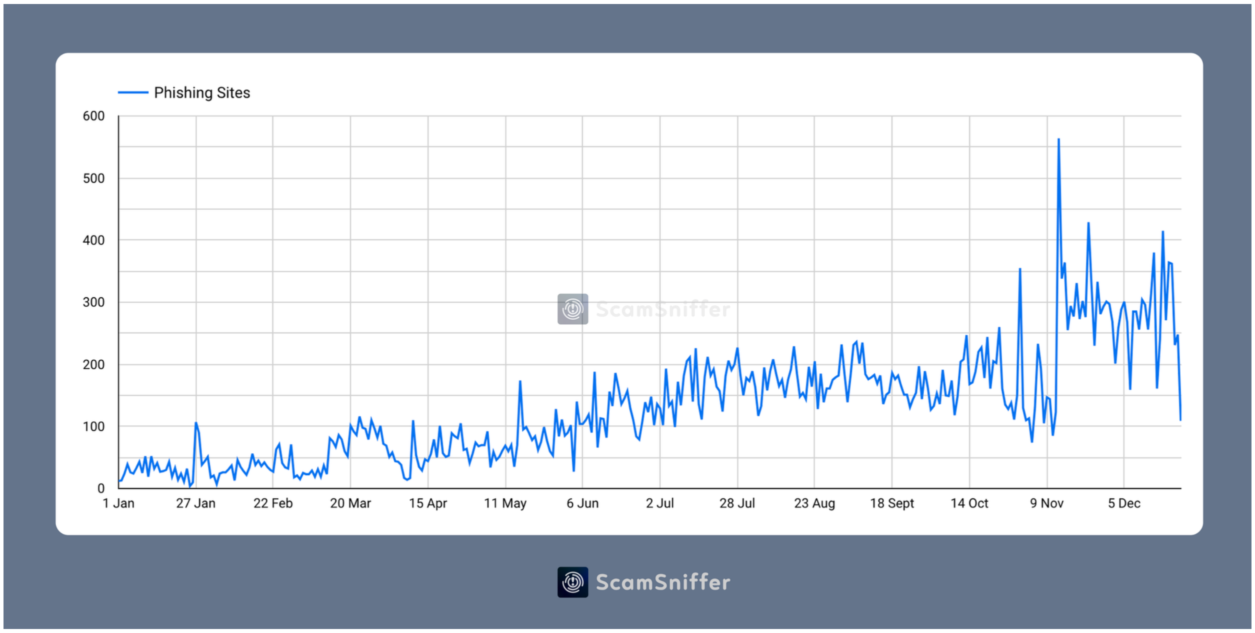
From	To	Amount	Token	Standard	USD
0x4d9f77...c92d40	0x53d0e4...9bc8e1	3.099	SFRXETH	ERC-20	$7,358.865
0x4d9f77...c92d40	0x37124d...ff302b	14.609	SFRXETH	ERC-20	$34,691.79

```
CALL      ⌄ ([Sender] 0x0000db5c8b030ae20308ac975898e09741e70000 => [Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572).0xcebc2af4(0xceb
S·CALL       ([Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572 => StorageContract).getOwners(0xa0e67e2b) => (["0x0000db5c8b030ae20308
S·CALL       ([Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572 => StorageContract).owners(0 = 0) => (0x0000db5c8b030ae20308ac975898e0
S·CALL       ([Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572 => StorageContract).0x9b2d7f65(0x9b2d7f65) => (0x000037bb05b2cef17c646
CREATE2      ([Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572 => 0x4d9f7773deb9cc44b34066f5e36a5ec98ac92d40).0x60806040(0x6080604052
CALL       > ([Receiver] 0xed0e416e0feea5b484ba5c95d375545ac2b60572 => 0x4d9f7773deb9cc44b34066f5e36a5ec98ac92d40).0xcaa5c23f(0xcaa5c23f00
```

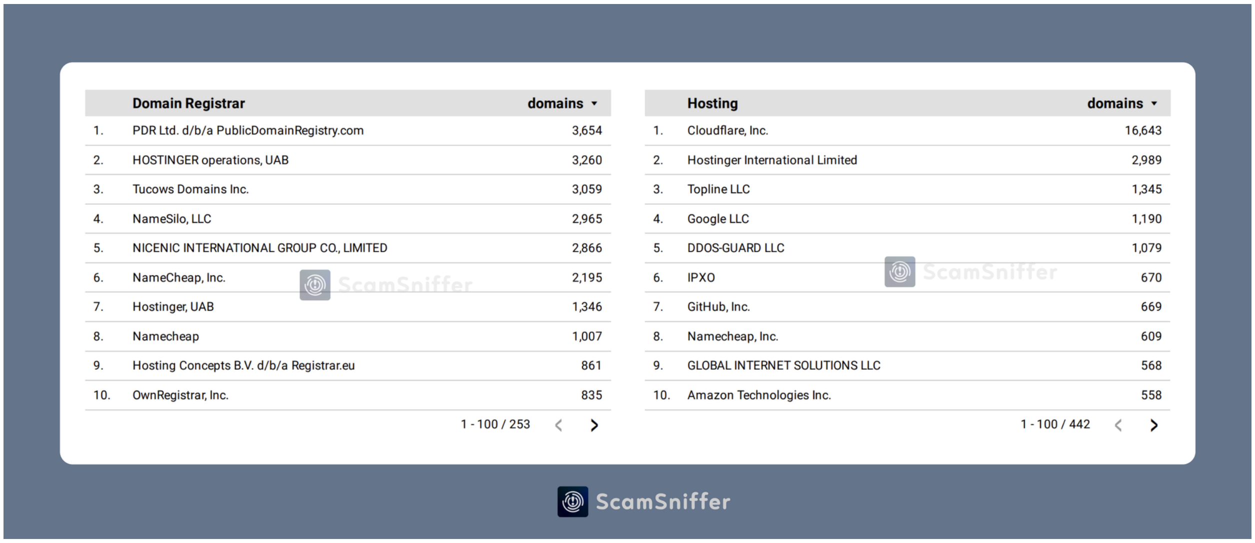
To bypass some wallet security checks, they also started experimenting with create2 or create to dynamically generate temporary addresses. This approach renders wallet-based blacklists ineffective and complicates research into phishing activities. Since you can't know where the assets will be transferred without signing, and temporary addresses don't offer much analytical value, this poses a significant challenge.

This marks a substantial change compared to last year.

- **Phishing Website**



Analyzing the number of phishing websites reveals a steady monthly increase in phishing activities, closely tied to the availability of stable wallet drainer services.



	Domain Registrar	domains ▾
1.	PDR Ltd. d/b/a PublicDomainRegistry.com	3,654
2.	HOSTINGER operations, UAB	3,260
3.	Tucows Domains Inc.	3,059
4.	NameSilo, LLC	2,965
5.	NICENIC INTERNATIONAL GROUP CO., LIMITED	2,866
6.	NameCheap, Inc.	2,195
7.	Hostinger, UAB	1,346
8.	Namecheap	1,007
9.	Hosting Concepts B.V. d/b/a Registrar.eu	861
10.	OwnRegistrar, Inc.	835

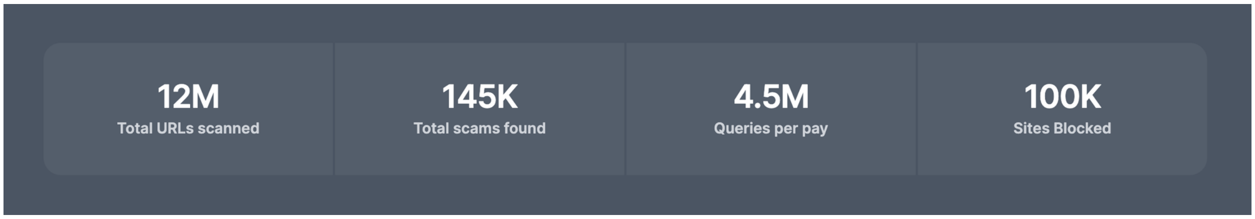
1 - 100 / 253

	Hosting	domains ▾
1.	Cloudflare, Inc.	16,643
2.	Hostinger International Limited	2,989
3.	Topline LLC	1,345
4.	Google LLC	1,190
5.	DDOS-GUARD LLC	1,079
6.	IPXO	670
7.	GitHub, Inc.	669
8.	Namecheap, Inc.	609
9.	GLOBAL INTERNET SOLUTIONS LLC	568
10.	Amazon Technologies Inc.	558

1 - 100 / 442

The domains used by these phishing websites are mainly registered with specific domain registrars. Analysis of server addresses shows that most use Cloudflare to hide their real server locations.

Over the past year, Scam Sniffer scanned nearly 12 million URLs and identified about 145,000 malicious URLs, serving 400 million queries daily. Scam Sniffer's open-source blacklist currently contains nearly 100,000 malicious domains, which are continuously pushed to platforms like Chainabuse.



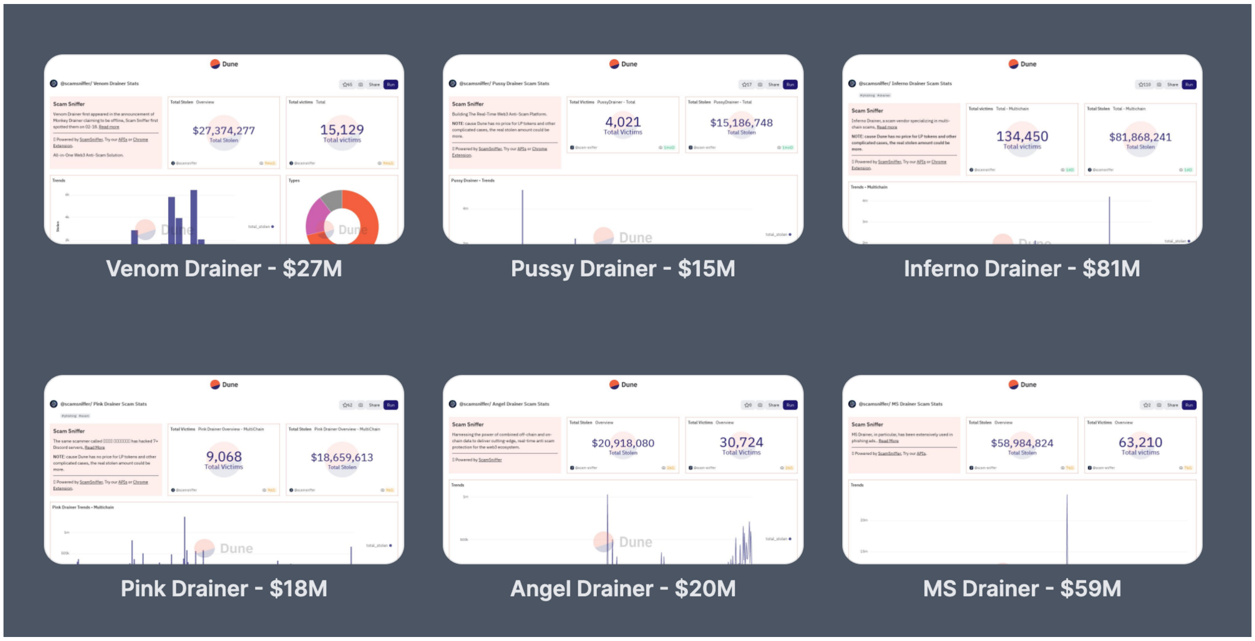
12M
Total URLs scanned

145K
Total scams found

4.5M
Queries per pay

100K
Sites Blocked

As a Web3 anti-fraud platform, Scam Sniffer is dedicated to providing a secure Web3 environment for the next billion users. They have reported on several well-known Wallet Drainers and continuously share information about major theft cases on social media platforms to raise public awareness about phishing. Scam Sniffer has already assisted some well-known platforms in protecting their users. Interested parties can contact them at b2b@ScamSniffer.io.



Venom Drainer - $27M

Pussy Drainer - $15M

Inferno Drainer - $81M

Pink Drainer - $18M

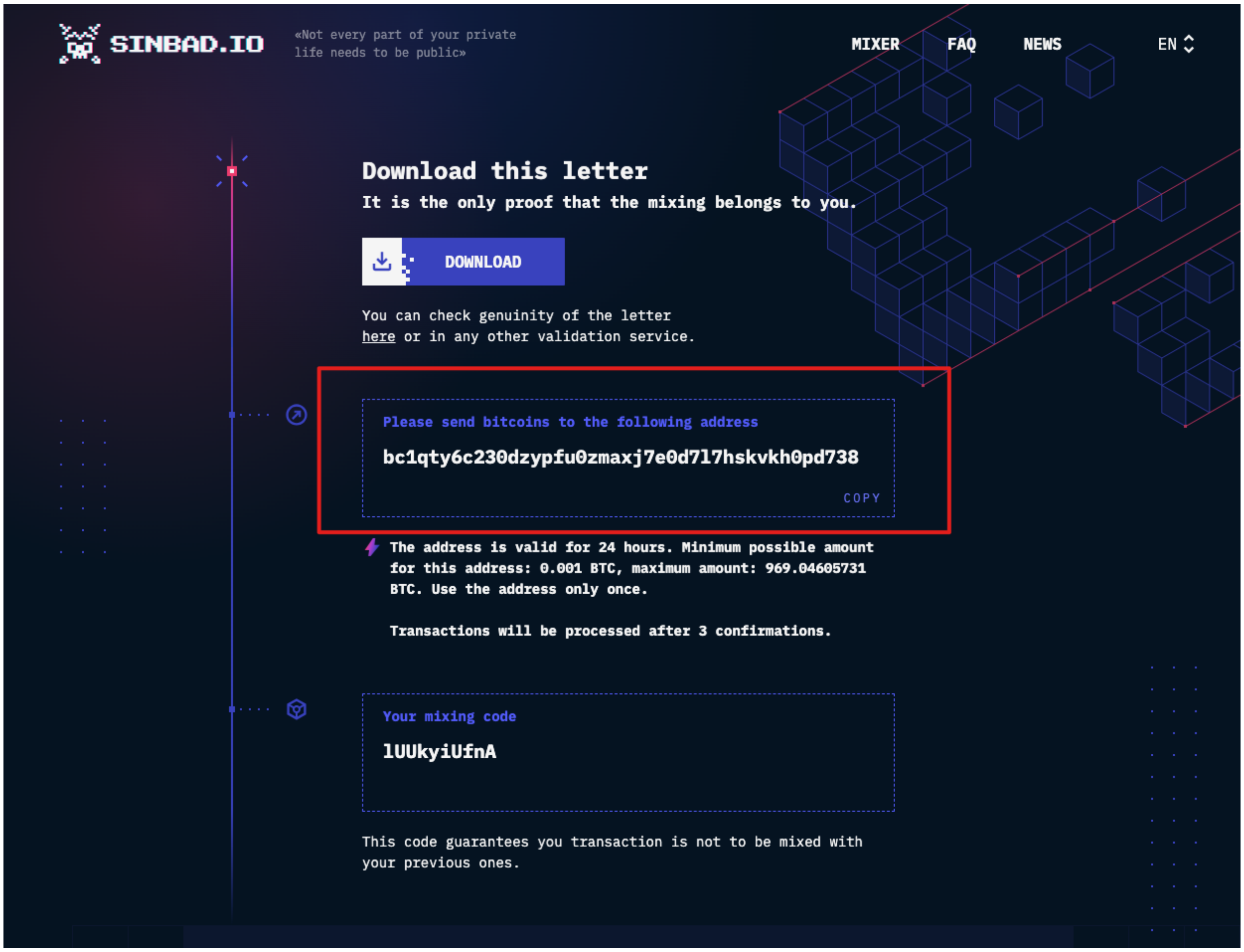
Angel Drainer - $20M

MS Drainer - $59M

3.4 Money Laundering Tools

3.4.1 Sinbad Mixer

Sinbad is a Bitcoin mixer established on October 5, 2022.



Download this letter

It is the only proof that the mixing belongs to you.

You can check genuinity of the letter here or in any other validation service.

Please send bitcoins to the following address

bc1qty6c230dzypfu0zmaxj7e0d7l7hskvkh0pd738

The address is valid for 24 hours. Minimum possible amount for this address: 0.001 BTC, maximum amount: 969.04605731 BTC. Use the address only once.

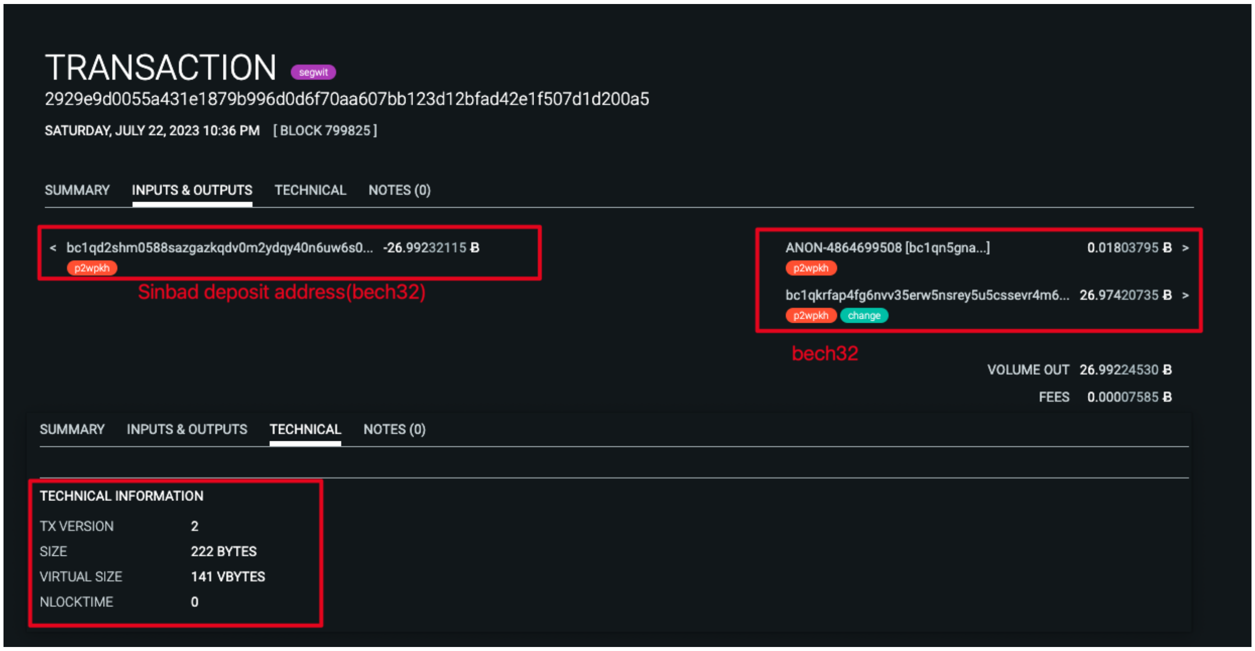
Transactions will be processed after 3 confirmations.

Your mixing code

1UUkyiUfnA

This code guarantees you transaction is not to be mixed with your previous ones.

The Alphapo hackers (Lazarus Group) used Sinbad in their money laundering process, as seen in transactions like:



TRANSACTION segwit
2929e9d0055a431e1879b996d0d6f70aa607bb123d12bfad42e1f507d1d200a5
SATURDAY, JULY 22, 2023 10:36 PM [BLOCK 799825]

< bc1qd2shm0588sazgazkqdv0m2ydqy40n6uw6s0... -26.99232115 Ƀ
p2wpkh

Sinbad deposit address(bech32)

ANON-4864699508 [bc1qn5gna...] 0.01803795 Ƀ >
p2wpkh

bc1qkrfap4fg6nvv35erw5nsrey5u5cssevr4m6... 26.97420735 Ƀ >
p2wpkh change

bech32

VOLUME OUT 26.99224530 Ƀ
FEES 0.00007585 Ƀ

TECHNICAL INFORMATION

TX VERSION	2
SIZE	222 BYTES
VIRTUAL SIZE	141 VBYTES
NLOCKTIME	0

(https://oxt.me/transaction/2929e9d0055a431e1879b996d0d6f70aa607bb123d12bfad42e1f507d1d200a5)

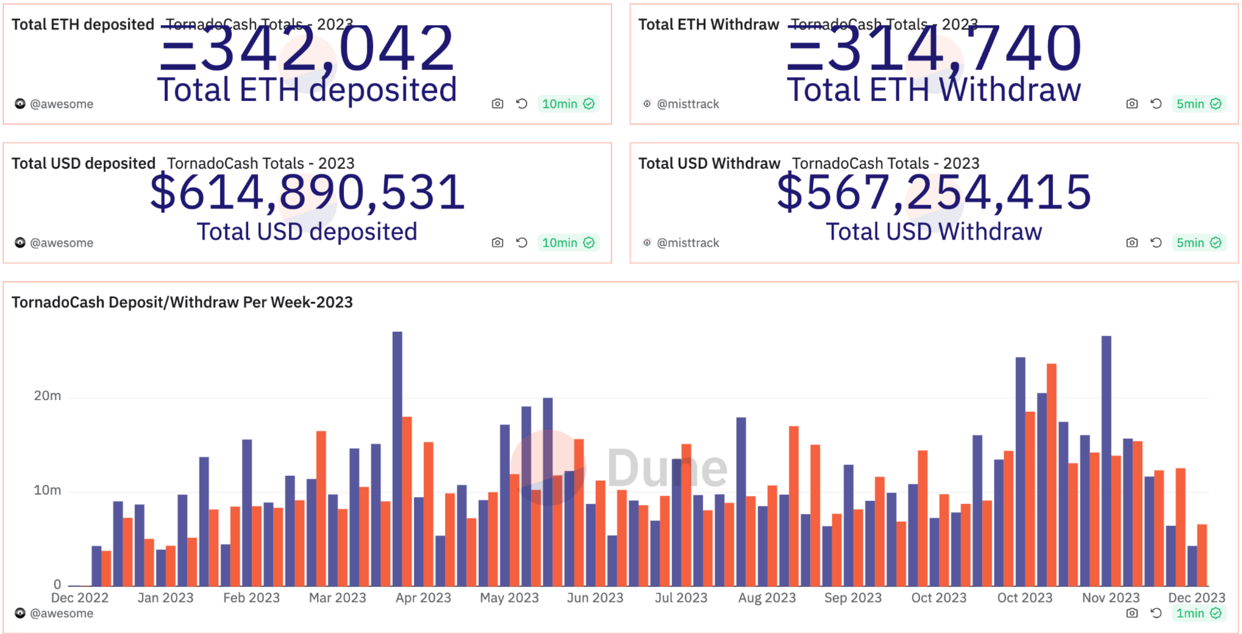
Sinbad's wallet fingerprint for this transaction is as follows:

Input Address Type	Output Address Type	Version	Locktime
bech32(bc1q...)	bech32(bc1q...)	2	0

On November 29, the U.S. Department of the Treasury blocked the cryptocurrency mixing service Sinbad from the global U.S. dollar financial system, citing its support for transactions associated with the North Korean hacking group. The website of Sinbad has been seized by the Federal Bureau of Investigation (FBI), the Dutch Financial Intelligence and Investigation Service, the Dutch Public Prosecution Service, and the National Bureau of Investigation in Finland.

The U.S. Department of the Treasury describes Sinbad as a "virtual currency mixer, a primary money laundering tool for the North Korean hacking group Lazarus, designated by OFAC." Sinbad has handled funds from the Horizon Bridge and Axie Infinity hacking incidents and has also transferred funds related to activities such as "evading sanctions, drug trafficking, purchasing materials related to child sexual exploitation, and engaging in other illegal sales on the dark web market."

3.4.2 Tornado Cash



Total ETH deposited TornadoCash Totals - 2023

Ξ342,042

Total ETH deposited

@awesome 10min

Total ETH Withdraw TornadoCash Totals - 2023

Ξ314,740

Total ETH Withdraw

@misttrack 5min

Total USD deposited TornadoCash Totals - 2023

$614,890,531

Total USD deposited

@awesome 10min

Total USD Withdraw TornadoCash Totals - 2023

$567,254,415

Total USD Withdraw

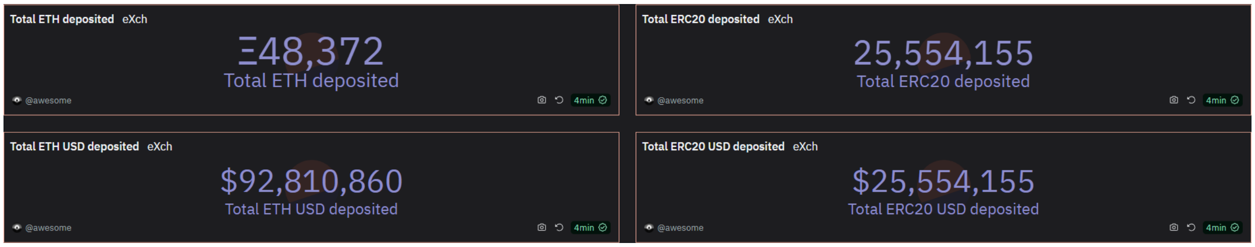
@misttrack 5min

TornadoCash Deposit/Withdraw Per Week-2023

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

In 2023, users deposited a total of 342,042 ETH (approximately $614 million) into Tornado.Cash, and a total of 314,740 ETH (approximately $567 million) was withdrawn from Tornado.Cash.

3.4.3 eXch



Total ETH deposited eXch

Ξ48,372

Total ETH deposited

@awesome 4min

Total ERC20 deposited eXch

25,554,155

Total ERC20 deposited

@awesome 4min

Total ETH USD deposited eXch

$92,810,860

Total ETH USD deposited

@awesome 4min

Total ERC20 USD deposited eXch

$25,554,155

Total ERC20 USD deposited

@awesome 4min

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

In 2023, users deposited a total of 48,372 ETH (approximately $92.81 million) into eXch and 25,554,155 ERC20 stablecoins (approximately $25.55 million) into eXch.

3.4.4 Railgun

At the beginning of 2023, the Federal Bureau of Investigation (FBI) in the United States reported that the North Korean hacker group Lazarus Group used the privacy mixer — Railgun — to launder over $60 million stolen from Harmony's Horizon Bridge. This made tracking the stolen funds more challenging.

To address sanctions, enhance anti-money laundering compliance, and protect user privacy, Railgun entered into a collaboration with Chainway on May 8. They jointly introduced a new feature known as “proof of innocence.” This feature allows users to prove the legitimacy of their transactions, confirming they did not involve any blacklisted addresses, while still protecting their personal identities.

IV. Conclusion

2023 was undoubtedly a year of change and challenge for the blockchain industry, marked by innovation and breakthroughs but also accompanied by risks and volatility. This report was created against this backdrop to provide readers with a comprehensive analysis and in-depth interpretation of the current state of blockchain industry security.

This report summarizes key regulatory compliance policies and trends in the blockchain industry for 2023, including but not limited to the global attitude towards cryptocurrency regulation and a series of critical policy changes. Additionally, it covers blockchain security incidents and anti-money laundering dynamics of the year, analyzes certain money laundering tools, explains typical security incidents and phishing scams, and proposes corresponding prevention and response measures. We hope our efforts will enhance the security awareness of practitioners and users in the blockchain industry.

We are also honored to have contributions from the Web3 anti-fraud platform Scam Sniffer on phishing groups, particularly Wallet Drainers. We believe this content is crucial for understanding their operating methods and profit scenarios. Moreover, we have analyzed and summarized the money laundering tactics of the hacker group Lazarus Group, revealing how they conduct their laundering activities, to provide references for preventing such threats.

Overall, we hope this report provides valuable information, helping readers comprehensively understand the current state of security and anti-money laundering in the blockchain industry. We aim for every industry participant to benefit from this report and contribute to the secure development of the 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 Us

SlowMist is a blockchain security firm established in January 2018. The firm was started by a team with over ten years of network security experience to become a global force. Our goal is to make the blockchain ecosystem as secure as possible for everyone. We are now a renowned international blockchain security firm that has worked on various well-known projects such as Huobi, OKX, Binance, imToken, Crypto.com, Amber Group, Klaytn, EOS, 1inch, PancakeSwap, TUSD, Alpaca Finance, MultiChain, Cheers UP, etc.

SlowMist offers a variety of services that include by 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, Vulpush (Vulnerability monitoring) , SlowMist Hacked (Crypto hack archives), FireWall.x (Smart contract firewall) , Safe Staking and other SaaS products. We have partnerships with domestic and international firms such as Akamai, BitDefender, FireEye, RC², TianJi Partners, IPIP, etc.

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

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

Block money laundering and avoid risks

MistTrack

A crypto tracking and compliance platform for everyone

SlowMist Hack

A comprehensive repository of blockchain incidents

False Deposit Vulnerability Scanner

Creating safe deposit and withdrawals for trading platforms

SLOWMIST

Website

https://slowmist.com

Twitter

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