
SLOWMIST 2023 Mid-year
Blockchain Security and AML Report

Table of Contents

I. Introduction **2**

II. Security Incidents **4**

1. Public Chains 4

2. Exchanges 5

3. DeFi 5

4. Bridges 8

5. NFT 9

6. Wallets 11

7. Asset Recovery 14

III. Anti-Money Laundering **16**

1. Anti-Money Laundering and Regulatory Dynamics 16

2. Crypto Mixers 17

2.1 Tornado Cash 17

2.2 eXch 18

3. Phishing Gangs 18

3.1 Pink Drainer 18

3.2 Vemon Drainer 19

3.3 Monkey Drainer 21

3.4 Pussy Drainer 22

3.5 Inferno Drainer 23

4. Hacker Groups 24

4.1 Lazarus Group 24

4.1.1 Harmony Hack 24

4.1.2 Atomic Wallet Hack 24

IV. Summary **27**

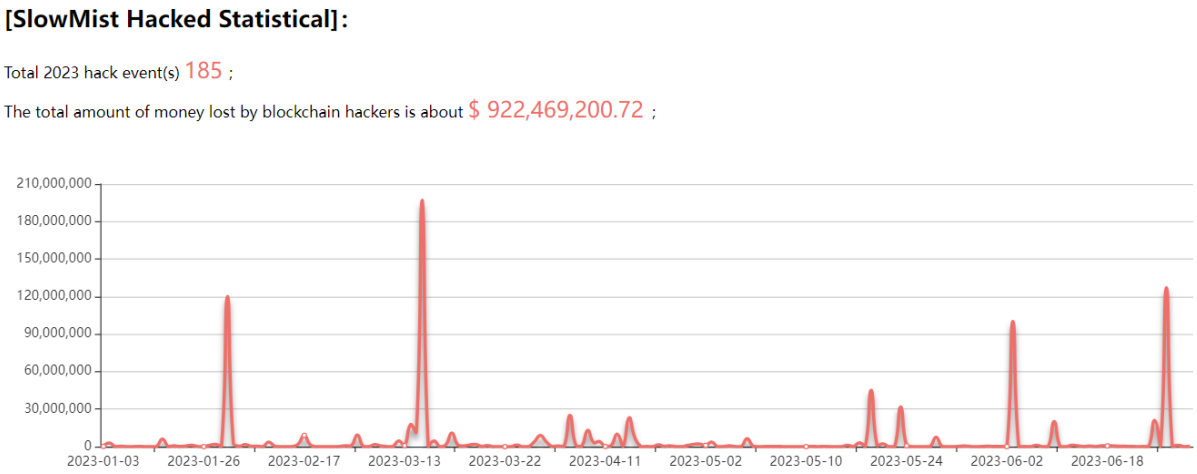
V. Disclaimer **28**

VI. About Us **29**

I. Introduction

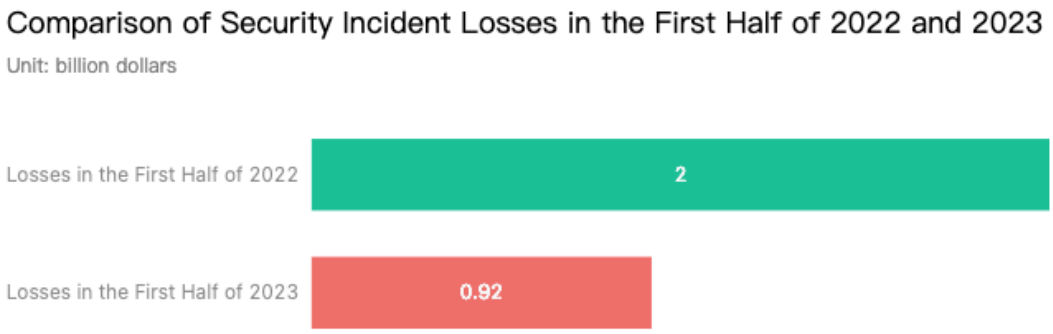
Over the past six months, the global landscape of blockchain technology has witnessed a continuous evolution, bringing forth new possibilities and opportunities for the digital economy. However, with this progressive momentum comes an escalating challenge in blockchain security. As the application of blockchain expands and penetrates deeper, attackers are becoming more cunning and sophisticated, constantly breaching and exploiting vulnerabilities in the blockchain systems, leading to significant losses. In the first half of the year, we have observed a series of security incidents, including attacks on smart contracts, phishing attacks, thefts from exchanges, and various online fraud schemes.

According to statistics from SlowMist Hacked, as of June 30, 2023, there had been a total of 185 security incidents in the first half of the year alone, resulting in a staggering loss of $920 million.



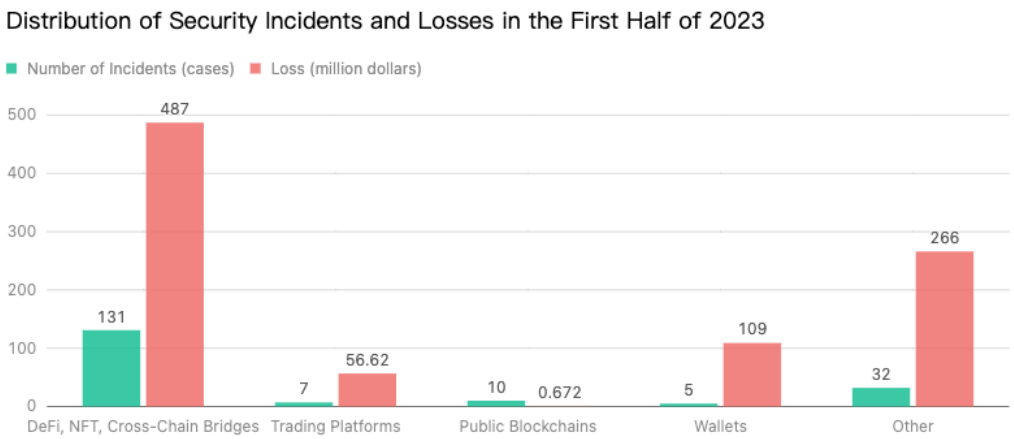
(https://hacked.slowmist.io/)

In comparison to the first half of 2022, where there were a total of 187 incidents resulting in losses of around $2 billion, losses have decreased by 54% year on year.



(Security Incident Losses for the First Half of 2022 and 2023)

Among these, DeFi, NFT, and Bridge events combined totaled 131 incidents, with losses amounting to approximately $487 million. Security incidents involving exchanges numbered 7, resulting in losses of about $56.62 million. Public chain security incidents occurred 10 times, causing a loss of around $672,000. Wallet security incidents were recorded 5 times, accounting for losses of approximately $109 million. Other security incidents numbered 32, resulting in losses of about $266 million.



(Distribution and Loss Amounts of Security Incidents in the First Half of 2023)

Given this backdrop, this report focuses on the safety of the blockchain ecosystem, summarizing the major security incidents of the first half of 2023 and the recovery of funds, providing a comprehensive understanding of current and future blockchain security risks. In addition, due to

the anonymity and decentralized nature of blockchain technology, it is often abused by malicious actors for money laundering activities. Money laundering not only threatens the stability of the financial system, but large-scale activities can also lead to market price fluctuations, market manipulation, and unfair competition in the financial markets. Therefore, this report also seeks to identify suspicious transaction patterns and behaviors through certain incidents, exploring the anti-money laundering status within the blockchain ecosystem.

II. Security Incidents

1. Public Chains

As the foundational infrastructure of blockchain, public chains bear people's expectations for blockchain as the underlying network of Web3. They achieve decentralized control through distributed data and transaction record storage and provide a traceable, secure, and efficient transaction environment. Given the large amounts of digital assets typically present on public chains, attackers may exploit vulnerabilities, malicious code, or other means to attack public chains and steal user funds.

According to SlowMist Hacked, as of June 30, 2023, there were 10 public chain security incidents in the first half of the year, resulting in losses of about $672,000. Most of these security incidents in public chains were caused by forks, usually due to the large number of validators in the public chain, causing divergence in their synchronization and mutual agreements. Additionally, supply chain security has gradually become a focal point in the Web3 industry and globally in recent years. Malicious software and codes can be implanted at different stages of the software supply chain, including development tools, third-party libraries, cloud services, and update processes. Once these malicious elements are successfully implanted, attackers can utilize them to steal digital assets and sensitive user information, disrupt system functions, extort businesses, or massively propagate malicious software.

Although the losses caused by public chain security vulnerabilities are generally small, the impact on the entire chain ecosystem is substantial. So the public chains must undergo professional security audits before going online. It is recommended that public chain projects collaborate

deeply with trustworthy and professional security teams, deploying suitable security measures to minimize the potential for security issues, thereby ensuring the stability and sustainable development of the entire public chain ecosystem.

2. Exchanges

In the realm of blockchain, exchanges play a crucial role. As the primary venues for digital asset trading, these platforms provide users with digital asset storage and management services. If the exchange has security vulnerabilities or is subject to hacker attacks, user assets may be lost or stolen. According to statistics from SlowMist Hacked, as of June 30, 2023, there were 7 security incidents involving exchanges in the first half of the year, leading to losses of up to $56.62 million.

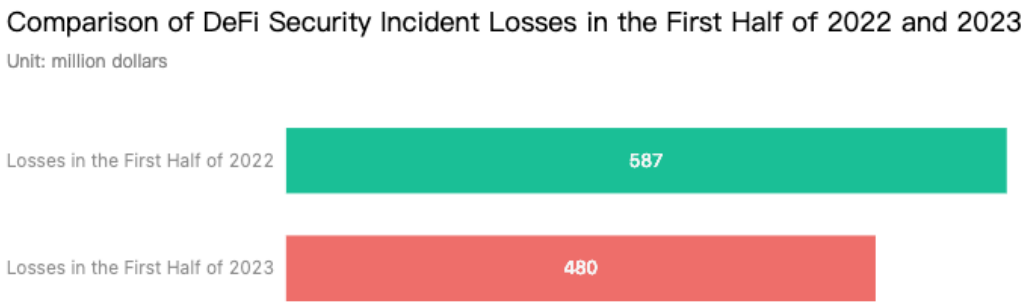
On the one hand, last year the blockchain industry experienced a series of significant incidents, highlighting the importance of operational transparency in exchanges. Regardless of whether users choose to store their assets on an exchange or use custodial services, they must understand that each method carries associated risks. The key is understanding one's risk tolerance and how to manage these risks.

On the other hand, the security of exchanges is vital for protecting user assets, ensuring smooth transactions, building user trust, and promoting the stable development of the cryptocurrency market. It is recommended that all major exchanges strengthen their security by providing training to enhance awareness of potential security threats and social engineering attacks, conducting regular security audits to identify and address potential vulnerabilities and security issues, and ensuring that the software and systems are kept updated with the latest security patches and updates.

3. DeFi

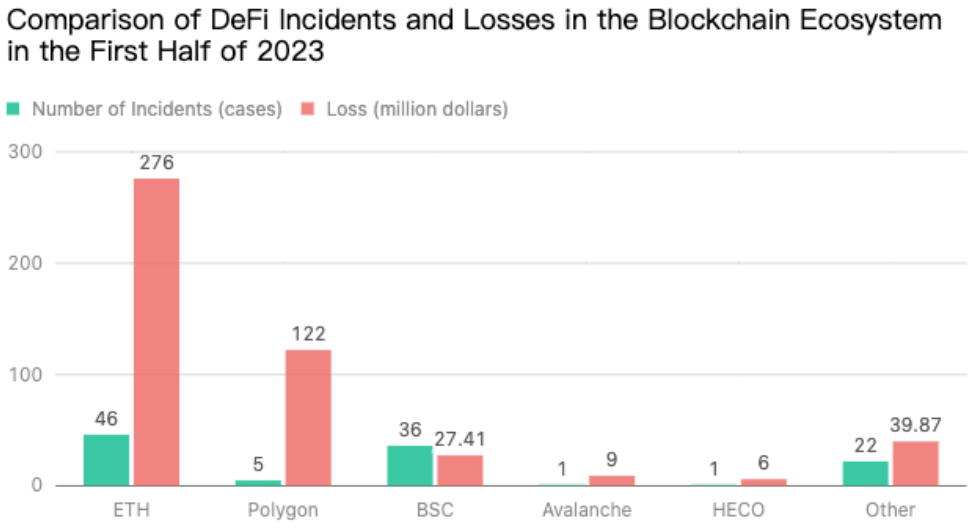
Decentralized Finance (DeFi) offers users a more open, inclusive, and innovative financial experience. It grants individuals greater financial autonomy and provides seamless, secure, and transparent financial services to users globally. DeFi applications often rely on smart contracts to execute various functions such as transactions, lending, and liquidity mining. However, due to quick returns, privacy, anonymity, and relatively lagging regulatory enforcement, DeFi remains an

attractive target for hackers. According to SlowMist Hacked, as of June 30, 2023, there were 111 DeFi security incidents in the first half of the year, leading to losses of up to $480 million. Compared to the first half of 2022 (93 incidents, losses of approximately $587 million), losses have decreased by 18% year-on-year.



(Comparison of DeFi Security Incident Losses in the First Half of 2022 and 2023)

In this, the Ethereum ecosystem suffered the most losses, about $276 million, followed by the Polygon ecosystem with approximately $122 million.



(Comparison of DeFi incidents and Losses in the various ecosystems in the first half of 2023)

Common types of DeFi attacks include exploitation of smart contract vulnerabilities, flash loan attacks, liquidity mining attacks, price manipulations, fake tokens, rug pulls, etc. Most of the recent DeFi security incidents are related to flash loans. Flash loans are not inherently malicious tools, but attackers can use them to borrow a large amount of money in a very short time. These funds can be used to exploit code vulnerabilities, manipulate prices, attack business logic, and more. Of course, the key point here is contract vulnerability. Smart contracts are "smart" because they are highly flexible and can control large amounts of assets and data. Once deployed on the blockchain, they are immutable, do not require human intervention, and their execution process is transparent and visible. However, if smart contracts are exploited due to vulnerabilities, these features of blockchain technology can become a hindrance.

For instance, on February 2, 2023, the non-custodial lending platform BonqDAO and the crypto infrastructure platform AllianceBlock were attacked by hackers due to a vulnerability in BonqDAO's smart contract, resulting in a loss of about $120 million. The hackers removed approximately $114 million of WALBT (worth $11 million), AllianceBlock's packaging of native tokens, and 98 million BEUR tokens ($108 million) from one of BonqDAO's vaults. According to SlowMist’s analysis, the fundamental cause of the attack was that the cost for the attacker to manipulate the oracle's quote was far less than the profit from the attack, thereby maliciously submitting incorrect prices to manipulate the market and liquidate other users.

A month later, another DeFi protocol, Euler Finance, was attacked, with the attacker profiting about $197 million. According to SlowMist’s analysis, the attacker's entire attack process was to use flash loan funds to deposit, then trigger the liquidation logic by directly donating funds to the reserve address after two leveraged borrowings, and finally use soft liquidation to arbitrage out all remaining funds. There were two main reasons for the attack: first, after donating funds to the reserve address, there was no check on whether it was in a liquidation state, which led directly to the mechanism of soft liquidation. Second, when the high leverage triggered a soft liquidation, the yield value would increase, allowing the liquidator to transfer only part of the debt to themselves to obtain most of the liquidated person's collateral. Since the value of collateral is greater than the value of the debt (only part of the debt was transferred due to soft liquidation), the liquidator can successfully pass their health coefficient check (checkLiquidity) to extract the obtained funds. Moreover, multiple projects were affected by the Euler Finance incident, such as Balancer losing

$11.9 million, Yearn Finance losing $1.38 million, Angle Protocol losing $17.6 million, Idle Finance losing $10.99 million, Yield Protocol losing $1.5 million, and Inverse Finance losing $0.86 million. Thankfully, as of April 4, after successful negotiations, the attacker has returned all stolen funds, and other affected projects are gradually recovering.

In light of technological advancements and market expansion, smart contracts are evolving into increasingly intricate and multifaceted entities. It is anticipated that they will carry even greater value in the future. Yet, as we explore the vast potential on the one hand, we must uphold a steadfast commitment to security on the other. The safeguarding of DeFi platforms and smart contracts is an absolute necessity in this landscape. In response to the recurrent emergence of contract security flaws, developers are compelled to engineer smart contracts that are not only robust and secure but also resilient. They must adopt a comprehensive and focused approach, leaving no stone unturned when it comes to safety.

Additionally, DeFi project teams can commission professional third-party security companies or auditors to audit the smart contracts and code and then promptly fix vulnerabilities and security issues based on the audit results. Moreover, the importance of vulnerability disclosure and regulatory compliance mechanisms cannot be understated. These measures serve as crucial shields, protecting DeFi project teams and users from potential attacks. As we chart a course towards the future, let's balance our pursuit of progress with an unwavering commitment to security.

4. Bridges

Bridges, as part of the foundational infrastructure of blockchain, provide solutions and infrastructure for interoperability, asset liquidity, data transmission, decentralized finance, and cross-chain governance among blockchain networks. However, since bridges typically need to handle communication and asset transfers between multiple blockchains, this can involve complex protocols and technologies, and the complexity leads to a greater probability of vulnerabilities and attacks.

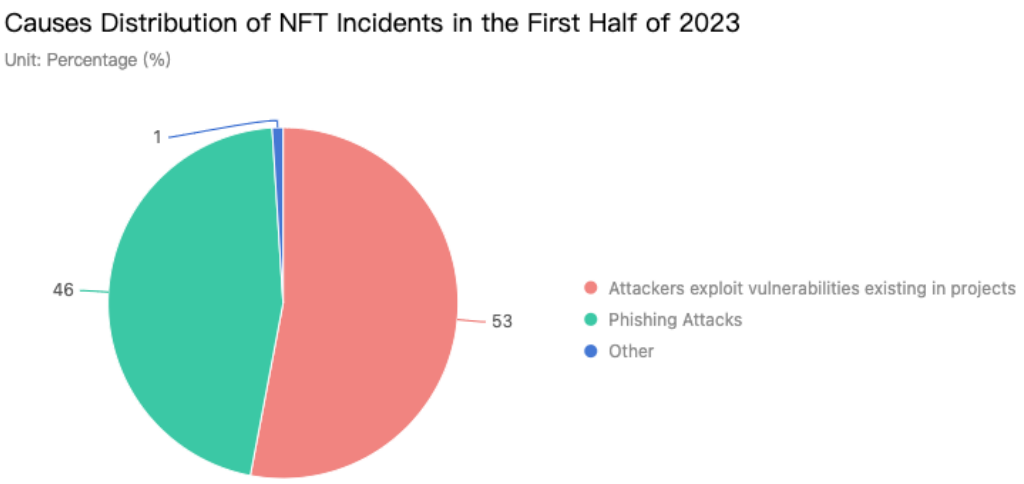
According to statistics from SlowMist Hacked, there were 7 security incidents involving bridges in the first half of 2023, resulting in losses of up to $1.37 million. Compared to the same period in 2022 (7 incidents with losses around $1.043 billion), there was a significant reduction in losses.

These security incidents highlight that bridges can be susceptible to fundamental and technical flaws. Whether it is false deposit issues, private key leaks, or multiple signature verification problems, the security of bridges is often tied to design logic, a key challenge brought about by their interoperability. If bridges have security vulnerabilities or are subject to attacks, user assets may be at risk of being stolen or manipulated as bridges deal with the locking, unlocking, and transfer of assets.

Therefore, ensuring the security and reliability of bridges is of utmost importance for effectively protecting user assets and preventing unnecessary losses. First, the risk of attack can be mitigated by increasing the proportion of signatories. Secondly, partnering with security companies for audits and anti-money laundering efforts can enhance the security of bridges. Lastly, the security of bridges can be strengthened by offering bug bounties.

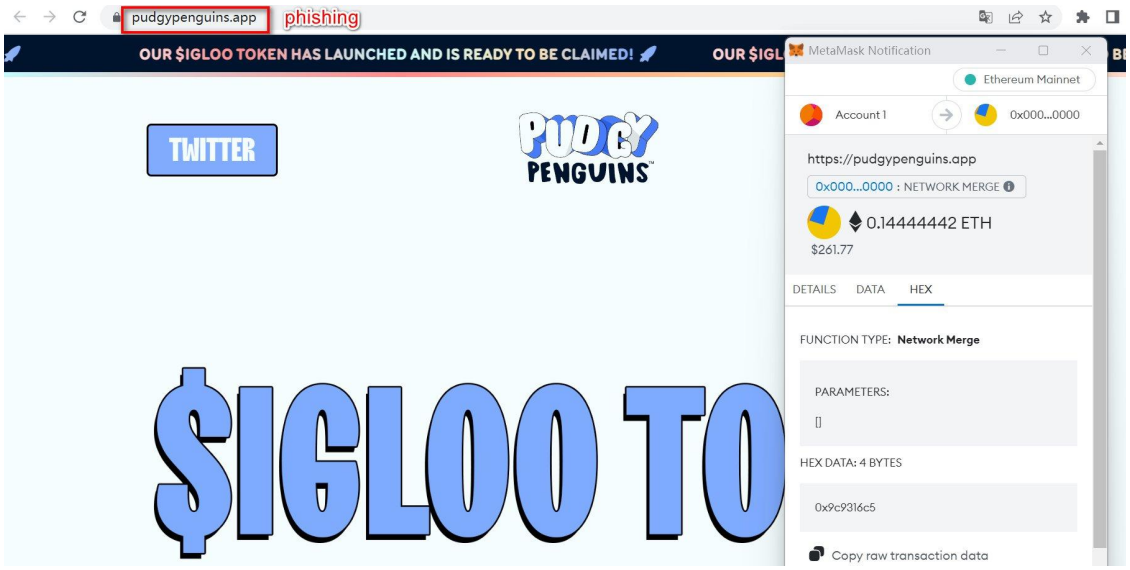
5. NFT

NFTs (Non-Fungible Tokens) represent the uniqueness and ownership of digital assets. They have made it possible for digital art pieces, virtual land, game props, and more to be owned and have rights, bestowing real and irreplaceable value on digital assets. With the development of the NFT market and the high value of NFT artworks, they have also drawn the attention of hackers. According to statistics from SlowMist Hacked, by June 30, 2023, there had been 13 NFT-related security incidents in the first half of the year, resulting in losses of up to $6.31 million. In these NFT security incidents, 53% originated from vulnerabilities inherent in the projects themselves, which were exploited by attackers, followed by phishing attacks, accounting for 46%.



(Causes Distribution of NFT Incidents in the First Half of 2023)

In most NFT phishing attacks, they occurred because official media platforms like Discord/Twitter were hacked, and the hackers posted phishing links to deceive users.



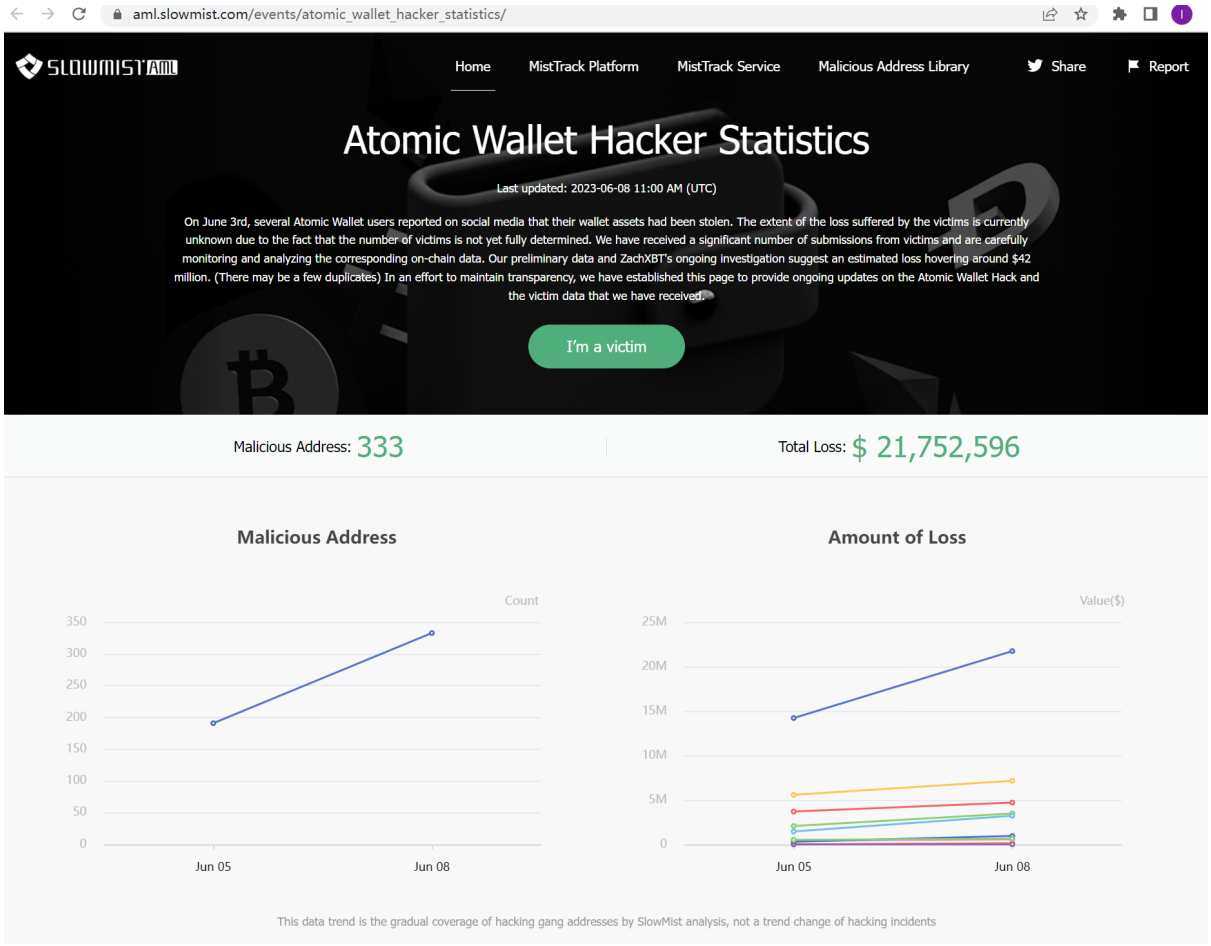
Users and platforms need to enhance their security awareness and adopt appropriate preventive measures. This includes staying vigilant, scrutinizing transactions and application sources, conducting security audits, and using reliable wallets and platforms, all to ensure the security of NFTs and the protection of assets.

6. Wallets

Wallets, as the gateway to the world of blockchain, provide features such as asset management, security assurance, user experience, decentralized control, and interoperability, playing a pivotal role in the blockchain ecosystem. As the interface between users and the blockchain world, wallets offer a convenient, secure, and autonomous blockchain experience, making them attractive targets for hackers. According to SlowMist Hacked statistics, as of June 30, 2023, there were 5 wallet security incidents in the first half of the year, leading to losses of up to $109 million. The most widespread and damaging incident was the Atomic Wallet Hack.

On June 3rd, several Atomic Wallet users reported on social media that their wallet assets had been stolen. By June 4th, based on information provided by numerous victims, the estimated loss from the Atomic Wallet hacking incident was approximately $14.83 million. By June 8th, the loss caused by the hackers had soared to $21.75 million, an increase of $7.63 million from the previous estimate. Currently, the stolen amount has reached a staggering $100 million, and the

cause of the theft is unknown, with the official party stating that an investigation is still underway. During our analysis, we received a large amount of information submitted by victims. In order to maintain transparency, we've set up a dedicated page to continuously update information about the Atomic Wallet attack and data from victims we've received.



(https://aml.slowmist.com/events/atomic_wallet_hacker_statistics/)

Given the frequency of wallet use and the fact that wallet security is directly related to user asset safety, users should stay vigilant and adopt appropriate security measures. These measures include choosing secure and reliable wallets, protecting private keys, avoiding clicking on suspicious links, and refraining from downloading software from unknown sources. These actions can significantly reduce the risk of hacker attacks.

For wallet providers, a comprehensive security audit is necessary, with a focus on enhancing the user interaction security aspect, strengthening the “what you see is what you sign” mechanism, and minimizing the risk of phishing attacks. For example:

- Phishing website alerts: Accumulate phishing websites using community or ecological resources and prominently alert and warn users when they interact with these sites.
- Signature recognition and alerts: Recognize and alert users to signature requests like eth_sign, personal_sign, and signTypedData, with particular emphasis on the risks of eth_sign blind signatures.
- What you see is what you sign: Wallets can have an exhaustive parsing mechanism for contract calls to avoid phishing, so users know the detailed content when DApps construct transactions.
- Pre-execution mechanism: The transaction pre-execution mechanism can help users understand the effect after the transaction broadcast, assisting them in predicting transaction execution.
- Scam alerts for the same last digits: When displaying addresses, prominently remind users to check the complete target address to avoid scams with the same last digits. Implement a whitelist address mechanism where users can add commonly used addresses to the whitelist, avoiding similar attacks.
- For transaction display, consider the option to hide small or worthless token transactions to avoid the same last digits phishing.
- AML compliance alerts: When transferring funds, remind users if the target address of the transfer will trigger AML rules using the AML mechanism.

For individual users, the main risks lie in "domain and signature". Following the security laws and principles below can help avoid most risks:

Two main security laws:

- Zero trust: To make it simple, stay skeptical, and always stay so.
- Continuous Security Validation: In order to trust something, you have to validate what you doubt and make validating a habit.

Security principles:

- For all the knowledge on the Internet, refer to at least two sources, corroborate each other, and always stay skeptical.
- Segregate. Don't put all the eggs in one basket.
- For wallets with important assets, don't do unnecessary updates.
- What you see is what you sign. You need to be aware of what you are signing, and of the expected result after the signed transaction is sent out. Don't do things that you will regret afterwards.
- Pay attention to system security updates. Apply them as soon as they are available.
- Don't download & install programs recklessly; this can actually prevent most risks.

We highly recommend reading and mastering the "Blockchain Dark Forest Selfguard Handbook".

7. Asset Recovery

In the first half of 2023, there were 10 incidents in which all or part of the stolen assets were recovered after an attack, totaling approximately $232 million in stolen assets, of which $219 million was returned, accounting for 94% of the stolen assets. In these 10 incidents, assets from 3 protocols were fully refunded. The return of stolen assets may become a new trend, whether through a bounty or reasonable negotiation. However, this requires a complete and comprehensive strategy; otherwise, you may once again become prey to attackers.

The anonymity and decentralization of blockchain make it difficult to recover stolen funds. However, users and project teams can increase the likelihood of recovery in the following ways:

- Notify relevant institutions immediately: Report to local law enforcement agencies, financial regulatory bodies, and relevant blockchain project teams. Provide detailed information and evidence and cooperate with the investigation.
- Contact the exchange: If the funds were stolen on a certain exchange, immediately contact them and provide detailed information about the incident. The exchange or platform may take measures to investigate and assist in resolving the issue.
- Cooperate with the community: Publicize the incident and cooperate with relevant community members to share information and experience. Other users may provide useful information about the attackers or attack techniques.
- Seek professional help: Consult professional blockchain security companies or lawyers for legal and technical professional help. They can provide relevant advice. and guidance, help to recover funds as much as possible, or take other appropriate legal measures.

Of course, the most important thing is to take preventive measures to reduce the risk of funds being stolen. This includes using secure and reliable wallets and exchanges; protecting private keys and access credentials; avoiding clicking on suspicious links and downloading software from unknown sources; and maintaining security awareness and knowledge updates.

III. Anti-Money Laundering

1. Anti-Money Laundering and Regulatory Dynamics

Some anti-money laundering and regulatory dynamics in the first half of 2023 are as follows:

Tether: In the first half of 2023, a total of 85 ETH addresses were blocked, and the USDT-ERC20 assets on these addresses were frozen and not transferable.

Circle: In the first half of 2023, a total of 20 ETH addresses were blocked, and the USDC-ERC20 funds on these addresses were frozen and not transferable.

ChipMixer: On March 15, Europol stated that German and American authorities had seized 44 million euros from the cryptocurrency mixer ChipMixer. Europol stated that the authorities have shut down the platform's infrastructure, seized four servers, 7 TB of data, and 1909.4 BTC (47.7 million dollars).

U.S. Treasury Department: On April 24, it sanctioned three North Koreans who provided support for the North Korean hacker group Lazarus Group; on May 20, it sanctioned a crypto wallet helping Russia to transfer funds; on May 24, it sanctioned crypto wallets associated with the North Korean government.

Hong Kong, China: On May 31, the Hong Kong Virtual Asset Rating Agency (HKVAC) announced its official establishment and will launch the "Virtual Asset Index" and "Virtual Asset Exchange Rating." On June 1, Hong Kong's virtual currency licensing system officially opened, and platforms interested in engaging in virtual asset business can apply for a license from the Hong Kong Securities and Futures Commission and be subject to its supervision.

Indonesia: On June 18, the Indonesia Commodity Futures Trading Supervisory Agency (Bappebti) released a list of crypto assets that can be traded in Indonesia. At the same time, Indonesia plans to establish a national-backed crypto exchange this year.

United Kingdom: On June 19, the UK's House of Lords passed the "Financial Services and Markets Bill (FSMB)." This bill defines cryptocurrency-related financial activities and market activities as regulated activities and implements financial regulation by treating stablecoins as a legal payment method.

France: On June 19, the French market regulatory agency released a discussion paper on DeFi, expressing support for global DeFi rules.

2. Crypto Mixers

2.1 Tornado Cash

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

In the first half of 2023, users deposited a total of 165,027 ETH (approximately $285 million) into Tornado.Cash, and a total of 142,347 ETH (approximately $246 million) were withdrawn from Tornado.Cash.

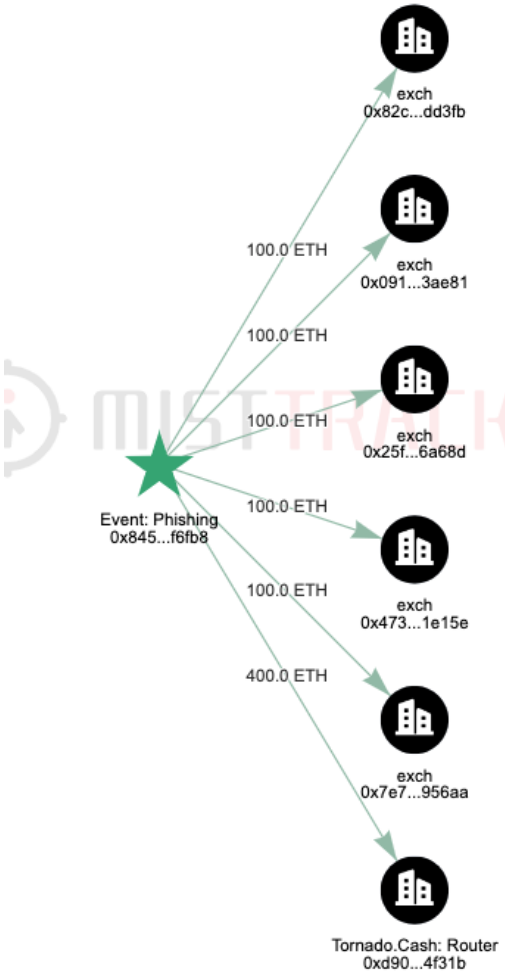
2.2 eXch

In the first half of 2023, users deposited a total of 9,983 ETH (approximately $17.72 million) into eXch, and deposited a total of 6,608,354 ERC20 stablecoins (approximately $6.6 million) into eXch.

3. Phishing Gangs

3.1 Pink Drainer

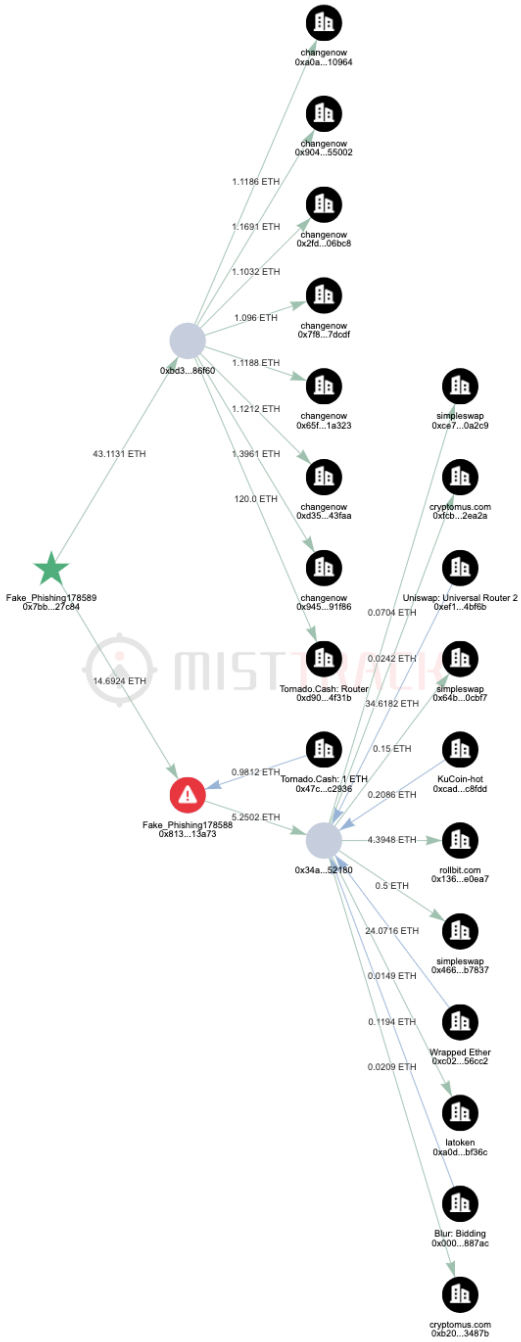
On June 9, several Discord and Twitter hacking incidents occurred, including those at Evomos, Pika Protocol, OpenAI CTO, Orbiter Finance, etc. These incidents are all related to an organization called Pink Drainer, which obtained Discord tokens through social engineering attacks and sent phishing links through Discord administrator accounts. Many users accidentally opened malicious websites and signed malicious signatures, resulting in asset losses. According to the data, the gang has stolen about $3 million in assets from nearly 1,932 victims. Among them, one victim lost an NFT worth nearly $320,000.



3.2 Vemon Drainer

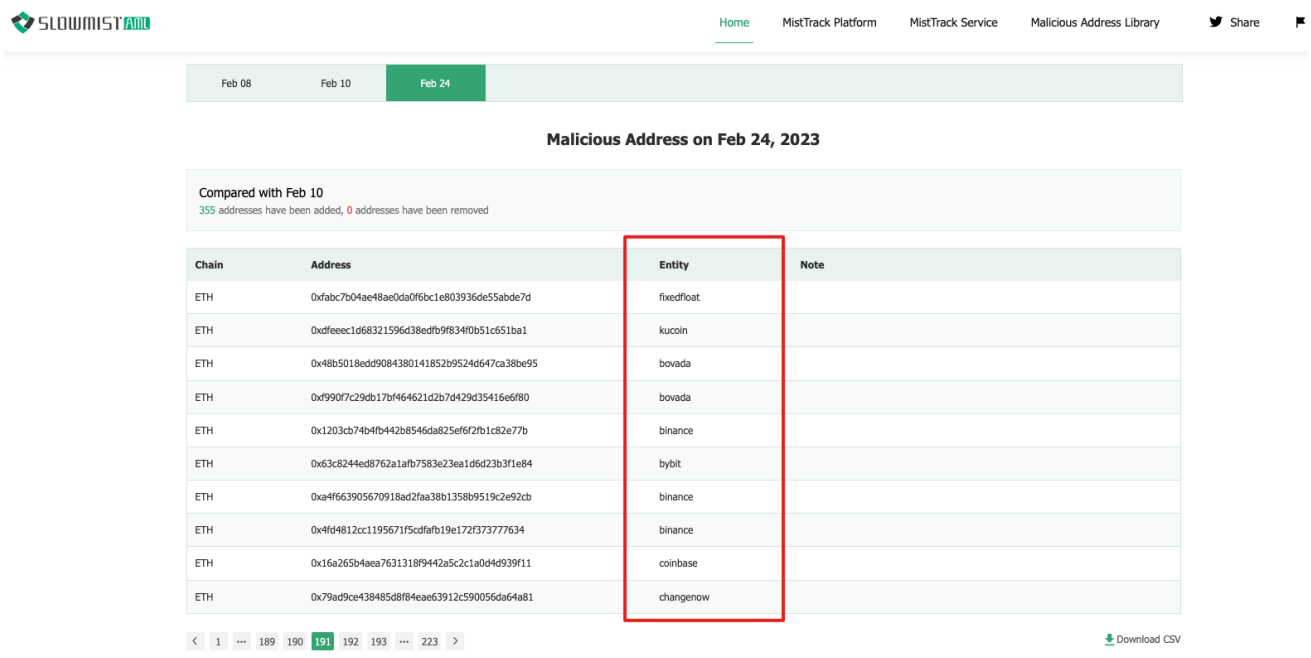
Venom Drainer is a phishing service provider. According to ScamSniffer data, the gang has defrauded $27 million from 15,000 victims. The service provider has created more than 530 phishing websites, targeting over 170 brands, including Arbitrum, Blur, zkSync, Optimism, and MetaMask. They use various scams, such as obtaining user approval through Permit or Approve, then moving the user's ERC20 tokens on-chain, or deceiving users into signing malicious NFT listings, which contain lower listing prices, usually 0. Once the user signs, their NFT can be transferred through the listing signature. The gang claims to have implemented a Blur-based phishing module and has been trying to recruit people since March 20. This is to facilitate sending private messages or work slips to Discord administrators of well-known crypto projects in order to participate in launching phishing activities and receive 15% of the proceeds. According to

MistTrack's analysis, the Venom Drainer gang mainly launders money through platforms such as Tornado Cash, ChangeNOW, and SimpleSwap.



3.3 Monkey Drainer

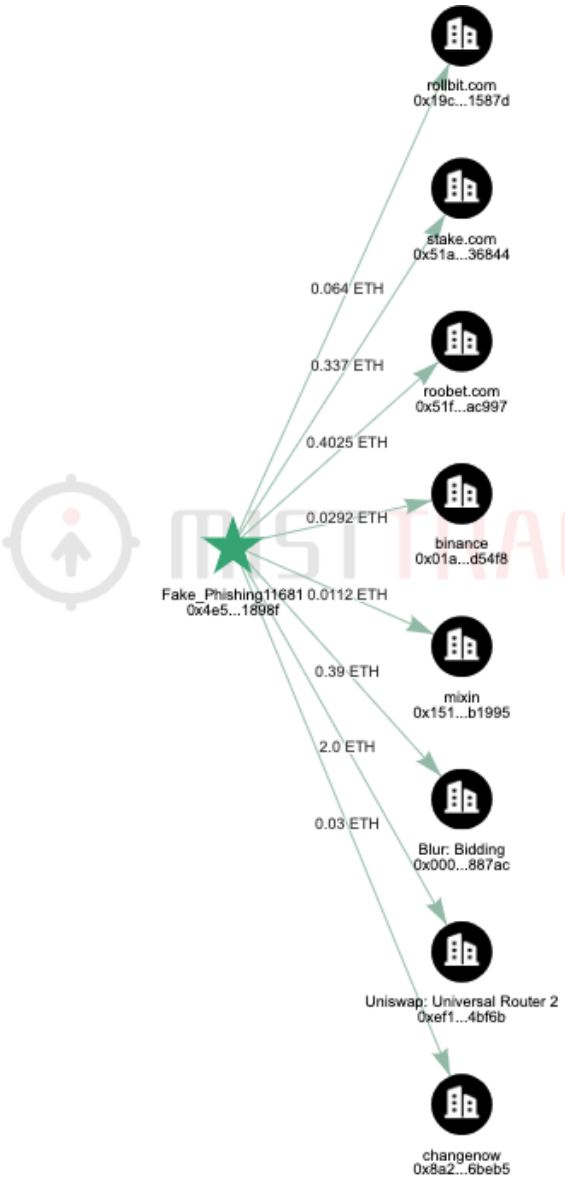
Monkey Drainer is a notorious online phishing organization that has stolen millions of dollars. On March 1, 2023, Monkey Drainer abruptly shut down its services and destroyed all related files, servers, and equipment. According to SlowMist's analysis, the organization mainly phishes through bait websites related to fake NFTs published by fraudulent KOL Twitter accounts, Discord groups, etc., involving more than 2,000 domain names. Phishing templates use templates provided by the gray supply chain, such as ad sales descriptions and phishing supply chain support functions. The core code uses obfuscation and inducement methods to make victims sign Seaport, Permit, etc., and uses Permit USDC's offline authorization signature mechanism, etc., upgrading the original phishing mechanism. The Monkey Drainer organization made a total profit of about $16,506,602 through phishing, of which phishing NFT made a profit of about $9,374,344, and ERC20 Token made a profit of about $7,132,257. The main profit ERC20 Token types are USDC, USDT, LINK, ENS, stETH. The organization does not use a dedicated website to count victim visits on each site but uses a simple and crude method to directly fish and deploy in batches. It is speculated that the organization used phishing templates for batch automated deployment.



(https://aml.slowmist.com/events/monkey_drainer_statistics/)

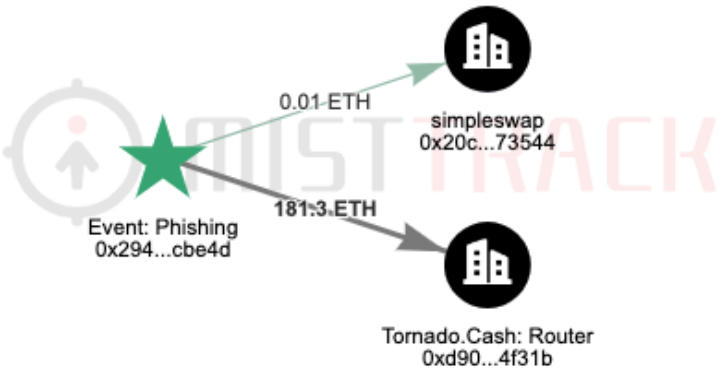
3.4 Pussy Drainer

Since January 6, Pussy Drainer phishing activities have affected more than 3,000 victims, with a total amount stolen of approximately $15 million. The biggest victim lost assets worth $2.3 million.



3.5 Inferno Drainer

On May 19, a scam manufacturer named Inferno Drainer gradually emerged, which specializes in multi-chain scams and mainly charges a 20% fee for stolen assets. According to the data, nearly 4,888 victims have been found so far, with stolen assets totaling about $5.9 million. Since March 27, Inferno has created more than 689 phishing websites, targeting more than 220 brands. According to MistTrack's analysis, the Inferno Drainer gang mainly uses Tornado Cash, SimpleSwap, and other platforms for money laundering.



4. Hacker Groups

4.1 Lazarus Group

4.1.1 Harmony Hack

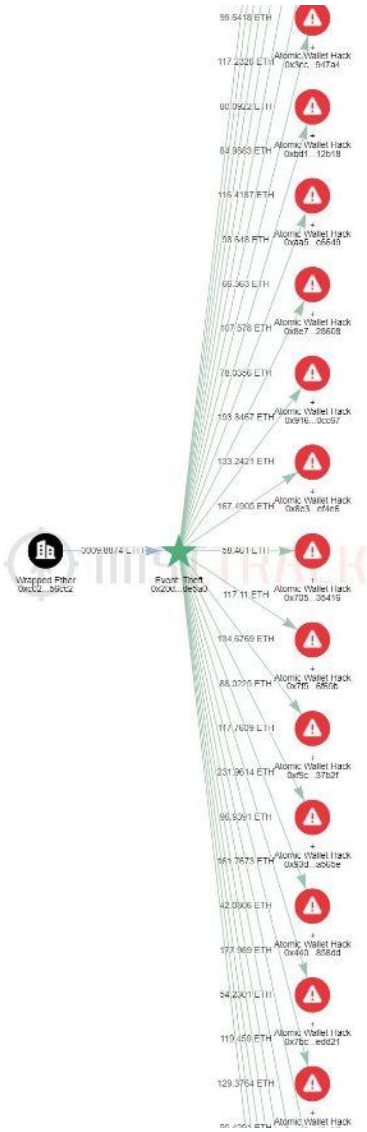
On June 23 last year, the Harmony Bridge was attacked, causing a loss of about $100 million. On January 13 this year, the hackers began to move funds extracted from Tornado Cash, depositing and withdrawing them in the privacy network Railgun, after which some of the funds were transferred to the exchange and withdrawn to the BTC network. On January 16, the hackers moved the BTC funds previously in the exchange. On January 23, the FBI identified Lazarus Group as responsible for the Harmony Hack incident. After several days of multi-layer transfers, some funds were transferred back to the exchange again, while others were cross-chained to the Avalanche chain via the Avalanche Bridge, finally exchanged into USDT or USDD, and transferred to the coin-mixing network in the ETH or TRON chains. In this process, the hackers used a new money-laundering method. According to MistTrack's analysis, its cross-chain path is BTC Network -> Avalanche -> ETH Network -> TRON Network.

4.1.2 Atomic Wallet Hack

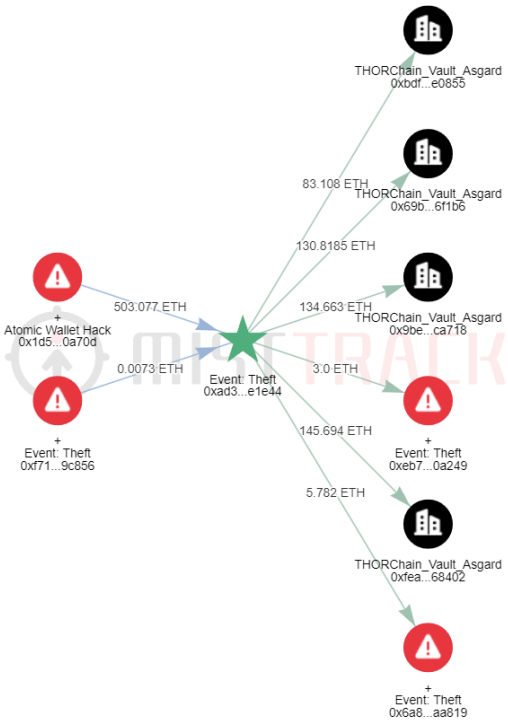
On June 3, some Atomic Wallet users reported on social media that their wallet assets had been stolen. According to statistics, the stolen amount has reached $100 million, and the investigation has found 142 new suspicious addresses related to hackers. By June 9, the investigation revealed that the fund transfer mode of the Atomic Wallet hackers was similar to the strategy previously

used by Lazarus Group. According to MistTrack's analysis, the following three methods of money laundering have emerged:

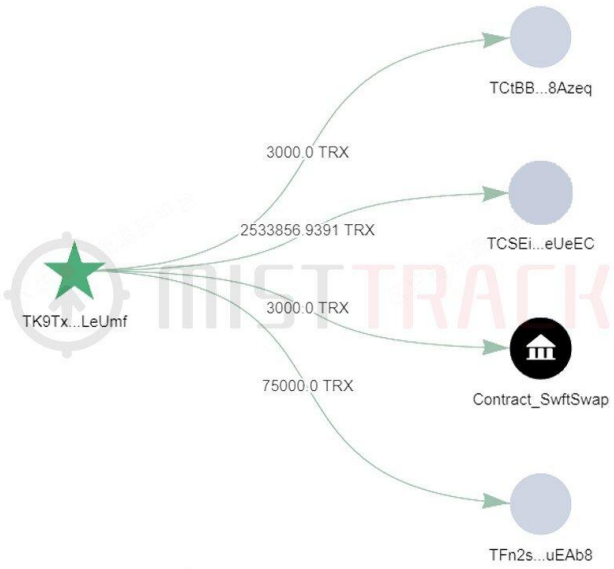
1) The hackers deployed two exchange contracts separately: one first exchanged ETH for WETH, and the second then exchanged WETH for ETH. Then the exchanged ETH was dispersedly transferred to multiple addresses, and after being exchanged for WETH again, it was cross-chained to Avalanche. Finally WETH was exchanged for BTC and cross-chained from Avalanche to the BTC network.



2) The hackers transferred ETH to THORChain, exchanged ETH for BTC, and cross-chained to a BTC address. In addition, the hackers also used SwftSwap for cross-chain.



3) The hackers swapped most of the USDT to TRX via SunSwap and gathered it at a certain TRON address. This TRON address then dispersed TRX to multiple addresses, with most finally going into the exchange deposit address. Some of it used SunSwap to swap TRX for USDT. Most USDT was dispersed into the exchange, and some was used SwftSwap for cross-chain.



IV. Summary

This report mainly introduces the blockchain security incidents and the anti-money laundering situation in the first half of 2023. We hope that this report can provide valuable insights for the blockchain industry and individuals, helping everyone better understand and respond to the ever-changing threats to blockchain security, promote the continuous development and innovation of blockchain security, and jointly build a more secure and trusted blockchain ecosystem.

Finally, we would like to thank each of our ecosystem partners. This includes our clients, media partners, Dark Handbook contributors, and SlowMist Zone partners. We would like to give special thanks to Safeheron, BugRap, Keystone, Scam Sniffer, GoPlus, Eigenphi, Chainbase, SunSec, Alphatu, Steven, and other partners. It is your strong support that has made us more determined to keep moving forward and continue to be good guardians of the blockchain. We hope that we can continue to join forces and work together to bring more light to the dark forest of blockchain.

V. Disclaimer

The content of this report is based on our understanding of the blockchain industry, the SlowMist Blockchain Hack Archive, and the data support of the anti-money laundering tracking system, MistTrack. However, due to the "anonymity" characteristic of blockchain, we cannot guarantee the absolute accuracy of all data, and we cannot be responsible for any errors, omissions, or losses caused by using this report. At the same time, this report does not constitute any investment advice or other analytical basis.

If there are any omissions or deficiencies in this report, we welcome everyone's criticism and correction.

VI. About Us

SlowMist was built with a focus on blockchain ecosystem security. We were established in January 2018 by a team with over ten years of network security experience. Our team members have helped make our organization an industry leader in blockchain security. We have served many leading or well-known projects around the world through our integrated security solutions ranging from threat detection to threat defense.

We have actively participated in the promotion of blockchain security standards. We're one of the first organizations in China to enter the "2018 China Blockchain Industry White Paper" of the Ministry of Industry and Information Technology. We're also a member of the "Joint Laboratory of Blockchain and Network Security Technology" in the Guangdong-Hong Kong-Macao Greater Bay Area and recognized as a "National High-tech Enterprise" less than two years after our establishment.

SlowMist offers a variety of services including security audits, threat information, bug bounties, defense deployment, security consulting, and other security-related services. We also offer AML(Anti-money laundering) software, DoS (Denial of Service) scanners Vulpush (Vulnerability monitoring), SlowMist Hacked(Crypto hack archives), FireWall.x (Smart contract firewall) and other SaaS products. We have partnerships with domestic and international firms such as Akamai, BitDefender, FireEye, 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 were able to spread awareness and raise the security standards in the blockchain industry.

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

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